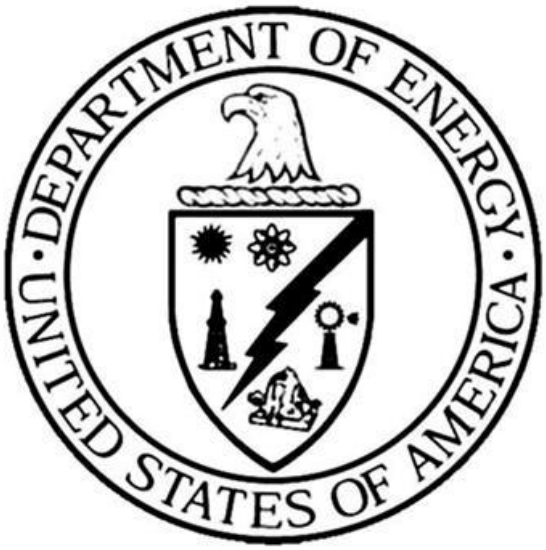
ORDER

DOE O 470.4B

Approved: 7-21-2011

SAFEGUARDS AND SECURITY PROGRAM



U.S. DEPARTMENT OF ENERGY

Office of Health, Safety and Security

SAFEGUARDS AND SECURITY PROGRAM

1. PURPOSE. To establish responsibilities for the U.S. Department of Energy (DOE) Safeguards and Security (S&S) Program, and to establish program planning and management requirements for the S&S Program. The requirements identified in this Order and its attachments and appendices are based on national policy promulgated in laws, regulations, Executive Orders, and national standards to prevent unacceptable adverse impacts on national security, the health and safety of DOE and contractor employees, the public, or the environment.

2. CANCELLATIONS. DOE O 470.4A, *Safeguards and Security Program*, dated 5-25-07; DOE M 470.4-1 chg 2, *Safeguards and Security Program Planning and Management*, dated 10-20-10; and DOE O 142.1, *Classified Visits Involving Foreign Nationals*, dated 1-13-04.

   Cancellation of a directive does not, by itself, modify or otherwise affect any contractual or regulatory obligation to comply with the directive. Contractor Requirements Documents (CRDs) that have been incorporated into a contract remain in effect throughout the term of the contract unless and until the contract or regulatory commitment is modified to either eliminate requirements that are no longer applicable or substitute a new set of requirements.

3. APPLICABILITY.

   a. Departmental Applicability. Except for the equivalencies/exemptions in paragraph 3.c., this Order applies to all Departmental elements.

      The Administrator of the National Nuclear Security Administration (NNSA) must ensure that NNSA employees comply with their responsibilities under this directive. Nothing in this directive will be construed to interfere with the NNSA Administrator's authority under section 3212(d) of P.L. 106-65, *National Nuclear Security Administration Act*, to establish Administration specific policies, unless disapproved by the Secretary.

      The Administrator of the Bonneville Power Administration (BPA) must ensure that BPA employees and contractors comply with their respective responsibilities under this directive consistent with BPA's procurement, self-financing, and statutory authorities.

   b. DOE Contractors. Except for the equivalencies/exemptions in paragraph 3.c., the CRD (Attachment 1) sets forth requirements of this Order that will apply to contracts that include the CRD.

      The CRD must be included in contracts that contain DOE Acquisition Regulation (DEAR) clause 952.204-2, *Security*. Heads of field elements and Headquarters Departmental elements must identify contracts that should incorporate the CRD

and notify contracting officers to incorporate the CRD into those contracts. Contracting officers are responsible for incorporating the CRD into the affected contracts as appropriate.

A violation of the provisions of the CRD relating to the safeguarding or security of Restricted Data or other classified information may result in a civil penalty pursuant to subsection a of section 234B of the Atomic Energy Act (42 U.S.C. Section 2282b). The procedures for the assessment of civil penalties are set forth in Title 10, Code of Federal Regulations (CFR), Part 824, *Procedural Rules for the Assessment of Civil Penalties for Classified Information Security Violations*.

c. Equivalencies/Exemptions for DOE O 470.4B. Equivalencies and exemptions from the requirements of this Order are processed in accordance with DOE O 251.1C, *Departmental Directives Program*.

When conditions warrant equivalencies or exemptions from the requirements in this Order, requests must be supported by a vulnerability assessment (VA) when required by the assets being protected, or by sufficient analysis to form the basis for an informed risk management decision; the analysis must identify compensatory measures, if applicable, or alternative controls to be implemented.

All approved equivalencies and exemptions under this Order must be entered in the Safeguards and Security Information Management System (SSIMS) database and incorporated into the affected security plan(s). Approved equivalencies and exemptions become a valid basis for operation when they have been entered in SSIMS and documented in the appropriate security plan, and must be incorporated into site procedures at that time.

