U.S. Department of Energy
Washington, D.C.

ORDER

DOE O 471.2A

Approved: 03-27-97
Sunset Review: 09-26-97
Expires: 09-26-99

SUBJECT: INFORMATION SECURITY PROGRAM

1. OBJECTIVES.

   a. To establish an Information Security Program for the protection and control of classified and sensitive information. The Information Security Program includes the following programs.

      (1) Operations Security (OPSEC).

      (2) Classified Matter Protection and Control (CMPC).

      (3) Classified Information Systems Security (ISS).

      (4) Technical Surveillance Countermeasures (TSCM).

      (5) Security of Foreign Intelligence Information (FII) and Sensitive Compartmented Information (SCI).

      (6) Security of Special Access Programs (SAP).

      (7) Protection of Unclassified Controlled Nuclear Information (UCNI), Official Use Only (OUO), and Naval Nuclear Propulsion Information.

   b. To ensure that individuals protect classified information and sensitive unclassified information to which they have access or custody.

   c. To ensure that classified information is not released to the public until it has been formally and officially declassified by an appropriate declassification authority and its release is otherwise permitted by applicable law or regulation. Likewise, no sensitive unclassified information shall be released without review for applicable release restrictions.

   d. To establish protection systems that require higher degrees of protection for each higher classification level (Confidential, Secret, Top Secret).

Vertical Line Denotes Change.

DISTRIBUTION:
All Departmental Elements

INITIATED BY:
Office of Safeguards and Security

2. CANCELLATIONS. The Orders listed below are canceled. Cancellation of an Order does not, by itself, modify or otherwise affect any contractual obligation to comply with such an Order. Canceled Orders which are incorporated by reference in a contract shall remain in effect until the contract is modified to delete the reference to the requirements in the canceled Orders.

   a. DOE 5630.8A, SAFEGUARDING OF NAVAL NUCLEAR PROPULSION INFORMATION, of 7-31-90.

   b. DOE 5639.1, INFORMATION SECURITY PROGRAM, of 10-19-92.

   c. DOE 5639.5, TECHNICAL SURVEILLANCE COUNTERMEASURES PROGRAM, of 8-3-92.

   d. DOE 5639.6A, CLASSIFIED AUTOMATED INFORMATION SYSTEM SECURITY PROGRAM, of 7-15-94.

   e. DOE 5639.7, OPERATIONS SECURITY PROGRAM, of 4-30-92.

   f. DOE M 5632.1C-1, MANUAL FOR PROTECTION AND CONTROL OF SAFEGUARDS AND SECURITY INTERESTS, of 7-15-94, Chapter III, paragraphs 1, 2, and 4 through 9.

3. APPLICABILITY.

   a. General. This Order applies to Departmental Elements responsible for protection and control of classified information and sensitive unclassified information.

   b. Application to Contracts. Except as excluded in paragraph 3c below, this Order applies to covered contractors (a DOE contractor or subcontractor subject to DOE Acquisition Regulation, Part 952.204-2, or other clause requiring protection of classified information, nuclear material, or other sensitive information or activities). Contractor requirements are listed in the Contractor Requirements Document, Attachment 1. The Contractor Requirements Document is issued to aid procurement request initiators in identifying requirements that are to be incorporated into contracts by contracting officers.

   c. Exclusion. Requirements of this Order that overlap or duplicate requirements of the Nuclear Regulatory Commission related to radiological emergency planning do not apply to the design, construction, operation, and decommissioning of Office of Civilian Radioactive Waste Management facilities.

Vertical Line Denotes Change.

4. REQUIREMENTS.

a. Access to Classified and Sensitive Unclassified Information.

(1) Access to classified information shall be granted only to persons who possess the appropriate access authorization and need-to-know according to DOE O 472.1, PERSONNEL SECURITY PROGRAM. Supervisors or other responsible officials who are knowledgeable about the classified information and the responsibilities of the individual may determine need-to-know. The individual disseminating classified information is responsible for ensuring that the recipient of the information has the appropriate access authorization and need-to-know.

(2) Before a facility is eligible for access to classified information, a DOE facility clearance must be granted according to DOE O 470.1, SAFEGUARDS AND SECURITY PROGRAM.

(3) Access to sensitive unclassified information shall be granted only to persons who possess the appropriate need-to-know. The individual disseminating sensitive unclassified information is responsible for determining the recipient's need-to-know. Access to Naval Nuclear Propulsion Information shall only be granted to U.S. citizens who have a need-to-know.

(4) Owners of data are responsible for determining the sensitivity of information before it is used, processed, or stored on information systems and for ensuring the system is accredited for the information to be used in it.

(5) Classified and unclassified Naval Nuclear Propulsion Information shall be protected in accordance with Naval Sea Systems Command Instruction C5511.32B, dated 12-22-93. Naval Nuclear Propulsion Information shall be protected pursuant to export control requirements and statute. Questions regarding Naval Nuclear Propulsion Information shall be directed to the Deputy Assistant Secretary for Naval Reactors.

b. Classified Information Systems. Security requirements for classified information systems contained in this Order and DOE M 5639.6A-1 are to be implemented as follows.

(1) Existing accredited classified information systems shall remain accredited until reaccreditation is required, either because of expiration of accreditation (3 years) or because of significant changes in the security requirements of the information system. Reaccreditation shall be accomplished under the requirements of this Order and DOE M 5639.6A-1. These systems must meet the requirements of this Order and DOE M 5639.6A-1 no later than July 15, 1997.

(2) Classified information systems in the process of accreditation on July 15, 1994, may be accredited under DOE 5639.6A; however, the requirements of this Order and DOE M 5639.6A-1 must be met by these systems no later than January 15, 1996.

Vertical Line Denotes Change.

(3) New classified information systems that are under development and that have not begun certification and security performance testing shall meet the requirements of this Order and DOE M 5639.6A-1.

c. Implementation Plans. Implementation plans are necessary only for requirements that cannot be implemented with existing resources or within 6 months of the effective date of this Order. These plans shall be developed within 90 days of the effective date of this Order and submitted to the Office of Safeguards and Security. Implementation plans shall ensure that full implementation of this Order is accomplished within 1 year of the effective date of the Order.

d. Deviations. Unless otherwise stated in this Order, deviations from the requirements in this Order shall be processed according to DOE O 470.1, SAFEGUARDS AND SECURITY PROGRAM.

e. Supplementary Directives. The following Manuals supplement this Order and contain non-discretionary, mandatory Information Security Program requirements, standards, and procedures.

