SUBJECT: SAFEGUARDS AND SECURITY PROGRAM

1. PURPOSE. To establish the policy and responsibilities for the Department of Energy (DOE) Safeguards and Security Program.

2. CANCELLATION. DOE 5630.11A, SAFEGUARDS AND SECURITY PROGRAM, of 12-7-92.

3. APPLICATION TO CONTRACTS. Except as excluded in paragraph 4, the provisions of this Order apply to all Departmental Elements and covered contractors performing work for the Department as provided by law and/or contract. A covered contractor is a seller of supplies or services involving access to and protection of classified information, nuclear materials, or other safeguards and security interests.

4. EXCLUSIONS. DOE facilities and activities subject to regulation by the Nuclear Regulatory Commission (NRC) are exempt from the requirements of this Order. Office of Civilian Radioactive Waste Management personnel and activities not directly associated with the NRC licensed facilities, and thus not covered by the NRC directives, are subject to the provisions of this Order.

5. REFERENCES. See Attachment 1.

6. DEFINITIONS. Definitions of terms commonly used in the Safeguards and Security Program are provided in the "Safeguards and Security Definitions Guide" which is maintained and distributed by the Office of Safeguards and Security.

7. POLICY.

   a. DOE interests shall be protected against a range of threats which include unauthorized access; theft or diversion of nuclear weapons, weapons components, or special nuclear material; sabotage; espionage; loss or theft of classified matter or Government property; and other hostile acts which may cause unacceptable adverse impacts on national security or on the health and safety of DOE and contractor employees, the public, or the environment.

   b. Design Basis Threat Policy, issued by the Director of Security Affairs, shall be utilized in the design and implementation of protection programs.

   c. Levels of protection appropriate to particular security interests shall be provided in a graded manner in accordance with the potential risks.

   d. Protection levels shall be comparable in effectiveness to other federally regulated programs with similar security interests, such as the Nuclear Regulatory Commission and the Department of Defense, when such levels are consistent with DOE protective needs, and national security interests.

   e. Deviations from the requirements of Safeguards and Security directives are only permissible with the written approval of the responsible officials according to this Order. Variances, waivers, and exceptions to Safeguards and Security directive requirements may be granted on a case-by-case basis.

   f. Deviations from the requirements of Safeguards and Security directives relating to Sensitive Compartmented Information Facilities and other intelligence facilities will be coordinated with the Director of Energy Intelligence and the Office of Safeguards and Security.

8. RESPONSIBILITIES AND AUTHORITIES.

   a. The Secretary has overall responsibility and authority for programs and takes necessary management actions, through the Under Secretary, to ensure that the Department's safeguards and security

interests are effectively protected.

b. The Under Secretary provides management direction and coordination in the development, implementation, and oversight of the comprehensive Departmental Safeguards and Security Program.

c. Secretarial Officers have primary responsibility to ensure that safeguards and security interests under their jurisdiction are protected in accordance with Departmental requirements. Secretarial Officers, as appropriate, shall:

(1) Provide program and project direction consistent with the safeguards and security directives and safeguards and security policy requirements.

(a) Provide clear and explicit delegations of authority and responsibilities for Safeguards and Security Program implementation and oversight.

(b) For interests over which they have programmatic responsibility:

1 Assure the development of Site Safeguards and Security Plans in coordination with cognizant DOE Field Elements and the Director of Security Affairs.

2 Coordinate within Headquarters Elements the review and comment process for proposed Site Safeguards and Security Plans and verify Site Safeguards and Security Plans.

3 Approve safeguards and security plans.

(c) Ensure that budget proposals for their assigned functions provide adequate safeguards and security resources.

(d) Implement a security program consistent with the Headquarters Security Plan for Washington, D.C. area facilities and programs.

(e) Ensure personnel supporting their assigned functions receive training in accordance with DOE 5630.15, SAFEGUARDS AND SECURITY TRAINING PROGRAM, of 8-21-92.

(f) Coordinate requests for exceptions to Safeguards and Security directives requirements for facilities over which they have programmatic responsibility according to paragraph 9g.

(g) Assure the procurement request packages, for each procurement requiring the application of this Order, include:

1 Identification of the Order and the specific requirements or paragraphs with which a contractor or other awardee is to comply.

2 Requirements for the flowdown of provisions to any subcontract or subaward.

(2) In coordination with the Director of Security Affairs, take action to ensure adequate protection is afforded safeguards and security interests, including curtailing or suspending operations when continuation of such operations would result in an unacceptable risk to national security or the health and safety of employees or the public.

(3) Participate in the development and review of policy and standards for safeguards and security interests associated with the programs under their cognizance.