Many DOE S&S Program requirements are found in or based on regulations issued by Federal agencies, and codified in the CFR or other authorities, such as Executive Orders or Presidential Directives. In such cases, the process for deviating from those requirements found in the source document must be applied. If the source document does not include a deviation process, the DOE Office of the General Counsel, or NNSA Office of General Counsel if an NNSA element is involved, must be consulted to determine whether deviation from the source can be legally pursued.

(1) Equivalency. In accordance with the responsibilities and authorities assigned by E.O. 12344, codified at 50 U.S.C. Sections 2406 and 2511 and to ensure consistency through the joint Navy/DOE Naval Nuclear Propulsion Program, the Deputy Administrator for Naval Reactors (Director) will implement and oversee requirements and practices pertaining to this Directive for activities under the Director's cognizance, as deemed appropriate.

(2) Exemption. Requirements in this Order that overlap or duplicate requirements of the Nuclear Regulatory Commission (NRC) related to radiation protection, nuclear safety (including quality assurance), and safeguards and security of nuclear material, do not apply to the design, construction, operation, and decommissioning of the facilities of the former Office of Civilian Radioactive Waste Management (RW) now managed by the Office of Nuclear Energy. This exemption does not apply to requirements for which the NRC defers to DOE or does not exercise regulatory jurisdiction.

4. REQUIREMENTS.

a. S&S programs must be developed and maintained that incorporate the responsibilities and requirements contained in this Order and its associated appendices and attachments.

b. Programs associated with each topical area found in the appendices and attachments to this Order must be implemented in accordance with the requirements stated for that topic.

c. The DOE Tactical Doctrine (Attachment 4) must be applied at facilities/sites possessing nuclear weapons and components, Category I special nuclear material (SNM), or targets subject to radiological or toxicological sabotage.

d. Incidents of security concern must be addressed in accordance with the requirements found in Attachment 5 and reported in accordance with applicable laws and regulations.

e. Interfaces and necessary interactions between S&S programs and other disciplines such as safety, emergency management, classification, counterintelligence, facility operations, cyber system operations and security, and business and budget operations including property management must be identified and clearly defined. These interfaces and interactions must be maintained throughout the lifecycle of protective measures to ensure that S&S planning and operations work together effectively with these disciplines. Sensitive Compartmented Information is under the purview of the Office of Intelligence and Counterintelligence; necessary interfaces and interactions between that office and S&S programs must also be identified, defined, and maintained

f. S&S programs must incorporate a risk-based approach to protect assets and activities against the consequences of attempted theft, diversion, terrorist attack, industrial sabotage, radiological sabotage, chemical sabotage, biological sabotage, espionage, unauthorized access, compromise, and other acts that may have an adverse impact on national security or the environment or that may pose significant danger to the health and safety of DOE Federal and contractor employees or the public.

g. S&S programs must be tailored to address site-specific characteristics and requirements, current technology, ongoing programs, and operational needs to achieve acceptable protection levels that reduce risks in a cost-effective manner.

5. RESPONSIBILITIES.

a. Secretary of Energy.

(1) Ensures that an effective S&S Program is established and executed within DOE under the authorities granted by relevant Executive Orders; the *U.S. Department of Energy Organization Act*, as amended (42 U.S.C. Sections 7101 to 7352); and the Atomic Energy Act, as amended (42 U.S.C. Sections 2011 to 2286), and in accordance with P.L. 106-65, the *National Nuclear Security Administration Act*.

(2) Designates senior Departmental officials to direct and administer the S&S Program.

(3) Delegates, in writing, all responsibilities and authorities as necessary for the administration of the S&S Program.

(4) Authorizes continuing operations of facilities/activities determined to be of high security risk.

(5) Exercises sole authority to approve the imposition of requirements on Civilian Radioactive Waste Management programs and activities that are more stringent and/or comprehensive than those imposed by the NRC.

(6) Designates the DOE program elements responsible for ensuring that foreign nationals' visits requiring access to classified information are conducted in accordance with governing international agreements or treaties.

b. Deputy Secretary.

(1) Exercises responsibility, as Chief Operating Officer of the Department, for S&S policy development and operations.

(2) Ensures that the S&S Program achieves excellence in performance, has internal compatibility, is graded in application, and integrates corporate programs and support activities with line programs consistent with the precepts of Integrated S&S Management.

(3) Reviews all staff and support office S&S policies that affect Departmental elements.

(4) Establishes the Department-wide base Security Conditions (SECON) level in consultation with the Under Secretaries; the Director, Office of Intelligence and Counterintelligence; and the Chief Health, Safety, and Security.