(1) DOE M 471.2-1, CLASSIFIED MATTER PROTECTION AND CONTROL.

(2) DOE M 5639.6A-1, MANUAL OF SECURITY REQUIREMENTS FOR THE CLASSIFIED AUTOMATED INFORMATION SYSTEM SECURITY PROGRAM.

(3) DOE "Technical Surveillance Countermeasures Procedural Manual," (classified).

f. Guides. The following Guides shall be maintained by the Office of Safeguards and Security to provide discretionary, non-mandatory assistance in implementing the requirements of the above Manuals and this Order:

(1) DOE G 471.2-1, CLASSIFIED MATTER PROTECTION AND CONTROL, and

(2) "DOE OPSEC Procedural Guide."

g. Definitions. Terms commonly used in the program are defined in the "Safeguards and Security Definitions Guide," which is maintained and distributed by the Office of Safeguards and Security.

5. RESPONSIBILITIES AND AUTHORITIES.

a. Heads of Departmental Elements.

(1) Designate an individual(s) to be responsible for bringing to the attention of the contracting officer the applicable requirements in the Contractor Requirements Document, including supporting details, for each procurement. Unless another

individual is designated, the responsibility is that of the procurement request originator (the individual responsible for initiating a requirement on DOE F 4200.33, "Procurement Request Authorization").

(2) Develop and submit implementing plans as required.

(3) In coordination with the Director of Security Affairs, approve the release of SECRET and CONFIDENTIAL information within their programmatic areas of responsibility, originated by DOE or contractors, to other Government agencies and their contractors, to foreign governments, and to international organizations, as deemed appropriate.

(4) Approve the distribution of classified scientific and technical reports within their programmatic areas of responsibility.

(5) Ensure the protection of other Federal agencies' classified matter with at least those precautions prescribed for DOE information of the same classification.

(6) Send classified information containing Restricted Data and/or Formerly Restricted Data that is to be provided to foreign entities to the Deputy Assistant Secretary for Facility Transition and Technical Support, who will channel the information to the Joint Atomic Information Exchange Group (JAIEG) for review prior to release.

(7) Ensure that upon completion of work under contract, subcontract, or other agreement, a review of classified matter associated with that effort is accomplished to reduce the volume of classified matter insofar as practical and that proper authorizations, if applicable, are obtained for the elimination or retention of such matter.

b. Managers of Operations Offices and Field Offices, and Director, Headquarters Operations Division, Office of Safeguards and Security.

(1) Ensure the designation and appointment of TOP SECRET control officers and alternates as custodians and notify Headquarters, Office of Safeguards and Security, of the selection and position titles of the designees.

(2) Request the approval of the Headquarters Office of Safeguards and Security for DOE and contractor employees on official Departmental business to hand-carry classified matter to and from foreign countries.

(3) Serve as the Designated Accrediting Authority (DAA) in coordination with the Classified Computer Security Program Manager, for classified information systems under their cognizance to be operated at a Protection Index of five, as defined in DOE M 5639.6A-1. This authority may not be redelegated.

(4) Appoint, in coordination with the Computer Security Program Manager, a senior-level DOE employee as the DAA, for classified information systems under their cognizance to be operated at a Protection Index of three.

(5) Appoint a Computer Security Operations Manager who will also serve as the DAA for classified computer systems under their cognizance to be operated at a Protection Index of zero, one, or two and to oversee classified information systems security programs at DOE and DOE-contractor facilities under their cognizance.

(6) Ensure the Headquarters Operations Division and each DOE Field Element, contractor, or subcontractor under their cognizance appoints a Classified Information Systems Security Site Manager, responsible to their management and to the CSOM for the implementation of Classified Information Systems Security within their organizations.

(7) Through each manager or supervisor responsible for a classified information system, ensure the following:

(a) Appointment of a Classified Computer Systems Security Officer (CSSO), either a DOE or covered contractor employee, for each classified information system at a facility and identification of that individual in the Classified Information Systems Security Plan. An individual may serve as the Classified System Security Officer for one or more classified information systems.

(b) Computer System Security Officer for each classified Information System is aware of and fulfills his/her duties as described in this Order and DOE M 5639.6A-1.

(8) Designate an OPSEC Manager, a CMPC Operations Manager, a TSCM Operations Manager, and a Special Access Program (SAP) Security Coordinator. These managers, for their assigned area(s) of responsibility, shall accomplish the following:

(a) Ensure the implementation of DOE policy and procedures.

(b) Develop and implement local policy and procedures.

(c) Conduct appropriate surveys and self-assessments to ensure effective implementation.

(d) Review the results of surveys and self-assessments for lessons learned and trends analysis.

(9) Ensure facilities included in the Operations Security program develop and maintain Operations Security plans, procedures, and program files to assist in implementing an active program, and approve these plans and procedures, as appropriate.

(10) Ensure issuance of infractions, when required, to DOE and DOE-contractor personnel.

c. Director of Nonproliferation and National Security.

(1) Determines (in coordination with the Director of Central Intelligence for intelligence information) whether sharing classified information with foreign governments will result in a net advantage to the national security of the United States.

(2) Establishes agreements, in coordination with other appropriate agencies, for sharing classified information with foreign governments.

(3) Obtains security assurances for the proposed exchange of classified information with foreign governments.

(4) Implements Chapter V of this Order for establishing nuclear, intelligence, acquisition, operations and support, law enforcement, and emergency operations-related SAPs.

(5) Authorizes specific DOE organizations and covered contractors to create and retain information designated as Protect as Restricted Data (PARD).

d. Director of Energy Intelligence.

(1) Exercises authorities vested in the Secretary by the Director of Central Intelligence in furtherance of the provisions of Executive Order 12958, sections 3.5© and 3.6(e).

(2) Accredits DOE and DOE-contractor Sensitive Compartmented Information Facilities.

(3) Approves access to FII and SCI for DOE and DOE contractor personnel.