(4) Obtain Office of Security Affairs guidance regarding safeguards and security requirements and Director of Security Affairs technical support and justification of construction or

alteration projects through the line-item-construction-project process and the crosscut budget process; obtain Director of Security Affairs concurrence of Site Safeguards and Security Plans; and obtain the Office of Field Management support and guidance on the policy and procedures for the administration of the planning, design, and construction or alteration of facilities having a security interest.

(5) Identify research and development needs to the Office of Safeguards and Security for possible incorporation into the safeguards and security research and development program.

(6) Upon assuming such positions, take action to review and determine the status of safeguards and security throughout their program area of responsibility. Upon completion of the review, and in any case within 15 calendar days of assuming the position, the individual will advise the Under Secretary in writing of the results, with a copy sent to the Director of Security Affairs. The communication will include a statement that the review has been completed and will identify any significant deficiencies noted. As appropriate, actions being taken or planned to correct deficiencies should be included.

(7) Report annually, on 12-1, to the Director of Security Affairs on the status of safeguards and security for interests under their respective program jurisdictions.

d. Director of Nonproliferation and Energy Intelligence, in addition to the duties outlined in subparagraphs c(1)-(5), through the Director of Security Affairs provides management direction and coordination in the development, implementation, and oversight of the policy for a comprehensive Departmental Safeguards and Security Program. The Director of Security Affairs, shall:

(1) Establish safeguards and security policies, standards, guidance, and requirements for DOE operations, including design basis threat guidance, for use in designing and implementing DOE protection programs.

(2) Provide advice and assistance concerning safeguards and security programs to line organizations, and coordinate with appropriate Departmental organizations to correct safeguards and security deficiencies, including those which have a programmatic or budgetary impact.

(3) Serve as concurring official for all Site Safeguards and Security Plans.

(4) Establish and maintain the DOE Classification Program and ensure consistency between classification and safeguards and security policies.

(5) Serve as the DOE central point for coordination and liaison with other agencies and groups in the development and execution of an effective Departmental Safeguards and Security Program. This includes coordination with Heads of Departmental Elements in resolution of safeguards and security issues applicable to DOE operations and review of proposed statutes, regulations, standards, and requirements for their application to and potential impact on DOE activities.

(6) Provide a priority listing of safeguards and security corrective actions and upgrade projects to Program Offices, selected Secretarial Officers, and the Assistant Secretary for Human Resources and Administration.

(7) Coordinate with the appropriate Program Offices in the recommended curtailment or suspension of operations at DOE facilities when continuation of such operations would result in an unacceptable risk to national security or the health and safety of employees or the public. Decertify any facility where the level of the facility's safeguards and security program affords significant vulnerability, unacceptable risk, or does not provide adequate protection and approve removal

from the Master Facility Register. Recertify facilities when satisfactory conditions exist. Notify other agencies with concurrent security interests of such action.

(8) Provide review and advice to Program Offices on their safeguards and security requirements and budgets before Departmental approval. Differences identified through the review process will be resolved during the Department's budgeting process (or equivalent process for reprogramming actions).

(9) Review and approve or disapprove exceptions to Safeguards and Security directives requirements, after consideration of Director of Safeguards and Security recommendations, according to paragraph 9g.

(10) Consolidate and coordinate the annual report to the Secretary on the status of safeguards and security.

e. Director of Safeguards and Security shall:

(1) Serve as Office of Security Affairs focal point for safeguards and security matters.

(2) Formulate policies, procedures, and plans to assure effective and efficient protection of nuclear materials, classified matter, property and DOE facilities, and control and accountability of nuclear materials, including design basis threat statements, standards, requirements, and guidelines. Ensure policies, procedures and plans adequately set forth Departmental responsibilities for law enforcement activities. Review, on an as-needed basis, but at least annually, Departmental policies and requirements to assure that protection afforded DOE security interests is comparable to that required by other Government agencies with similar security interests.

(a) Develop and approve policy and requirements for the Headquarters Security Program.

(b) Provide, as required, assistance to Secretarial Officers and Heads of Field Elements in the implementation of safeguards and security requirements.

(c) Act as the Departmental focal point for the collection, retention, evaluation, and dissemination of information having safeguards and security significance, including threat assessment and protection systems data.

(d) Develop policies for the reporting of violations, losses, and management of incidents of security concern.

(e) Maintain a centralized automated data base system for monitoring requested and approved deviations to DOE Safeguards and Security directives.

(f) Recommend approval or disapproval of deviations according to paragraph 9g.

(3) Direct and coordinate the DOE Personnel Security Program.