(5) In accordance with 50 U.S.C. Section 2656, ensures that the Committees on Armed Services of the U.S. House of Representatives and the U.S. Senate are notified of each significant nuclear defense intelligence loss.

(6) Approves and issues the *Graded Security Protection (GSP) Policy*.

c. Under Secretary for Nuclear Security/ Administrator for the National Nuclear Security Administration.

(1) Responsible for the management and implementation of S&S programs administered by NNSA.

(2) Authorizes continuing operations of NNSA facilities/activities determined to be of moderate security risk.

(3) In coordination with the Under Secretaries, the Office of Intelligence and Counterintelligence, and the Chief Health, Safety and Security Officer, provides recommendations on SECON levels to the Deputy Secretary.

(4) Through the Associate Administrator for Emergency Operations, monitors the SECON level for the Department and for all DOE facilities and sites.

(5) Through the Deputy Administrator for Defense Programs:

(a) Ensures that all visits by foreign nationals and access to classified information in connection with the military application of atomic energy under 42 U.S.C. Section 2164 and 42 U.S.C. Section 2121 are conducted in accordance with governing international agreements or treaties.

(b) Approves requests for classified visits and access to weapons programs, nuclear materials production facilities, sensitive nuclear materials production information, and classified information pertaining to Nuclear Weapons Data.

(c) Delegates in writing to a senior Federal official at each site under NNSA cognizance the authority to make, in connection with classified visits, an affirmative determination that permitting a U.S. citizen holding a clearance granted by another Federal agency to have access to Restricted Data will not endanger the common defense and security prior to granting such access in connection with a specific classified visit.

(6) Through the Deputy Administrator for Defense Nuclear Nonproliferation, ensures that all foreign national visits and access to classified information in connection with nonproliferation, international security, or International Atomic Energy Agency requirements are conducted in accordance with governing international agreements or treaties.

(7) Through the Deputy Administrator for Naval Reactors:

(a) Ensures that all foreign national visits and access to classified information in connection with naval nuclear propulsion are conducted in accordance with governing international agreements or treaties.

(b) Approves requests for classified visits and access to naval nuclear propulsion facilities.

(8) Through the Associate Administrator for Defense Nuclear Security:

(a) Serves as the DOE cognizant security officer responsible for the development and implementation of security programs, operations, and facilities under the purview of NNSA.

(b) Delegates authority to serve as the cognizant security office in writing as appropriate to subordinate NNSA line managers; delegations must be reflected in the affected facility/site security plans.

(c) Issues direction for and oversees implementation of SECON levels for operations under the cognizance of NNSA.

(d) Acts as senior NNSA official responsible for the direction and administration of the NNSA implementation and compliance with the National Industrial Security Program.

(e) Establishes procedures for reporting incidents of security concern, and provides resources for conducting inquiries and damage assessments and for implementing corrective actions.

(f) Directs the implementation of S&S programs in accordance with the requirements of this Order, including development of procedures and guidance on how to apply the requirements of the Order and its appendices and attachments at NNSA facilities and sites.

(g) Acts as the senior NNSA official responsible for all classified visits except for those assigned in Section 5c(5)(b) above to the Deputy Administrator for Defense Programs; delegates in writing

to a senior Federal official at each site under NNSA cognizance the authority to make, in connection with such classified visits, an affirmative determination that permitting a U.S. citizen holding a clearance granted by another Federal agency to have access to Restricted Data will not endanger the common defense and security prior to granting such access in connection with a specific classified visit.

(h) Ensures that facility and/or site defensive plans for the protection of nuclear weapons and components, Category I SNM, or targets subject to radiological or toxicological sabotage are developed in accordance with the DOE Tactical Doctrine.

(i) Implements the DOE North Atlantic Treaty Organization (NATO) program for DOE and NNSA including access authorizations, policy, operations of the DOE Sub-Registry, and the conduct of DOE domestic inspections.

d. Under Secretary for Science.

(1) Responsible for management and implementation of S&S programs administered by the DOE Office of Science.

(2) Serves as the DOE cognizant security officer responsible for the development and implementation of security programs, operations, and facilities under the purview of the Office of Science.

(3) Delegates authority to serve as the cognizant security office in writing as appropriate to subordinate line management within the Office of Science; delegations must be reflected in the affected facility/site security plans.

(4) In coordination with the Under Secretary for Energy, the NNSA Administrator, the Office of Intelligence and Counterintelligence, and the Chief Health, Safety and Security Officer, provides recommendations on SECON levels to the Deputy Secretary.

(5) Issues direction for and oversees the implementation of SECON levels for operations under the cognizance of the Office of Science.

(6) Directs the implementation of S&S programs in accordance with the requirements of this Order, including development of procedures and guidance on how to apply the requirements of the Order and its appendices and attachments at facilities and sites under the cognizance of the Office of Science.