(4) Controls use and dissemination of FII and SCI by DOE and DOE contractor personnel.

(5) Functions as the Department's point-of-contact involving activities related to intelligence and counterintelligence, to include oversight of program access to intelligence information provided to, or originated within, DOE. Coordinates with the Office of Security Affairs concerning security issues, to include espionage and the possible or potential compromise of intelligence-related information.

(6) Serves as the DAA for classified information systems that process intelligence information and are located in Sensitive Compartmented Information Facilities.

(7) Establishes, as necessary, policy and procedures, beyond those described in this Order and DOE M 5639.6A-1, for processing classified intelligence information in Sensitive Compartmented Information Facilities, in coordination with the Classified Information System Security Program Manager.

(8) Processes National Security Council matter containing SCI received and dispatched from DOE.

e. Director of Security Affairs.

(1) Acts as the Senior Agency Official responsible for the direction and administration of the Information Security Program.

(2) Exercises authorities vested in the Secretary under Executive Order 12958 and implementing directives, except the following.

(a) The authority in the Executive Order, section 4.4, pertaining to the creation of SAPs.

(b) Authority delegated to the Secretary by the Director of Central Intelligence in the Executive Order, sections 3.5.(c) and 3.6(e).

(3) Advises and assists DOE and DOE contractors in implementing information security programs.

(4) Ensures other Government agencies and foreign governments are informed of any potential compromise of their information.

(5) Through the Director of Safeguards and Security.

(a) Administers and oversees implementation of the Atomic Energy Act of 1954, as amended, for the protection of Restricted Data and Formerly Restricted Data.

(b) Administers and oversees implementation of Executive Order 12958, "Classified National Security Information," pertaining to SAPs, personnel, and physical security requirements for the control and protection of National Security Information.

(c) Designates DOE Information Security Program Managers. These managers shall be DOE employees who are highly knowledgeable in their specialty. They are appointed to manage elements of the Information Security Program and shall be designated as the OPSEC Program Manager, Classified Information Systems Security Program Manager, Classified Matter Protection and Control Program Manager, Technical Surveillance Countermeasures Program Manager, and Special Access Program Security Program Manager (excluding intelligence SAP program security managers). These managers, for their assigned areas of responsibility, shall accomplish the following:

(1) Represents the DOE on national-level committees.

Vertical Line Denotes Change.

(2) Develops policies, standards, and procedures.

(3) Directs safeguards and security technology development efforts as required.

(4) Provides advice and guidance to Information Security Operations Managers at Field Elements in implementing the program.

(5) Oversees the development of information security training courses.

(6) Periodically assesses the effectiveness of the program.

(7) Ensures compliance with security-related reporting requirements of Federal or legislative directives and provides details of unauthorized disclosures to the Information Security Oversight Office.

(d) Ensures the establishment of an Independent Validation and Verification capability to be made available to DOE site and facility managers.

| (e) Ensures the development and implementation of an Information Security training program meeting the requirements of DOE O 470.1.

| (f) Establishes accreditation criteria for classified AIS systems.
|

f. Assistant Secretary for Human Resources and Administration.

| (1) Develops policy and provides oversight for the implementation of the TEMPEST, Protected Distribution System (PDS), Communications Security (COMSEC), and Unclassified Computer Security Programs for the Department.

(2) Assists the Director of Security Affairs, as needed, during the Internal Review Budget | process by ensuring that integrated security systems are planned, designed, and constructed.

(3) Assists the Director of Security Affairs during the conduct of certifications, reviews, surveys, and program reviews of Information Security Programs.

(4) Represents the Department as a member of the National Security Telecommunications Information Systems Security Committee.

(5) Provides advice and assistance in determining solutions to correct any telecommunications vulnerabilities detected by safeguards and security activities.

Vertical Line Denotes Change.

(6) Designates the Headquarters Classified Information System Security Site Manager for classified information systems in Headquarters Elements in the Washington metropolitan area.

(7) Processes all National Security Council matter received and dispatched by DOE, with the exception of matter that contains SCI, or matter submitted by the National Security Council or other Federal agencies to the Office of Declassification for classification review.

(8) Processes all classified matter for the Secretary, Deputy Secretary, and Under Secretary.

(9) Establishes the DAA structure for the Department.

g. Assistant Secretary for Defense Programs.

(1) Implements Chapter V of this Order for establishing defense-related SAPs.

(2) Through the Deputy Assistant Secretary for Facility Transition and Technical Support.

(a) Develops policy and requirements and executes approvals and delegations of authority for controlling access to weapon data according to DOE 5610.2, CONTROL OF WEAPON DATA, of 8-1-80.
(b) For unaccounted-for classified matter or compromised classified information, coordinates the required reporting to the Joint Atomic Information Exchange Group.
(c) Channels all matters containing Restricted Data or Formerly Restricted Data being sent to foreign entities to the Joint Atomic Information Exchange Group (JAIEG) for review prior to release.

h. Director for Nuclear Energy shall implement Chapter V of this Order for establishing nuclear energy-related SAPs.

I. Director Naval Nuclear Propulsion Program shall implement and oversee all policy and practices pertaining to Information Security for activities under the Director's cognizance.

j. Procurement Request Originators (the individuals responsible for initiating a requirement on DOE F 4200.33 or other individual(s) designated by the cognizant Head of Departmental Element) shall bring to the attention of the cognizant contracting officer:

(1) each procurement to which elements of the Contractor Requirements Document apply, and
(2) elements of the Contractor Requirement Document that apply to any subcontract or subaward.

k. Contracting Officers shall, based on advice received from the procurement request originator or other designated individuals, apply pertinent requirements in the Contractor Requirements Document to awards falling within its scope. For awards other than management and operating contracts, this shall be by incorporation or reference using explicit language in a contractual action.

6. CONTACT. Questions concerning this Order should be directed to Technical and Operations Security of the Policy, Standards, and Analysis Division, Office of Safeguards and Security, at 301-903-2528.