(4) Represent the Department in the law enforcement community; provide focus for interagency matters pertaining to safeguards and security, including wartime protection planning; and provide liaison with the NRC, the Federal Bureau of Investigation, Department of Defense, and other Federal law enforcement and security agencies.

(5) Recommend to the Director of Security Affairs the decertification and removal from the Master Facility Register of any facility whose safeguards and security program is unacceptable to meet minimum levels of safeguards and security protection and associated risk, until such condition is rectified.

(6) Identify needs for research and development to support safeguards and security programs and initiate appropriate actions and direct the safeguards and security research and development program which supports user needs and policy objectives.

(7) Provide program management and oversight of the Safeguards and Security Central Training Academy and New Brunswick Laboratory.

(8) Provide an annual prioritized listing of recommended safeguards and security line-item-construction projects for Departmentwide programs and facilities to Program Offices and the Assistant Secretary for Human Resources and Administration; and participate in ongoing staffing actions to define and refine priorities for accomplishing such projects and programs through validation of specific projects.

(9) Provide advice and assistance to all Headquarters Elements on safeguards and security matters.

(10) Develop, issue, and maintain guidelines for Site Safeguards and Security Plans, in consultation with Secretarial Officers.

(11) Provide certification, in coordination with the Director of Energy Intelligence, that planned/installed physical and technical security systems create an environment of acceptable risk for intelligence-related facilities.

f. Director of Energy Intelligence, in addition to the duties outlined in subparagraphs c(1)-(5) above, shall:

(1) Serve as Senior Intelligence Officer for the Department.

(2) In coordination with the Office of Security Affairs, and consistent with line-management security responsibilities, develop guidelines, instructions, plans, and procedures for the protection of intelligence information consistent with safeguards and security policy and Director of Central Intelligence directives.

(3) Coordinate with the Director of Security Affairs to provide timely and current intelligence threat information to support the Safeguards and Security Program and threat assessment information.

(4) Act as Special Security Officer for line management security administration of Department Sensitive Compartmented Information Facilities.

(5) Provide liaison within the U.S. Intelligence community.

(6) Provide accreditations, in coordination with the Office of Safeguards and Security, that planned/installed physical and technical security systems create an environment of acceptable risk for intelligence-related facilities.

(7) Serve as the Department's point of contact involving activities related to intelligence, to include management of program access. Coordinate with Director of Security Affairs concerning security issues, to include espionage, and the possible or potential compromise of intelligence-related information.

g. Assistant Secretary for Environment, Safety and Health, in addition to the duties outlined in subparagraphs c(1)-(5) above, shall through the Deputy Assistant Secretary for Security Evaluations:

(1) Maintain an inspection, performance testing, and evaluation program to provide independent oversight of the Department's Safeguards and Security Program to assess the effectiveness of the implementation of policies, procedures, and operations.

(2) Assure that development and implementation of safeguards and security measures, in part through consultation, achieves consistency with environment, health, and safety requirements.

h. Assistant Secretary for Human Resources and Administration establishes policies, procedures, and programs for communications security, controlling electronic emissions (emissions security), and safeguarding unclassified computer systems.

i. Associate Deputy Secretary for Field Management shall:

(1) Have responsibility for strategic planning for all field elements, and management coordination and oversight of the multi-purpose Operations Offices as they impact the protection and control program planning process.

(2) Ensure guidance and requirements for physical protection of facilities is incorporated into DOE 6430.1A.

j. Director, Naval Nuclear Propulsion Program shall, in accordance with the responsibilities and authorities assigned by Executive Order 12344 (statutorily prescribed by Public Law 98-525 (42 U.S.C. 7158, note)) and to ensure consistency throughout the joint Navy/DOE organization of the Naval Nuclear Propulsion Program, implement and oversee all policy and practices pertaining to this DOE Order for activities under the Director's cognizance.

k. Heads of Field Elements are responsible for assuring that all operations under their jurisdiction are carried out consistent with sound safeguards and security practices and in accordance with the Safeguards and Security directives, supplementary policies and other Departmental guidance. In carrying out this responsibility the Heads of Field Elements shall:

(1) In conjunction with cognizant Program Offices, assure that safeguards and security interests under their jurisdiction are provided protection in accordance with the Departmental safeguards and security policy.

(a) Execute programs and ensure that contractors and their subcontractors execute programs and policies which utilize appropriate safeguards and security program elements for siting, design, construction, operation, maintenance, and modification of DOE facilities and activities.

(b) Take such action as may be appropriate to ensure acceptable safeguards and security, including curtailment or suspension of operations when such operation would result in an unacceptable risk to national security, or the health and safety of employees, or the public.

(c) Conduct performance tests of safeguards and security systems to verify the maintenance of a high state of effectiveness, as delineated in Departmental directives or as agreed in Site Safeguards and Security Plans.