(7) Establishes procedures for reporting incidents of security concern and provides resources for conducting inquiries and damage assessments and for implementing corrective actions.

(8) Authorizes continuing operations of Office of Science facilities/activities determined to be of moderate security risk.

(9) Ensures that facility and/or site defensive plans for the protection of nuclear weapons and components, Category I SNM, or targets subject to radiological or toxicological sabotage are developed in accordance with the DOE Tactical Doctrine.

(10) Delegates in writing to a senior Federal official at each site under his/her cognizance the authority to make, in connection with classified visits, an affirmative determination that permitting a U.S. citizen holding a clearance granted by another Federal agency to have access to Restricted Data will not endanger the common defense and security prior to granting such access in connection with a specific classified visit.

e. Under Secretary for Energy.

(1) Responsible for management and implementation of S&S programs administered by the DOE Offices of Energy Efficiency and Renewable Energy, Environmental Management, Electricity Delivery and Energy Reliability, Fossil Energy, Nuclear Energy, and Legacy Management.

(2) Serves as the DOE cognizant security office responsible for the development and implementation of security programs, operations and facilities under the purview of the Offices in paragraph (1).

(3) Delegates authority to serve as the cognizant security office in writing as appropriate to subordinate line management within the Departmental Offices in paragraph (1); delegations must be reflected in the affected facility/site security plans.

(4) In coordination with the Under Secretary for Science, the NNSA Administrator, the Office of Intelligence and Counterintelligence, and the Chief Health, Safety and Security Officer, provides recommendations on SECON levels to the Deputy Secretary.

(5) Issues direction for and oversees the implementation of SECON levels for operations under the cognizance of the Departmental Offices in paragraph (1).

(6) Directs the implementation of S&S programs in accordance with the requirements of this Order, including development of procedures and guidance on how to apply the requirements of the Order and its appendices

and attachments at facilities and sites under the cognizance of the Offices in paragraph (1).

(7) Establishes procedures for reporting incidents of security concern, and provides resources for conducting inquiries and damage assessments and for implementing corrective actions.

(8) Authorizes continuing operations of facilities/activities under the cognizance of the Departmental Offices in paragraph (1) determined to be of moderate security risk.

(9) Ensures that facility and/or site defensive plans for the protection of nuclear weapons and components, Category I SNM, or targets subject to radiological or toxicological sabotage are developed in accordance with the DOE Tactical Doctrine.

(10) Through the Assistant Secretary for Nuclear Energy:

(a) Ensures that visits by foreign nationals to uranium enrichment plants or facilities and access to classified information on uranium enrichment technology development, including advanced isotope separation technology, are conducted in accordance with governing international agreements or treaties.

(b) Approves requests for classified visits and access to uranium enrichment plants or facilities engaged in uranium enrichment technology development, including advanced isotope separation technology.

(11) Delegates in writing to a senior Federal official at each site under his/her cognizance the authority to make, in connection with classified visits, an affirmative determination that permitting a U.S. citizen holding a clearance granted by another Federal agency to have access to Restricted Data will not endanger the common defense and security prior to granting such access in connection with a specific classified visit.

f. Heads of Field Elements and Headquarters Departmental Elements.

(1) Oversee the development of S&S plans that describe S&S policy implementation in accordance with the requirements in this Order and its appendices and attachments and include detailed information on the assignment of roles, responsibilities, delegations, authorities, and development of budgets and allocation of resources.

(2) Oversee the development of S&S implementation procedures and guidance for programs described in this Order and its appendices and

attachments, implement the programs, and provide oversight and technical direction for the programs.

(3) Develop and allocate S&S budgets for assigned programs including budgets for the infrastructure that supports S&S missions.

(4) Ensure that line management implements the applicable provisions of programs described in this Order and its appendices and attachments.

(5) Notify contracting officers of affected contracts that must include the CRD and attachments to this Order.

(6) Ensure that procurement requests for new contracts require inclusion of appropriate language, including the clause at 48 CFR Section 952.204-2, *Security*, and the CRD and attachments to this Order in the resulting contracts, when applicable.

(7) Ensure that contracting officers provide DOE F 470.1, *Contract Security Classification Specification (CSCS)*, to the DOE cognizant security offices or their designees.

(8) Curtail or suspend operations at facilities/sites under their cognizance when continued operations would result in an unacceptable risk to national security and/or to the health and safety of DOE and contractor employees, the public, or the environment.

(9) Ensure that the authorized SECON levels are implemented at facilities/sites under their cognizance and that any local changes at affected facilities are reported to the Operations Center, Office of Emergency Operations.

(10) Ensure that S&S personnel under their cognizance are managed, trained, and equipped and are provided with the resources and support services needed to maintain protection of S&S interests.