BY ORDER OF THE SECRETARY OF ENERGY:

ARCHER L. DURHAM
Assistant Secretary for Human Resources and Administration

TABLE OF CONTENTS

CHAPTER I

PROGRAM MANAGEMENT

1. SECURITY ORGANIZATION. To ensure an effective information security program, the following requirements shall be implemented.

   a. A clear chain of responsibility for information security shall exist within each organization.

   b Qualified personnel and other resources shall be available to implement and maintain the information security program.

   c. Individuals responsible for managing or implementing information security programs shall be provided adequate time and resources to satisfactorily accomplish assigned functions in accordance with applicable directives.

   d. Information security training shall be developed and implemented, as necessary.

   e. Heads of Departmental Elements responsible for programs requiring protection and control of classified and/or sensitive unclassified information shall ensure that plans are established and approved by the cognizant security office prior to initiation of such programs.

   f. Management shall be involved in and supportive of all aspects of information security. This involvement and support shall be demonstrated by regular visits to and inspections of information security operations to ensure that operations meet existing standards and policies.

   g. Management shall ensure that information security is included and documented in protection program planning documents. Site-specific characteristics shall be considered and documented to ensure that information is properly controlled.

2. SECURITY INFRACTIONS. An infraction is any knowing, willful, or negligent action contrary to the requirements of this Order that does not constitute a violation of law or result in the actual compromise or the unauthorized disclosure of classified information. Requirements for handling violations are contained in DOE O 470.1.

   a. Report of Security Infraction. DOE F 5639.3, "Report of Security Incident/Infraction," or a similar form shall be used to document infractions and a copy of the report kept in

Vertical Line Denotes Change.

the employee's official DOE personnel security file. With each occurrence, security practices or procedures shall be reviewed and revised, if necessary, to preclude recurrence.

b. Records of Security Infractions. The safeguards and security organization or officer reporting the security infraction and the cognizant Departmental Element shall maintain records of each infraction.

c. Disciplinary or Corrective Actions.

(1) For DOE employees, disciplinary or corrective action shall be determined by the Heads of Departmental Elements in coordination with the Office of Personnel. Any disciplinary or adverse action involving a DOE employee shall be according to DOE 3750.1, WORK FORCE DISCIPLINE, of 3-23-83.
(2) For contractor employees, disciplinary or corrective action shall be determined by appropriate management officials according to the contractor's personnel policies and procedures.
(3) For military personnel and employees of other Government agencies assigned to DOE or DOE contractors, DOE or its contractors shall take corrective action and submit a report of infraction to the military organization or Government agency to which the employee is permanently assigned for whatever disciplinary action that the cognizant agency or organization deems necessary.

3. UNACCOUNTED FOR MATTER AND COMPROMISE OF CLASSIFIED INFORMATION. Loss, compromise, or unauthorized disclosure of information and unaccounted-for matter shall be handled according to DOE O 470.1 and DOE M 471.2-1. In addition, the following requirements apply.

a. Discovery. Any person who determines that classified matter has been or may have been lost or compromised or is otherwise unaccounted-for shall take immediate action to preclude any further or potential compromises and immediately report this information to the facility security officer.

b. Inspection. Upon determining or learning that classified matter may be lost or unaccounted-for, an inspection of the area where the matter was stored, handled, or processed shall be conducted. Custodians providing support to the holder must be queried. When applicable, the accountability records shall be audited for evidence of destruction, transmission, or other disposition. The inspection and query process shall be completed within 48 hours.

c. Inquiry. When inspection efforts fail to reconcile unaccounted for matter, and for all potential compromises, the appointed Inquiry Official shall initiate an inquiry. The DOE safeguards and security organization shall advise the Office of Safeguards and Security of the initiation of an inquiry.

d. Damage Assessments.

(1) Purpose. Damage assessments to assess potential damage to national security are required by 32 CFR, Chapter XX, Part 2000, "National Security Information," Section 2001.47 "Loss or Possible Compromise." Damage assessments are used by responsible managers to determine future courses of action within the program and by security personnel to evaluate possible countermeasures and cover actions to limit potential damage.

(2) When Required. When the inquiries disclose evidence that information may have been compromised and the compromise can reasonably be expected to cause damage to the national security, a damage assessment shall be conducted. Compromises may occur through espionage, unauthorized disclosures to the press or other members of the public, loss of classified information, unaccounted for classified matter, or through various other circumstances. Both circumstances of the loss and sensitivity of the information must be considered in determining when a damage assessment is required.

e. Notification to Information Security Oversight Office. On receiving written confirmation from a Departmental Element of an unauthorized disclosure of, or access to, National Security Information by a DOE employee, DOE contractor, or consultant, the Office of Safeguards and Security shall notify the Information Security Oversight Office of the details. Such notification shall be given immediately when the disclosure results from systematic problems. Otherwise, semiannual reports of unauthorized disclosures shall be made.

f. Records Retention. Records of all actions pertaining to unaccounted for/compromised matter or compromises of classified information must be maintained by the facility security officer and the cognizant Departmental Element safeguards and security organization. Records shall be destroyed 5 years after the close of all associated actions. These records will not be sent to Federal Records Centers.

CHAPTER II

OPERATIONS SECURITY PROGRAM

1. OBJECTIVES. The objective of the OPSEC Program is to help ensure that sensitive information is protected from compromise and secured against unauthorized disclosure. The program is structured to provide management with the necessary information required for sound risk management decisions concerning the protection of sensitive information. OPSEC techniques and measures shall be utilized throughout the Department to achieve this objective. The counterimagery program shall be an integral part of the OPSEC Program pertaining to imagery-susceptible, sensitive activities.

2. APPLICABILITY. This section applies only to facilities possessing sensitive information, whether classified or unclassified, for which adequate OPSEC is required to detect and deter efforts to illegally gain access to that information. As determined by the cognizant Department authority, the amount and sensitivity of information, balanced against its vulnerability and attractiveness, will be considered when calculating the level of OPSEC activities required.