(d) Examine, test, and evaluate the programs, projects, and facilities of subordinate field activities in accordance with safeguards and security requirements to assure compliance, effectiveness, and efficiency.

(e) Develop, validate, and submit to cognizant Program Office for approval Site Safeguards and Security Plans based on vulnerability/risk analyses for a comprehensive safeguards and security program.

(f) Establish and maintain liaison with Federal, state, or local law enforcement officials as appropriate, and advise the responsible Program Office of any requirements issued by these officials that will significantly affect DOE safeguards and security operations.

(g) Ensure that budget proposals for their assigned functions

provide for adequate safeguards and security resources.

(h) Provide training for their employees and contractors to assure they are made aware of and understand their responsibilities for protecting security interests.

(i) Ensure that supporting contracting officers incorporate contract or solicitation provisions implementing the requirements of all applicable Safeguards and Security directives in new or existing contracts which involve classified matter, nuclear material, or DOE property.

(2) Submit requests for exceptions to Safeguards and Security Program Orders and associated Manuals for review and approval as set forth in paragraph 9g of this Order. Process variances and waivers according to paragraph 9g(1)(a).

(3) When assuming senior management positions, at DOE Field Element Manager level, take action to review and determine the status of safeguards and security throughout their area of responsibility. A report shall be made to the cognizant Program Office with a copy to the Director of Security Affairs within 15 calendar days after assuming a Head of DOE Field Element position. The communication will include a statement that the review has been completed and will identify any significant deficiencies noted. As appropriate, actions being taken or planned to correct deficiencies should be included.

(4) Assure the procurement request packages, for each procurement requiring the application of this Order, include:

(a) Identification of the Order and the specific requirements or paragraphs with which a contractor or other awardee is to comply.

(b) Requirements for the flowdown of provisions to any subcontract or subaward.

l. Procurement Request Originators (the individuals responsible for initiating a requirement on DOE F 4200.33, "Procurement Request Authorization"), or such other individuals(s) as designated by the cognizant Heads of Departmental Elements shall bring to the attention of the cognizant contracting officer the following: (1) each procurement requiring the application of this Order; (2) requirements for flowdown of provisions of this Order to any subcontract or subaward; (3) identification of the paragraphs or other portion of this Order with which the awardee, or, if different, a subawardee, is to comply; and (4) identify need for and process any exceptions to this Order prior to submitting a procurement request to the Contracting Officer.

m. Contracting Officers at all levels shall incorporate contract or solicitation provisions implementing the requirements of all DOE Safeguards and Security directives in new or existing contracts which involve any of the following: classified matter, nuclear material, or DOE property.

9. CONCEPT OF OPERATIONS.

a. Program Definition. Numerous and varied activities and assets under the Department of Energy are vital to the national defense and energy security. Accordingly, the Department must ensure appropriate levels of protection from loss or theft of classified matter or Government property and acts of unauthorized access, theft, diversion, sabotage, espionage, or other hostile acts which may cause unacceptable risks to national security or the health and safety of DOE and contractor employees, the public, or the environment.

(1) Safeguards are an integrated system of physical protection, material accounting, and material control measures designed to deter, prevent, detect, and respond to unauthorized possession, use, or sabotage of nuclear materials.

(2) Security refers to those activities through which the Department defines, develops, and implements its responsibilities under the Atomic Energy Act of 1954, as amended, Federal statutes, Executive orders, and other directives for the protection of Restricted Data and other classified information or matter, nuclear materials, nuclear weapons and nuclear weapons components, and for the protection of DOE and DOE contractor facilities, property, equipment, and personnel.

b. Key Program Elements. Levels of protection appropriate to particular safeguards and security interests are provided through the development and execution of a comprehensive safeguards and security program. This Order establishes the authorities and responsibilities for managing and implementing the protection of security interests and sets forth the framework for the Orders and Manuals which define the policies, baseline requirements and responsibilities specific to the major elements of the Safeguards and Security Program. The key program elements are:

(1) Program Management (5630 Series).

(a) Program Planning;

(b) Program Management and Administration;

(c) Personnel Development and Training;

(d) Foreign Ownership, Control, or Influence; and

(e) Incident Reporting and Management.

(2) Personnel Security (5631 Series).

(a) Access Authorization (Personnel Clearance);

(b) Security Awareness;

(c) Control of Classified Visits; and

(d) Unclassified Visits and Assignments by Foreign Nationals.

(3) Protection Program Operations (5632 Series).

(a) Physical Security;

(b) Security Systems;

(c) Protective Forces;

(d) Security Badges, Credentials, and Shields;

(e) Incident Response and Management; and

(f) Transportation Security.