(11) Ensure that contractors and subcontractors under their cognizance implement the provisions of the CRD and attachments to this Order when the CRD is incorporated in their contracts.

(12) Ensure that line management at sites under their cognizance has been delegated the authority for oversight and monitoring of contractor performance of the requirements contained in the CRD and its attachments, and that appropriate oversight and monitoring activities are conducted, including a process to validate established objectives, standards, and criteria for security training programs conducted by organizations other than the National Training Center.

(13) Ensure that a senior Federal official at each site under their cognizance has been delegated in writing the authority to make, in connection with classified visits, an affirmative determination that permitting a U.S. citizen holding a clearance granted by another Federal agency to have access to Restricted Data will not endanger the common defense and security prior to granting such access in connection with a specific classified visit.

g. Chief Health, Safety, and Security Officer.

(1) Develops the Department's S&S Program consistent with strategies and policies governing the protection of national security and other critical assets entrusted to the Department and in accordance with laws, regulations, and national-level policies and standards.

(2) Coordinates and promulgates the Department's policies and procedures for a comprehensive S&S Program.

(3) In coordination with the Under Secretaries, the NNSA Administrator, and the Office of Intelligence and Counterintelligence, provides recommendations on SECON levels to the Deputy Secretary.

(4) Directs the development and implementation of a security program for the protection of the DOE Headquarters, its personnel, and its assets; serves as the DOE cognizant security officer for DOE Headquarters facilities, and delegates this authority in writing as appropriate.

(5) Oversees implementation of the DOE Headquarters S&S Program, including the development of S&S implementation procedures and guidance for programs described in this Order and its appendices and attachments, to include the approval of Headquarters equivalencies and exemptions; provides oversight and technical direction for all DOE offices located in Headquarters facilities.

(6) Ensures that the authorized SECON levels are implemented for operations under the cognizance of the Office of Health, Safety and Security.

(7) Provides advice and assistance to DOE organizations concerning S&S programs described in this Order and its appendices and attachments.

(8) Implements the procedures for the assessment of civil penalties set forth in 10 CFR Part 824, *Procedural Rules for the Assessment of Civil Penalties for Classified Information Security Violations*.

(9) Serves as the executive agent responsible for the development of the GSP, ensures that the GSP is periodically reviewed and updated, staffs and obtains approval for the GSP through the offices of the Under Secretaries, and recommends action to approve the GSP to the Deputy Secretary.

(10) Reviews procurement requests for new HSS Headquarters contracts and ensures that the provisions of 48 CFR Section 952.204-2, *Security*, and the requirements of the CRD and its attachments in this Order are included in the contracts when required.

(11) Through the HSS Deputy Chief for Operations:

(a) Formulates and promulgates Departmental S&S policy.

(b) Acts as the senior Agency official responsible for directing and administering the DOE's implementation of E.O. 12829, *National Industrial Security Program*, Section 203(a).

(c) Maintains national-level liaison with Federal law enforcement, security, and intelligence agencies in support of the DOE S&S Program; and represents DOE in interagency efforts related to S&S activities.

(d) Develops S&S training programs, and provides S&S training to Departmental personnel, primarily through the National Training Center.

h. Director, Office of Intelligence and Counterintelligence.

(1) Ensures that information developed through intelligence/ counterintelligence program activities that affects S&S operations is shared with HSS and NNSA.

(2) Notifies the DOE/NNSA cognizant security office of security incidents during the course of intelligence/counterintelligence activities. This notification will be upon discovery unless such notification would severely impede or negate intelligence activities or counterintelligence investigations, or further compromise classified/sensitive information.

(3) Ensures coordination with cognizant security offices, as appropriate, concerning security issues and other matters of mutual concern for inclusion in security awareness activities and develops and conducts briefings to present information on intelligence and counterintelligence issues. Such briefings may be in conjunction with security awareness briefings.

(4) Ensures that all foreign national visits and access to classified information in connection with Sensitive Compartmented Information (SCI) are conducted in accordance with governing international agreements or treaties.

(5) Ensures that information on relevant intelligence/counterintelligence concerns is provided to Departmental elements responsible for classified visits by non-U.S. citizens under international agreements and treaties and to individuals responsible for hosting classified visits by non-U.S. citizens to DOE facilities and sites.

(6) In coordination with the Under Secretaries, the NNSA Administrator, and the Office of Intelligence and Counterintelligence, provides recommendations on SECON levels to the Deputy Secretary.

(7) Issues direction for and oversees the implementation of SECON levels for operations under the cognizance of the Office of Intelligence and Counterintelligence.

i. General Counsel, Office of the General Counsel. Provides legal advice and assistance to HSS regarding issues or changes in laws and regulations that may affect S&S interests and programs.

j. Contracting Officers.