3. REQUIREMENTS. To meet the objectives of the OPSEC Program, the organization shall accomplish the following.

   a. Develop and maintain OPSEC plans, procedures, and program files. OPSEC plans will include, at a minimum, goals, milestones, and, where applicable, an annex describing actions to identify and counter imagery collection from air- and space-borne platforms, OPSEC plans shall be reviewed and updated as required on an annual basis; a memorandum reflecting completion of this action will be placed in the OPSEC files.

   b. Establish a sufficient number of OPSEC working groups to perform the necessary management and support functions required for an effective OPSEC program, to include OPSEC education and awareness. Working groups shall develop and set priorities for their OPSEC program objectives consistent with approved plans and policies, meet on a regular basis, and maintain meeting records, a copy of which shall be held by the responsible OPSEC Manager.

   c. Prepare a threat statement that describes the local OPSEC threat and develop a Critical Sensitive Information List (CSIL) and supporting Essential Elements of Friendly Information (EEFI), which will be appropriately classified, set according to priorities, and disseminated to cognizant managers for review, comment, and action based on the adequacy of countermeasures in place at each site. The threat statement and CSIL/EEFI will be reviewed by the cognizant OPSEC Working Group and senior Headquarters' program management and updated at least annually. The results of such reviews will be recorded in OPSEC managers' files.

   d. Conduct OPSEC assessments of all facilities having Category I Special Nuclear Material, Top Secret matter, or a special access program and falling within their

purview. OPSEC assessments will be conducted at other facilities involved in the creating, handling, storing, processing, or transmission of sensitive information, whether classified or unclassified, as deemed necessary by the cognizant Department authority. A copy of these assessments, to include observations, recommendations, and actions taken, will be provided to the Office of Safeguards and Security for historical purposes.

(1) Either the programmatic or facility approach may be used to conduct the OPSEC assessment. If the facility approach is used, all activities at the facility will be included in the assessment. If the programmatic approach is used, all activities within the individual program will be included in the assessment. Priority of effort for the assessment should be based on the Critical and Sensitive Information List, threat assessment, risk management concepts, and direction from management.

(2) Effective immediately, facilities having Category I Special Nuclear Material, Top Secret matter, or a special access program will conduct an OPSEC assessment at least every 3 years, or sooner if the facility environment changes significantly. If the programmatic approach is used and more than one major program is located at the facility, a schedule will be developed and implemented that provides for the conduct of a minimum of one programmatic assessment annually. Major programs will be identified by the local Working Group.

e. Conduct an OPSEC review of all sensitive activities and facilities whenever:

(1) new construction is planned for a facility that will process or store classified or sensitive information or matter;

(2) new sensitive activities are initiated or significant changes occur to existing programs; or

(3) a sensitive program or activity has not been the subject of an OPSEC assessment or OPSEC review for the preceding 2 years.

f. Conduct OPSEC liaison with other Field Elements and local agencies. Advise the Office of Safeguards and Security of broadly based OPSEC initiatives involving these organizations.

g. Analyze the results of OPSEC assessments and, in consonance with risk management, develop and implement countermeasures, as appropriate.

h. Conduct an initial review of all ongoing sensitive activities to identify those susceptible to imaging exploitation.

i. Report annually, on November 1st, to the Office of Safeguards and Security and applicable program officials on the status of the OPSEC Program for the preceding fiscal year.

j. Ensure that OPSEC responsibilities for Work For Others programs to the extent specified in the basic contract or Memorandum of Understanding are fulfilled. Primary responsibility for OPSEC activity within any Work for Others program rests with the Work for Others Program Manager. Any OPSEC interaction between the Work for Others program and the local OPSEC program will be as mutually agreed between the Work for Others Program Manager and the cognizant OPSEC Manager.

CHAPTER III

CLASSIFIED INFORMATION SYSTEMS SECURITY

1. OBJECTIVE. To ensure classified information and unclassified information processed on classified information systems are protected against unauthorized disclosure or compromise.

2. APPLICABILITY. Systems requiring this protection include but are not limited to the following.

   a. Mainframe classified information systems, word processors, microprocessors, personal computers, programmable controllers, automated office support systems, memory typewriters, and other stand-alone or special systems that process, store, transfer, or provide access to classified information, including those classified information systems that also process, store, transfer, or provide concurrent access to both classified and unclassified information.

   b. Special purpose computers that perform classified functions and/or contain classified data, such as numerically controlled machines, smart switches, single-task preprogrammed controllers, programmable facsimile devices, automated testers, and digital-to-analog and analog-to-digital converters.

   c. Networks wherein classified information is processed, stored, transferred, or accessed in one or more components of the network.

3. REQUIREMENTS. This Order and DOE M 5639.6A-1 shall be used with other DOE directives to provide a comprehensive protection program for classified Information Systems. These directives establish minimum requirements for the design, procurement, and implementation of information systems that process, store, transfer, or provide access to classified information. Unclassified information processed on classified information systems is subject to the requirements of this Order and DOE M 5639.6A-1, unless processed under period processing procedures. If processing of only unclassified information takes place during period processing, the information processed is subject to DOE 1360.2B, UNCLASSIFIED COMPUTER SECURITY PROGRAM, of 1-7-93.

   a. Protection of Classified Information and Resources. The Classified Information Systems Security Program shall be implemented to ensure the following.

      (1) The integrity of the information on the classified information system is preserved.

      (2) Information processed on the classified information system is protected from unauthorized access, alteration, modification, disclosure, transmission, or destruction.

(3) The classified information system's resources provide an appropriate level of protection against denial of service, subversion of security measures, or improper use.

(4) The classified information system's resources are protected from damage, destruction, and unauthorized modification.

b. Protection Measures. All reasonable measures shall be used to protect information systems that process, store, transfer, or provide access to classified information. These measures include but are not limited to the following.

(1) Measures related to personnel security, physical security, telecommunications security, administrative security, technical security, and hardware and software security shall be used to protect information on the classified information system to result in an acceptable level of risk against loss, improper use, compromise, or unauthorized alteration or modification of classified information.

(2) Acquisitions or other procurement actions to obtain information system equipment or related contractual services (as defined in DOE 1360.1B) that will be used to process, store, transfer, or provide access to classified information shall be:

(a) evaluated by the Classified Information System Security Site Manager to ensure that appropriate security technology is being specified and
(b) integrated into the Information Resources Management Long Range Plan according to DOE 1360.1B.

(3) Information Systems used to process, store, transfer, or provide access to classified information shall meet the following requirements.