(4) Nuclear Materials Control and Accountability (5633 Series).

(a) Material Control; and

(b) Material Accountability.

(5) Surveys and Facility Approval (5634 Series).

(a) Security Surveys and Inspections;

(b) Materials Control and Accountability Surveys and Inspections; and

(c) Facility Activity Registration and Approval.

(6) Information Security (5639 Series).

(a) Classified Matter Protection and Control;

(b) Automated Information Systems Security;

(c) Technical Surveillance Countermeasures; and

(d) Operations Security.

(7) Independent Inspection and Evaluation (5630.12A).

c. Risk Analysis. The acceptance of some level of risk is inherent in any activity. The determination of the appropriate level of protection shall take into account the nature of the threat, the vulnerability of the potential target, and the potential consequences of an adversarial act. A rational and responsible balance will be obtained through the planning and execution of a comprehensive safeguards and security program. Specific site safeguards and security programs shall be based on vulnerability/ risk analyses. These programs shall be designed to provide a high degree of assurance that threats are deterred, denied, contained, mitigated, or neutralized, as appropriate. Risk associated with safeguards and security vulnerabilities should be reduced even where not mandated by specific requirements, when such reduction is consistent with the Department's mission and when supported by appropriate cost/benefit analyses.

d. Site Specific Programs. Individual safeguards and security programs shall be tailored to address specific site characteristics. The Site Safeguards and Security Planning process enables cognizant line organization program offices and field managers, in consultation with the Director of Safeguards and Security, to design and implement a protection program tailored to their respective operational needs, recognizing ongoing programs, current threat guidance, current policy and technology, and unique site specific requirements. Site-specific protection programs shall be documented in Site Safeguards and Security Plans. The residual risks to be accepted by the Department will be identified by vulnerability/risk analyses.

e. Independent Assessments. Assessment of possible environment, safety and health impacts at field organization level and review by the Assistant Secretary for Environment, Safety and Health provides a means to identify and resolve any environment, safety, and health issues which may arise in the execution of safeguards and security programs. Independent oversight to assess the effectiveness of the implementation of the Department's safeguards and security policies, procedures, systems and operations shall be provided through an inspection, performance testing and evaluation program conducted by inspection and evaluation teams of the Office of Security Evaluations.

f. Alternative Means and Deviations. Alternate or equivalent means of providing adequate safeguards and security may be proposed to meet a specific requirement of this and other Safeguards and Security Program Orders and associated Manuals. The following procedures and approval levels shall apply:

(1) Variance. A variance is an approved condition that technically varies from Safeguards and Security directive requirements, but affords equivalent levels of protection without compensatory measures.

(a) A variance may be approved by the Head of a Field Element. Notification of variances shall be made to the cognizant Headquarters Element and to the Office of Safeguards and Security.

(b) For Headquarters Elements, the cognizant Secretarial Officer may approve variances, with the concurrence of the Director, Headquarters Operations Divsion, Office of Safeguards and Security.

(c) Variances may be approved for an indefinite period of time.

(d) Variances shall be documented in the appropriate safeguards and security planning documents.

(e) Modifications to variances may be approved as described in paragraphs 9g(1)(a) and (b) above.

(2) Waiver. A waiver is an approved nonstandard condition that deviates from DOE directive requirements which, if uncompensated, would create a potential or real vulnerability and, therefore, requires implementation of compensatory measures for the period of the waiver (e.g., expenditure of additional resources to implement enhanced protection measures).

(a) Waivers may be approved by Heads of Field Elements providing:

(1) Cognizant Headquarters Program Office(s) and the Office of Safeguards and Security shall be notified of the nature of the waiver 30 days in advance of such approval.

(2) Comments provided by Headquarters Elements are considered before approving the waiver.

(3) Adequate compensatory measures are in place.

(4) Performance testing is accomplished, if appropriate.

(b) Waivers, for Headquarters Elements, may be approved by the cognizant Secretarial Officer providing:

(1) The Office of Safeguards and Security shall be notified of the nature of the waiver 30 days in advance of approval.

(2) The Director, Headquarters Operations Division has concurred in the waiver.

(3) The requirements of subparagraphs (a)(2), (3), and (4), above are met.

(c) A waiver shall be for a period not to exceed 2 years.

(d) Waivers shall be documented in appropriate safeguards and security planning documents.

(3) Exception. An exception is an approved deviation from a DOE Safeguards and Security directive requirement that creates a safeguards and security vulnerability. Exceptions shall be granted only when correction of the nonstandard condition is adjudged to be not feasible and compensatory measures are inadequate to preclude the acceptance of risk. An exception must be approved by both the Secretarial Officer and the Director of Security Affairs.