(1) Upon notification by a DOE/NNSA line management official initiating a procurement activity, incorporate CRDs into affected contracts as appropriate.

(2) Assist originators of procurement requests who want to incorporate the provisions of 48 CFR Part 952.204-2, *Security*, and appropriate CRDs in new contracts.

(3) Provide written notification to DOE/NNSA cognizant security offices in accordance with Appendix B, Section 2, of this Order when contractual changes impacting a company's foreign ownership, control, or influence occur.

k. DOE Cognizant Security Offices. Responsibilities of the designated DOE cognizant security offices applicable to each topical area are found in the appendices.

6. REFERENCES. The following general references apply to this Order. Additional references applicable to each topical area in the appendices and attachments are listed under that topic for ease of identification. Complete reference information and links to the most current official version of each document or successor documents are available through the S&S Policy Information Resource (PIR) tool at http://pir.pnl.gov/.

a. 42 U.S.C. Sections 2011 to 2296, *Atomic Energy Act of 1954*, as amended. Establishes authorities and programs related to atomic energy, including programs for Federal control of the possession, use, and production of nuclear energy and SNM whether owned by the U.S. Government or others.

b. 42 U.S.C. Sections 7101 to 7352, *Department of Energy Organization Act*, as amended. Establishes DOE and its basic authorities and responsibilities, including the responsibility of the Secretary of Energy for developing and promulgating DOE security policies.

c. 10 CFR Part 824, *Procedural Rules for the Assessment of Civil Penalties for Classified Information Security Violations*. Establishes rules to assess a penalty against contractors for violation of a directive relating to the protection of classified information.

d. 10 CFR Part 1016, *Safeguarding of Restricted Data*. Establishes requirements for granting facility security approval to an access permittee.

e. 10 CFR Part 1045, *Nuclear Classification and Declassification*. Establishes the program for managing, identifying, generating, reviewing, and declassifying Restricted Data and Formerly Restricted Data, and the sanctions for violations of the procedures.

f. 32 CFR Chapter XX, *Information Security Oversight Office, National Archives and Records Administration*. Establishes implementation requirements and procedures for classified national security information and the National Industrial Security Program.

g. 48 CFR Chapter 9, *Department of Energy Acquisition Regulation*. Supplements 48 CFR Chapter 1, *Federal Acquisition Regulation*, and includes the security provisions and clauses to be used in DOE solicitations and contracts when a facility security clearance and/or access to classified information will be necessary for the performance of the contract.

h. E.O. 12829, *National Industrial Security Program*, dated 01-26-93. Establishes the National Industrial Security Program to protect classified information released by Federal agencies to their contractors.

i. E.O. 13526, *Classified National Security Information*, dated 12-29-09. Establishes the requirements for protection of classified information.

j. DOE P 226.1B, *Department of Energy Oversight Policy*, dated 4-25-11. Establishes a Department-wide oversight process to protect the public, workers, environment, and national security assets effectively through continuous improvement.

k. DOE O 226.1B, *Implementation of Department of Energy Oversight Policy*, dated 4-25-11. Implements the policy that establishes a Department-wide oversight process to protect the public, workers, environment, and national security assets.

l. DOE O 414.1D, *Quality Assurance*, dated 4-25-11, which ensures that the quality of DOE/NNSA products and services meets or exceeds the customers' requirements and expectations.

m. DOE O 475.2A, *Identifying Classified Information*, dated 2-1-11. Establishes the program to identify information classified under the Atomic Energy Act or E.O. 13526 so that it can be protected against unauthorized disclosures.

n. DOE Order 475.1, *Counterintelligence Program*, dated 10-04-04, establishes the Counterintelligence (CI) Program requirements and responsibilities for the Department of Energy (DOE), including the National Nuclear Security Administration (NNSA), pursuant to Executive Order 12333 in order to detect and deter insiders who engage in activities on behalf of a foreign intelligence service or international terrorist entity.

o. DOE Order 243.1, *Records Management Program*, dated 2-3-06, which sets forth requirements and responsibilities for implementing and maintaining a cost-effective records management program throughout the Department of Energy.

p. 36 CFR Chapter XII, Subchapter B, *Records Management*. Establishes requirements for the creation, maintenance, and disposition of Federal records and penalties for unlawful or accidental removal, alteration, or destruction of records.

q. Homeland Security Presidential Directive-7, *Critical Infrastructure Identification, Prioritization, and Protection*, dated 12-17-03, which establishes a national policy for Federal departments and agencies to identify and prioritize United States critical infrastructure and key resources and to protect them from terrorist attacks.

7. DEFINITIONS.

a. Cognizant security office means the office assigned responsibility for a given security program or function. Where DOE cognizant security office is stated, the reference is to a Federal activity.

b. Definitions applicable to each topical area are found in the appendices and attachments. Definitions for terms used in a general S&S context are available through the Safeguards and Security Policy Information Resource (PIR) tool at http://pir.pnl.gov/.