(a) Accredited by a DAA to be operated:

(1) in a particular mode of operation as defined in DOE M 5639.6A-1;

(2) with a prescribed set of personnel, administrative, operational, physical, telecommunications, hardware, software, and technical requirements;

(3) under a stated operational concept; and

(4) with identified interconnections to other information systems.

(b) Reaccredited by a DAA at least once every 3 years except classified information systems processing SCI.

(c) Covered by a continuity of operations decision or a plan (see DOE M 5639.6A-1, Chapter I, paragraph 9).

(d) Operated under the oversight of a designated Departmental or covered contractor manager or supervisor.

(e) Accessed only by personnel who have:

(1) received training in their security responsibilities;

(2) a proper level of access authorization and need-to-know; and

(3) acknowledged in writing their responsibilities to protect information on classified information systems.

c. Information Systems Containing Intelligence Information. The requirements of this Order and DOE M 5639.6A-1 apply to classified information systems that process classified intelligence information within a Sensitive Compartmented Information Facility. However, these requirements may not fully represent the protection requirements for processing intelligence information; further requirements may be established by directives of the intelligence community.

d. Baseline for Protection. This Order and DOE M 5639.6A-1 provide a uniform baseline for the protection of classified information systems. Each DAA, as described in this Order and DOE M 5639.6A-1, is responsible for ensuring that the security requirements of this Order and DOE M 5639.6A-1 are met for each classified information system that he/she accredits.

CHAPTER IV

PROTECTION AND CONTROL OF CLASSIFIED MATTER

1. OBJECTIVES. To establish a system of procedures, facilities, and equipment to protect and control classified matter that is being generated, received, transmitted, used, stored, reproduced, or destroyed.

   a. To establish a system of procedures to provide an adequate audit trail for all accountable classified matter.

   b. To establish a control system geared to providing controls based on classification category (Restricted Data, Formerly Restricted Data, or National Security Information) or special handling instructions or caveats.

2. APPLICABILITY. This section applies only to facilities that have classified matter.

3. REQUIREMENTS.

   a. Classification level and category shall be used in determining the degree of protection and control required to prevent unauthorized access to classified matter.

   b. Controls shall be established to detect and deter unauthorized access to classified matter.

   c. Custodians and authorized users of classified matter are responsible for the protection and control of such matter.

   d. Buildings and rooms containing classified matter shall be afforded the security measures necessary to prevent unauthorized persons from gaining access to classified matter, specifically to include security measures to prevent unauthorized visual and/or aural access.

| e. Classified information and sensitive unclassified information shall be disclosed to contractors pursuant to an authorized and legitimate U.S. government requirement only.

   f. Detailed requirements for marking, accountability and control systems, reproduction, receipt, transmission, and destruction are contained in DOE M 471.2-1, MANUAL FOR CLASSIFIED MATTER PROTECTION AND CONTROL.

   g. Emergency Procedures. Procedures shall be developed for safeguarding classified matter in emergency situations.

Vertical Line Denotes Change.

CHAPTER V

SPECIAL ACCESS PROGRAMS

1. OBJECTIVES. To establish requirements for and limit the types of SAPs authorized for use within the Department. Authorized SAPs are categorized as acquisition, operations and support, and intelligence SAPs. Terms and activities such as Limited Access Program, Controlled Access Program, and Limited Distribution Programs are not authorized.

2. APPLICABILITY. This section applies only to facilities that provide oversight for, operate, or host special access programs.

3. REQUIREMENTS. All DOE-originated SAPs must be approved by the Secretary, with the recommendation of the Deputy Secretary, who serves as the Chairperson of the Special Access Programs Oversight Committee, which oversees the development of policy and procedures for SAPs.

   a. Security policy and procedures for DOE SAPs are developed by the Office of Safeguards and Security, in coordination with the appropriate Program Office.

   b. DOE and Non-DOE (Work-For-Others) SAPs, with the exception of intelligence SAPs, are registered through the established Facility Data and Approval Record process (see DOE O 470.1). The Facility Data and Approval Record will be classified in accordance with "Classification Guide for Safeguards and Security Information" (CG-SS-3), Chapter II. DOE SAPs are registered with the SAP Security Program Manager. Intelligence SAPs are registered with the Office of Energy Intelligence.

   c. SAP facilities and activities will be surveyed according to DOE O 470.1 by the cognizant Operations Office and/or Office of Safeguards and Security, in coordination with the appropriate Program Office and/or sponsor. Intelligence SAPs are inspected by the Office of Energy Intelligence.

   d. Protection program planning documents, including security plans and standard operating procedures, must comply with established SAP policies.

   e. Any possible or probable loss, compromise, or unauthorized disclosure of SAP information must be immediately reported to the appropriate Program Office and the Director of Safeguards and Security, according to established Departmental polices.

CONTRACTOR REQUIREMENTS DOCUMENT

INFORMATION SECURITY PROGRAM

1. This contractor requirement document is issued to aid procurement request initiators to identify requirements that are to be incorporated into contracts by contracting officers. The following requirements are based on statutes, Executive Orders, and national directives that are designed to deter unauthorized access to classified information and sensitive unclassified information.

The contractor is responsible for protecting classified and sensitive unclassified information and shall ensure the following:

a. That individuals protect classified information and sensitive unclassified information to which they have access or custody.

b. That classified information is not released to the public until it has been formally and officially declassified by an appropriate declassification authority and its release is otherwise permitted by applicable law or regulation. Likewise, no sensitive unclassified information shall be released without review for applicable release restrictions.

c. That protection systems that require higher degrees of protection be established for each higher classification level (Confidential, Secret, Top Secret).

d. That provisions of this CRD flow down to all subcontractors with responsibilities for protecting classified and sensitive unclassified information.