(a) For Field Elements, exception requests shall be submitted to the cognizant Secretarial Officer for review and approval by the Secretarial Officer and the Director of Security Affairs.

(b) For Headquarters Elements, approval of exceptions is granted by the cognizant Secretarial Officer and the Director of Security Affairs, through the Headquarters Operations Division.

(c) Exceptions may be granted for a period of up to 3 years.

(d) The need for continuation of exceptions shall be validated annually.

(e) Exceptions shall be documented in appropriate safeguards and security planning documents, and be included in Site Profiles which form the basis for the Department's Annual

Report to the President on the Status of Safeguards and Security.

(4) Specific elements of information to be included with each request for a deviation are provided in Attachment 2. Such cases shall be documented, and approved deviations shall be documented in safeguards and security documents. A deviation which is approved out of cycle with the safeguards and security plan formulation and approval process shall be documented as an attachment to the applicable safeguards and security plan.

(5) Compensatory measures which have been implemented and are used to form the basis for an exception request shall be subject to formal vulnerability assessments and must be performance tested and validated by the cognizant Field Element. The results of the vulnerability assessment(s) and performance tests shall be included in documentation support for the Site Safeguards and Security Plan. Performance testing and documentation, as necessary, may also be required for locally approved variances and waivers.

(6) Cognizant Secretarial Officer's and personnel representing the Office of Safeguards and Security may perform onsite reviews, assessments, and validation visits in order to obtain a full understanding of the nature and impact of deviation requests.

(7) Secretarial Officers shall ensure waivers and exception requests include realistic schedules for correcting the conditions requiring deviations, ensure funding is effectively managed to address safeguards and security interests, and monitor compliance with approved schedules.

g. Management Review of Safeguards and Security Programs. Individuals upon assuming senior management positions as set forth in paragraphs 8d(1) and 8k(3) shall complete a review to determine the status of safeguards and security programs under their responsibility. These reviews should include detailed briefings on the safeguards and security posture in the individual's area of responsibility. Results of oversight activities such as inspections and evaluations, security surveys, self-assessments, General Accounting Office audits, and other internal and external evaluation functions should be assessed. Where applicable, ratings included in reports to the President on the status of safeguards and security at domestic nuclear weapons facilities should be reviewed. The review must provide sufficient data and information to permit a determination of the current status of safeguards and security throughout the organization by the individual assuming responsibility for the organization. Onsite visits shall be conducted as soon as practical.

REFERENCES

1. Atomic Energy Act of 1954, as amended, Title 42 U.S.C.:

a. Chapter 2, "Definitions," section 11, which defines selected key terms.

b. Chapter 7, "Source Material," section 65, which authorizes orders requiring reports of ownership, possession, shipment of source material.

c. Chapter 12, "Control of information," sections 141-146, inclusive which sets forth the principles for the control of Restricted Data.

d. Chapter 12, "Control of information," sections 148, which prohibits unauthorized dissemination of unclassified nuclear information with respect to atomic energy defense programs.

e. Chapter 14, "General Authority," section 161, "General Provisions," which sets forth the authority for establishing and implementing a DOE security program for controlling access to Restricted Data and special nuclear material, including authority to carry firearms.

f. Chapter 18, "Enforcement," sections 221-234, which sets forth the authority necessary to protect Restricted Data and to safeguard property and establishes criminal penalties for violations; and section 235, which addresses "Protection of Nuclear Inspectors."

2. The Internal Security Act of 1950, as amended, Title 50 U.S.C.:

   a. Section 47a concerning illegal introduction, manufacture, acquisition, or export of special nuclear materials or atomic weapons, or conspiracies relating thereto;

   b. Section 781 regarding control of subversives;

   c. Section 784 regarding employment of members of communist organizations; and

   d. Section 797 on security regulations and orders and the penalty for violation.

3. National Security Act, Title 50, U.S.C., section 403, Chapter 15 which establishes the Central Intelligence Agency and gives it intelligence oversight over all Federal agencies.

4. Public Law 76-443, "Espionage Act," of 3-28-40, which establishes punishments for acts of interference with the foreign relations and commerce of the United States and espionage.

5. Executive Order 10450, "Security Requirements for Government Employees," of 4-27-53, as amended, which establishes the requirement for determining that all Federal employees are loyal, reliable, trustworthy, and of good conduct and character.

6. Executive Order 10865, "Safeguarding Classified Information Within Industry", of 2-24-60, as amended, which establishes the basis for industrial security program for civilian personnel.