8. CONTACT. Questions concerning this Order should be addressed to the Office of Security Policy, Office of Health, Safety and Security at 301-903-4642.

BY ORDER OF THE SECRETARY OF ENERGY:

DANIEL B. PONEMAN
Deputy Secretary

TABLE OF CONTENTS

APPENDIX A. SAFEGUARDS AND SECURITY PROGRAM PLANNING

This appendix establishes the U.S. Department of Energy (DOE) requirements for developing facility and site security plans and for ensuring that plans are current and address the actual operating conditions at the covered location through performance assurance testing and a program of regular periodic surveys. Section 1 addresses planning activities. Section 2 covers activities to be implemented in connection with surveys.

SECTION 1. SAFEGUARDS AND SECURITY PROGRAM PLANNING

1. OBJECTIVE. To establish a safeguards and security (S&S) planning approach that will provide facilities and sites with a consistent method for identifying, developing and documenting sound risk mitigation strategies by identifying all critical S&S performance, technical, schedule, and cost elements.

2. PURPOSE. S&S planning activities are conducted to ensure that an S&S plan describing the assumptions and approved operating conditions necessary to protect national security and property assets, as well as the public, DOE employees, and contractor employees, from malevolent actions by adversaries is prepared for each facility and site and approved by an appropriate Federal authority.

3. DEFINITIONS.

   a. Facility. A facility consists of one or more security interests under a single security management responsibility or authority and a single facility security officer within a defined boundary that encompasses all the security assets at that location. A facility operates under a security plan that allows security management to maintain daily supervision of its operations, including day-to-day observations of the security program.

   b. Site. A site consists of one or more facilities operating under a centralized security management, including a site security officer with consolidated authority and responsibility for the facilities, and covered by a site security plan that may consolidate or replace, wholly or partially, individual facility plans.

   c. S&S Interest(s) and/or Assets. A general term for any Departmental resource or property that requires protection from malevolent acts. It includes but is not limited to Federal and contractor personnel; classified information and/or matter; sensitive compartmented information facilities; automated data processing centers; facilities storing, processing, and transmitting classified information and/or matter; vital equipment; special nuclear material (SNM); other nuclear materials; certain radiological chemical or biological materials; sensitive unclassified information; or other Departmental property.

   d. Essential Elements. Protection and assurance elements necessary for the overall success of the S&S program at a facility or site, the failure of any one of which would result in protection effectiveness being significantly reduced or which would require performance of other elements to be significantly better than expected in order to mitigate the failure. Essential elements can include but are not limited to equipment, procedures, and personnel.

4. REFERENCES.

a. DOE P 470.1A, *Safeguards and Security Program*, dated 12-29-10.

b. DOE O 470.3B, *Graded Security Protection (GSP) Policy*, dated 8-12-08.

c. 48 CFR Section 952.204-2, *Security*, and Section 952.204-73(c), *Facility Clearance*.

d. E.O. 12977, *Interagency Security Committee*, dated 10-19-95.

e. Interagency Security Committee (ISC) Standard, *Physical Security Criteria for Federal Facilities*.

f. ISC Standard, *Facility Security Level Determinations for Federal Facilities*.

g. ISC Report, *The Design Basis Threat (DBT).*

h. DOE-STD 1192-2010, *Vulnerability Assessment Standard*.

i. PDD 39, *U.S. Policy on Counterterrorism*.

j. HSPD 3, *Homeland Security Advisory System*.

k. DoD 5220.22-M, *National Industrial Security Program Operating Manual (NISPOM).*

l. DOE O 150.1, *Continuity Programs*, dated 5-8-08.

m. HSPD-7, *Critical Infrastructure Identification, Prioritization, and Protection*.

5. REQUIREMENTS. DOE cognizant security offices, as designated by the Program Secretarial Office or, for NNSA, the Office of the Administrator through the Chief, Defense Nuclear Security, are responsible for ensuring that the following security planning activities are accomplished for facilities and sites under their cognizance.

a. Ensure that planning activities support the Department's Strategic Plan, the facility's/site's mission, forecasts of significant changes to facility/site operations, and current and projected operational and fiscal constraints.

b. Review and approve contractor security plans, establishing a Federally approved authorization for site security operations.

c. Ensure that designated Federal approval officials with authority for security plans explicitly accept any residual risk involved in operations under the requirements of approved security plans.

d. Ensure that approved security plans continue to accurately describe site/facility S&S procedures and requirements.

e. Ensure that site operations are conducted in compliance with approved security plans.

f. Monitor progress on completion of implementation plans to ensure that approved actions are completed within the approved time frames.