2. General Requirements. Access to classified information shall be granted only to persons who possess the appropriate need-to-know and access authorization in accordance with applicable DOE directives and the Manual for Personnel Security Activities when issued. Supervisors or other responsible officials who are knowledgeable of the classified information and the responsibilities of the individual may determine need-to-know. The individual disseminating classified information is responsible for ensuring that the recipient of the information has the appropriate access authorization and need-to-know. Additionally, the contractor shall accomplish the following:

a. Obtain a DOE facility clearance before a facility is eligible for access to classified information.

b. Ensure access to sensitive unclassified information is granted only to persons who possess the appropriate need-to-know. The individual disseminating sensitive unclassified information is responsible for determining the recipient's need-to-know. Access to Naval

Nuclear Propulsion Information shall only be granted to U.S. citizens who have a need-to-know.

c. Ensure that owners of data are responsible for determining the sensitivity of information before it is used, processed, or stored on information systems and for ensuring the system is accredited for the information to be used in it.

d. Ensure classified and unclassified Naval Nuclear Propulsion Information is protected in accordance with Naval Sea Systems Command Instruction C5511.32B, dated 12-22-93. Naval Nuclear Propulsion Information shall be protected pursuant to export control requirements and statute. Questions regarding Naval Nuclear Propulsion Information shall be directed to the Deputy Assistant Secretary for Naval Reactors.

3. Classified Information Systems (ISS) Security requirements for classified information systems contained in this CRD and DOE M 5639.6A-1 shall be implemented as follows.

a. Existing accredited classified information systems shall remain accredited until reaccreditation is required, either because of expiration of accreditation (3 years) or because of significant changes in the security requirements of the information system. Reaccreditation shall be accomplished under the requirements of this CRD and DOE M 5639.6A-1. These systems must meet the requirements of this CRD and DOE M 5639.6A-1 no later than July 15, 1997.

b. Classified information systems in the process of accreditation on July 15, 1995 may be accredited; however, the requirements of this CRD and DOE M 5639.6A-1 must be met by these systems no later than January 15, 1996.

c. New classified information systems that are under development, and that have not begun certification and security performance testing, shall meet the requirements of this CRD and DOE M 5639.6A-1.

4. Supplementary Directives. The following Manuals supplement this CRD and contain non-discretionary, mandatory Information Security Program requirements, standards, and procedures.

a. DOE M 471.2-1, CLASSIFIED MATTER PROTECTION AND CONTROL.

b. DOE M 5639.6A-1, MANUAL OF SECURITY REQUIREMENTS FOR THE CLASSIFIED AUTOMATED INFORMATION SYSTEM SECURITY PROGRAM.

c. DOE "Technical Surveillance Countermeasures Procedural Manual" (classified).

5. Program Management. To ensure an effective information security program, the contractor shall accomplish the following:

a. Maintain a clear chain of responsibility for information security within each organization.

b. Ensure that qualified personnel and other resources are available to implement and maintain the information security program.

c. Provide adequate time and resources to individuals responsible for managing or implementing information security programs to satisfactorily accomplish assigned functions.

d. Ensure information security training is developed and implemented, as necessary.

| e. Ensure programs requiring protection and control of classified and/or sensitive unclassified information have plans established and approved by the cognizant security office prior to initiation of such programs.

f. Have programs that are unclassified, but potentially sensitive, receive a timely review by the appropriate OPSEC Working Group. Once a determination has been made that sensitive information is involved, the identity of the information shall be forwarded to the cognizant security office.

g. Ensure management is involved in and supports of all aspects of information security. This involvement and support shall be demonstrated by regular visits to and inspections of information security operations to ensure that operations meet existing standards and policies.

h. Ensure that information security is included and documented in protection program planning documents. Site-specific characteristics shall be considered and documented to ensure that information is properly controlled.

6. Security Infractions.

a. Use DOE F 5639.3, "Report of Security Incident/Infraction," or a similar form to document infractions and forward a copy of the report to DOE. With each occurrence, security practices or procedures shall be reviewed and revised, if necessary, to preclude recurrence.

b. Ensure the safeguards and security organization or officer reporting the security infraction maintains records of each infraction.

c. Administer disciplinary or corrective actions as follows.

(1) For contractor employees, disciplinary or corrective action shall be determined by appropriate management officials according to the contractor's personnel policies and procedures.

(2) For military personnel and employees of other Government agencies assigned to DOE contractors, DOE or its contractors shall take corrective action and submit a report of infraction to the military organization or Government agency to which the employee is permanently assigned for whatever disciplinary action that the cognizant agency or organization deems necessary.

7. Unaccounted For Matter and Compromise of Classified Information. Loss, compromise, or unauthorized disclosure of information and unaccounted-for matter shall be handled according to DOE O 470.1 and DOE M 471.2-1. In addition, the following requirements shall apply.

a. Any person who determines that classified matter has been or may have been lost or compromised or is otherwise unaccounted-for shall take immediate action to preclude any further or potential compromises and immediately report this information to the facility security officer.

b. Upon determining or learning that classified matter may be lost or unaccounted-for, an inspection shall be completed within 48 hours.

c. When inspection efforts fail to reconcile unaccounted for matter, and for all potential compromises, the appointed Inquiry Official shall initiate an inquiry and ensure notification to DOE.

d. Records Retention. Records of all actions pertaining to unaccounted for/compromised matter or compromises of classified information must be maintained by the facility security officer. Records shall be destroyed 5 years after the close of all associated actions. These records will not be sent to Federal Records Centers.

8. Operations Security. To meet the objectives of the Operations Security Program, the organization shall accomplish the following.

a. Develop and maintain Operations Security plans, procedures, and program files. Operations Security plans will include, at a minimum, goals, milestones, and, where applicable, an annex describing actions to identify and counter imagery collection from air- and space-borne platforms. Operations Security plans shall be reviewed and updated as required on an annual basis; a memorandum reflecting completion of this action will be placed in the Operations Security files.

b. Establish a sufficient number of Operations Security working groups to perform the necessary management and support functions required for an effective Operations Security program, to include Operations Security education and awareness. Working groups shall develop and set priorities for their Operations Security program objectives consistent with approved plans and policies, meet on a regular basis, and maintain meeting records, a copy of which shall be held by the responsible Operations Security Manager.

c. Prepare a threat statement that describes the local Operations Security threat and develop a Critical Sensitive Information List (CSIL) and supporting Essential Elements of Friendly Information (EEFI), which will be appropriately classified, set according to priorities, and disseminated to cognizant managers for review, comment, and action based on the adequacy of countermeasures in place at each site. The threat statement and CSIL/EEFI will be reviewed by the cognizant Operations Security Working Group and senior Headquarters' program management and updated at least annually. The results of such reviews will be recorded in Operations Security managers' files.

d. Conduct Operations Security assessments of all facilities having Category I Special Nuclear Material, Top Secret matter, or a special access program falling within their purview. OPSEC assessments will be conducted at other facilities involved in creating, handling, storing, processing, or transmitting sensitive information, whether classified or unclassified, as deemed necessary by the cognizant Department authority. A copy of these assessments, to include observations, recommendations, and actions taken, will be provided to the Office of Safeguards and Security for historical purposes.