7. Executive Order 12356, "National Security Information", of 4-2-82, which sets forth access guidance, provides requirements for information security including education and oversight programs, and authorizes establishment of procedures and promulgation of regulations to implement the Order.

8. National Security Decision Directive 84, of 3-11-83, titled "Safeguarding National Security Information," which establishes responsibilities for ensuring that nondisclosure agreements are obtained.

9. National Security Decision Directive 197, of 11-1-85, which establishes requirements for reporting hostile contacts and maintaining security awareness programs.

10. "Privacy Act of 1974," Title 5 U.S.C. Section 552a, which establishes the legal requirements for collecting and retaining information on individuals.

11. Title 10 CFR Part 710, Criteria and Procedures for Determining Eligibility for Access to Classified Matter or Significant Quantities of Special Nuclear Material, which is used in cases in which there are questions of eligibility for DOE access.

12. Title 10 CFR Part 860, Trespassing on Administration Property, which is issued for the protection and security of facilities, installations, and real property subject to the jurisdiction or administration of, or in the custody of, the Department.

13. Title 10 CFR 1008, Privacy Act; Records Maintained on Individuals, which establishes the procedures to implement the Privacy Act of 1974 within the DOE.

14. Title 10 CFR Part 1016, Safeguarding of Restricted Data, which establishes policy and requirements for the protection of Secret and Confidential Restricted Data.

15. Title 10 CFR Part 1046, Defense Programs, Physical Protection of

Security Interests, which sets forth policies and procedures applicable to DOE contractor employees and provides medical and physical fitness qualification standards, physical fitness training program requirements and medical examination and certification requirements.

16. Title 10 CFR Part 1047, Defense Programs; Limited Arrest Authority and Use of Force by Protective Force Officers, which establishes policy concerning arrests and associated use of physical and deadly force by DOE and DOE contractor employees engaged in protective force duties.

17. Title 18 U.S.C., relating to:

    a. Espionage or information control (Sections 792-98);

    b. Sabotage (Sections 2151-56);

    c. Treason and subversive activity (Sections 2381-85);

    d. Actual or threatened use of explosives against persons or property (Sections 841-48);

    e. Embezzlement and theft (Sections 641 and 6619);

    f. Extortion and threats (Sections 876-78):

    g. Riots (Section 2101);

    h. Acts of malicious mischief (Sections 1362-63); and

    i. Theft and destruction of Government property and civil disorders (Section 231).

18. Title 32 CFR, Chapter XX, Part 2001, "National Security Information, " Subparts D - Safeguarding, and Subpart E - Implementation and Review, Sections 2001.40 - .62.

19. Title 41 CFR Chapter 101, Federal Property Management Regulations, which sets forth policies and procedures for the protection of Government-owned and leased buildings and grounds under assignment responsibility of General Services Administration.

20. Title 48 CFR 970.2201, Basic Labor Policies, which establishes employment standards for management and operating contractors, including preemployment checks.

21. Federal Personnel Manual, Chapter 732, "Personnel Security," and Chapter 736, "Personnel Investigations," which implements Executive Order 10450 throughout Federal Departments and Agencies. These provisions provide for the establishment and maintenance of an effective personnel security program to insure that the employment and continued employment of each civilian in his or her capacity is clearly consistent with the interests of the national security and ADP-Computer security requirements.

22. DOE 1000.3B, INTERNAL CONTROL SYSTEMS MANUAL, of 07-05-88, which prescribes policies and standards for internal control systems in DOE, assigns responsibility and accountability to managers for internal controls within their programs and administrative functions, and establishes a requirement for an annual report assessing compliance with the Comptroller General's standards.

23. DOE 1324.2A, RECORDS DISPOSITION, of 09-13-88, which assign responsibility for the disposition of Departmental records.

24. DOE 1324.5A, RECORDS MANAGEMENT PROGRAM, of 04-30-92, which assigns responsibilities and authorities and prescribes policies, procedures, standards, and guidelines for the orderly disposition of DOE records.

25. DOE 5000.3B, OCCURRENCE REPORTING AND PROCESSING OF OPERATIONS INFORMATION, of 1-19-93, which establishes a system for reporting of operations information related to DOE-owned and operated facilities and processing of that information to provide for appropriate corrective action.

26. DOE 5500.1B, EMERGENCY MANAGEMENT SYSTEM, of 04-30-91, which establishes

overall policy and requirements for an Emergency Management System that will provide for development, coordination, and direction of DOE planning, preparedness, and readiness assurance for response to operational energy,and continuity of Government emergencies involving DOE or requiring DOE assistance.

27. DOE 5500.2B, EMERGENCY CATEGORIES, CLASSES, AND NOTIFICATION AND REPORTING REQUIREMENTS, of 04-30-91, which provides a DOE emergency notification and reporting system and establishes DOE emergency response levels and associated response actions.

28. DOE 5500.3A, PLANNING AND PREPAREDNESS FOR OPERATIONAL EMERGENCIES, of 04-30-91, which establishes requirements for the development of DOE site specific emergency plans and procedures for radiological emergencies occurring in existing or planned DOE reactors and nonreactors facilities.

29. DOE 5610.2, CONTROL OF WEAPON DATA, of 08-01-80, which establishes the policy and requirements for control of weapon data.

30. DOE 5630.12A, SAFEGUARDS AND SECURITY INSPECTION AND ASSESSMENT PROGRAMS, of 06-23-92, which establishes the policies and responsibilities for independent oversight of Safeguards and Security programs.

31. DOE 5630.13A, MASTER SAFEGUARDS AND SECURITY AGREEMENTS, of 6-8-92, which establishes DOE policy, requirements, responsibility and authorities for the development and implementation of Master Safeguards and Security Agreements.

32. DOE 5630.14A, SAFEGUARDS AND SECURITY PROGRAM PLANNING, of 6-9-92, which establishes a standardized approach to protection program planning.

33. DOE 5630.15, SAFEGUARDS AND SECURITY TRAINING PROGRAM, of 8-21-92, which establishes procedures for standardizing and implementing the DOE Safeguards and Security Training Program.

34. DOE 5630.16A, SAFEGUARDS AND SECURITY ACCEPTANCE AND VALIDATION TESTING PROGRAM, of 6-3-93, which establishes policy, requirements and responsibilities for the program that encompasses systematic processes for demonstrating the adequacy and functional reliability of critical system elements and/or total systems employed to meet protection needs.

35. DOE 5630.17, SAFEGUARDS AND SECURITY (S&S) STANDARDIZATION PROGRAM, of 9-29-92, which provides policies, procedures, responsibilities and authority for the program to ensure the most effective and efficient use and procurement of S&S equipment and systems.

36. DOE 5639.8A, SECURITY OF FOREIGN INTELLIGENCE INFORMATION AND SENSITIVE COMPARTMENTED INFORMATION FACILITIES, of 7-23-93, which establishes responsibilities and authorities for the protection of Foreign Intelligence Information (FII) and Sensitive Compartmented Information Facilities (SCIFs) within the Department of Energy.

37. DOE 5650.2B, IDENTIFICATION OF CLASSIFIED INFORMATION, of 12-31-91, which establishes the policy and requirements for the classification of information, documents, or material.

38. DOE 5670.1A, MANAGEMENT AND CONTROL OF FOREIGN INTELLIGENCE, of 01-15-92, which establishes the policy and requirements for the control of foreign intelligence.

39. DOE 6430.1A, GENERAL DESIGN CRITERIA, of 04-06-89, which provides guidance in the planning, design, and construction of new facilities and alteration of existing facilities.

40. "Safeguards and Security Definitions Guide", of 12-20-93, which lists Safeguards and Security terms and their accepted definitions.

41. Design Basis Threat Policy for the Department of Energy (DOE) Programs and Facilities, of 7-28-93, which provides various threats against which all facility Safeguards and Security protection plans must be designed.

DEVIATION REQUEST FORMAT

A. Date: Date the request is signed by the requesting official.

B. Request Number: A unique alphanumeric identifier beginning with "OSS," followed by the element symbol used in the DOE National Telephone Directory, followed by the last two digits of the calendar year in date of request, followed by a three digit number that is next in the sequence of requests from that field element in that calendar year. For example, the twenty-third request from Rocky Flats Office during 1992 would be OSS-RF-92-023.

C. Order Citation: Identification of the Order provision from which a deviation is being requested with a citation (paragraph or other provision) and summary of the Order requirement.

D. Impacted Entity: Identification of the specific facility (Master Facility Register number), process, procedure, system etc.

E. Deviation Justification: Specific description of the deviation and the associated reason or rationale for the deviation request. A description of the relationship of the subject of the deviation request to other safeguards and security interests shall be included if they are significantly effected.

F. Protection Measures: Description of the current measure(s) used for protection and an evaluation of the effectiveness of such measure(s); description of alternative measure(s) or level(s) of protection to be provided as an alternative to the Order requirement(s).

G. Duration: Expected duration of the condition for which the deviation is requested, including milestones for correcting, alleviating, or eliminating the deviant condition, if applicable.

H. Risks: An evaluation of the risk associated with the deviation, if approved. Results of vulnerability analyses and performance tests conducted on proposed alternative(s) shall be included.

I. Signatures: Requesting Officials Signatures.

<<EOD>>