(1) Either the programmatic or facility approach may be used to conduct the OPSEC assessment. If the facility approach is used, all activities at the facility will be included in the assessment. If the programmatic approach is used, all activities within the individual program will be included in the assessment. Priority of effort for the assessment should be based on the Critical and Sensitive Information List, threat assessment, risk management concepts, and direction from management.

(2) Effective immediately, facilities having Category I Special Nuclear Material, Top Secret matter, or a special access program will conduct an OPSEC assessment at least every 3 years, or sooner if the facility environment changes significantly. If the programmatic approach is used and there is more than one major program located at the facility, a schedule will be developed and implemented that provides for the conduct of a minimum of one programmatic assessment annually. Major programs will be identified by the local Working Group.

e. Conduct an OPSEC review of all sensitive activities and facilities whenever:

(1) new construction is planned for a facility that will process or store classified or sensitive information or matter;

(2) new sensitive activities are initiated or significant changes occur to existing programs; or

(3) a sensitive program or activity has not been the subject of an OPSEC assessment or OPSEC review for the proceeding 2 years.

f. Conduct Operations Security liaison with local agencies. Advise the Office of Safeguards and Security of broadly based Operations Security initiatives involving these organizations.

g. Analyze the results of Operations Security assessments and, in consonance with risk management, develop and implement countermeasures, as appropriate.

h. Conduct an initial review of all ongoing sensitive activities to identify those susceptible to imaging exploitation.

i. Report annually, on October 1st, to the cognizant DOE field office Safeguards and Security Director on the status of Operations Security Program for the preceding fiscal year.

j. Ensure that Operations Security responsibilities for Work For Others programs are fulfilled to the extent specified in the basic contract or Memorandum of Understanding.

9. Classified Information Systems Security. The Classified Information Systems Security Program shall be implemented to ensure the following.

a. The integrity of the information on the classified information system is preserved.

b. Information processed on the classified information system is protected from unauthorized access, alteration, modification, disclosure, transmission, or destruction.

c. The classified information system's resources provide an appropriate level of protection against denial of service, subversion of security measures, or improper use.

d. The classified information system's resources are protected from damage, destruction, and unauthorized modification.

e. All reasonable measures shall be used to protect information systems that process, store, transfer, or provide access to classified information. These measures include but are not limited to the following.

(1) Measures related to personnel security, physical security, telecommunications security, administrative security, technical security, and hardware and software security shall be used to protect information on the classified information system to result in an acceptable level of risk against loss, improper use, compromise, or unauthorized alteration or modification of classified information.

(2) Acquisitions or other procurement actions to obtain information system equipment or related contractual services that will be used to process, store, transfer, or provide access to classified information shall be:

(a) evaluated by the Classified Information System Security Site Manager to ensure that appropriate security technology is being specified and

(b) integrated into the Information Resources Management Long Range Plan.

(3) Information Systems used to process, store, transfer, or provide access to classified information shall meet the following requirements.

(a) Accredited by a DAA to be operated:

1 in a particular mode of operation as defined in DOE M 5639.6A-1;

2 with a prescribed set of personnel, administrative, operational, physical, telecommunications, hardware, software, and technical requirements;

3 under a stated operational concept; and

4 with identified interconnections to other information systems.

(b) Reaccredited by a DAA at least once every 3 years except classified information systems processing SCI.

(c) Covered by a continuity of operations decision or a plan (see Chapter I, paragraph 9, DOE M 5639.6A-1).

(d) Operated under the oversight of a designated Departmental or covered contractor manager or supervisor.

(e) Accessed only by personnel who have:

1 received training in their security responsibilities;

2 a proper level of access authorization and need-to-know; and

3 acknowledged in writing their responsibilities to protect information on classified information systems.

f. Information Systems Containing Intelligence Information. The requirements of this CRD and DOE M 5639.6A-1 apply to classified information systems that process classified intelligence information within a SCIF. However, these requirements may not fully represent the protection requirements for processing intelligence information; further requirements may be established by directives of the intelligence community.

g. Baseline for Protection. This CRD and DOE M 5639.6A-1 provide a uniform baseline for the protection of classified information systems. Each Designated Accrediting Authority, as described in this CRD and DOE M 5639.6A-1, is responsible for ensuring that the security requirements are met for each classified information system accredited.

10. Protection and Control of Classified Matter. The contractor will establish a system of procedures, facilities, and equipment to protect and control classified matter that is being generated, received, transmitted, used, stored, reproduced, or destroyed. Note: This section only applies only to facilities with have classified matter. The following provisions shall apply.

a. Classification level and category shall be used in determining the degree of protection and control required to prevent unauthorized access to classified matter.

b. Controls shall be established to detect and deter unauthorized access to classified matter.

c. Custodians and authorized users of classified matter are responsible for the protection and control of such matter.

d. Buildings and rooms containing classified matter shall be afforded the security measures necessary to prevent unauthorized persons from gaining access to classified matter, specifically to include security measures to prevent unauthorized visual and/or aural access.

| e. Classified information and sensitive unclassified information shall be disclosed to contractors pursuant to an authorized and legitimate U.S. government requirement only.

f. Detailed requirements for Classified Matter Protection and Control will be implemented as mandated in DOE M 471.2-1.

g. Emergency Procedures. Procedures shall be developed for safeguarding classified matter in emergency situations.

11. Special Access Programs. Contractors will notify the local DOE SAP Security Coordinator prior to acceptance of all non-DOE SAPs.

a. Contractors shall ensure that protection program planning documents, including security plans and standard operating procedures, comply with established SAP policies.

b. Any possible or probable loss, compromise, or unauthorized disclosure of SAP information must be immediately reported to the appropriate Program Office and the Director of Safeguards and Security, according to established Departmental policies.