g. Ensure that facilities/sites that possess nuclear weapons and components, Category I SNM, or targets subject to radiological or toxicological sabotage develop and implement defense strategies and Security Incident Response Plans in accordance with the DOE Tactical Doctrine contained in Attachment 4.

h. Ensure that assessments of protection effectiveness are conducted at a level of detail and rigor appropriate to the assets and security interests being protected and in accordance with national standards and DOE directives, and ensure that documentation of such analyses are maintained in support of the security plan.

i. Provide assurances for safeguarding against loss, theft, diversion, unauthorized access, misuse, or sabotage of radioactive materials and radioactive sealed sources that could adversely affect national security and the health and safety of employees, the public, and the environment in accordance with DOE O 470.3B, *Graded Security Protection (GSP) Policy*, DOE M 231.1A chg 2, *Environment, Safety and Health Reporting Manual*, and 10 CFR Part 835, *Occupational Radiation Protection*, Subpart M and Appendix E.

j. Develop Security Condition (SECON) response plans that can be immediately implemented when there is a change in either the Department's or a specific facility's/site's SECON status.

CHAPTER I. SECURITY PLANS

1. GENERAL. All facilities and sites under DOE cognizance must have a security plan that reflects the assets, security interests, approved S&S program implementation at that location and any residual risks associated with operation under the security plan.

   a. DOE site security managers, in consultation with contractor security managers, will determine and define the facilities under their cognizance and how or if a group of facilities will be consolidated into a site. This decision is made locally in order to facilitate the security management at each location.

   b. For those facilities that do not have security assets (e.g., classified information or matter, SNM, or other assets requiring a facility security clearance (FCL) in accordance with the Facility Clearance section in Appendix B), the security plan must be developed to address the protection of employees and Government-owned or leased property.

   c. For all U.S. Government owned or leased properties that do not have security assets (e.g., classified information or matter, SNM, or other assets requiring an FCL in accordance with the Facility Clearance section of this directive), but to which DOE Federal employees are assigned, the standards set forth by the ISC under E.O. 12977, *Interagency Security Committee*, must be used as the baseline for developing the security plan.

   d. While the ISC standards do not apply to contractor owned or leased facilities in which Federal employees are not routinely assigned, they should be used to establish the basis for planning for the protection of employees and Government-owned or leased property at contractor facilities that do not have security assets (e.g., classified information or matter, SNM, or other assets requiring an FCL in accordance with the Facility Clearance section of this directive).

   e. Facilities with security interests that require an FCL but that do not fall under the provisions of the *Graded Security Protection (GSP)* policy must develop security plans that, in addition to the protection of employees and property, address the protection of security interests at that location and meet the requirements in national-level policy and DOE directives for the protection of those interests. Non-possessing facilities must develop a security plan in sufficient detail to address how the contractor will fulfill its responsibilities (reporting requirements, management of employee clearances, etc.) under the Facility Clearance Program.

   f. For facilities under the cognizance of the Power Marketing Administrations, which do not fall under the provisions of the GSP but must meet specific critical infrastructure requirements, security plans will be developed under locally

determined field element security levels and will be approved by the Chief Security Officer for each Power Marketing Administration.

g. Facilities with security interests to which GSP performance standards or other requirements apply must develop security plans that comply with the requirements in the GSP and incorporate the DOE Tactical Doctrine in addition to complying with the requirements in national-level policy and DOE directives for the protection of any security interests not covered by the GSP performance standards, and in addition to the protection of employees and property.

2. SECURITY PLAN. The security plan is the approved method for conducting security operations at a facility or site and therefore must reflect security operations at that facility or site at all times. The plan must describe in detail, either in its content or in combination with other explicitly referenced documents, all aspects of S&S operations occurring at the location and must include documentation of any deviations from national or DOE requirements. At those locations where management has determined that several facilities can be consolidated into a site, the site security plan may consolidate or replace individual facility security plans in whole or in part but must establish a unified approach to conducting site operations. Security plans must be based on in-depth analysis of considerations specific to the location and the assets and interests to be protected.

3. ASSESSMENTS AND ANALYSES. Security plans must be supported by a sufficient analytical basis to establish that protection requirements will be met if the plan is completely and effectively executed. The analytical basis must include, as applicable, qualitative and quantitative simulations, performance test results, and/or expert analysis that reflect the complexity of facility/site operations and the consequences of loss or unauthorized access or use of the security assets present.

When facility/site security assets include Category I (or credible rollup to Category I) SNM, vulnerability assessments (VAs), force-on-force system performance tests, other applicable performance tests, and expert analysis must be used in combination to establish the requirements for specific security measures and equipment, the effectiveness of the proposed security posture, and the requirements for improvements in the protection of Category I SNM documented in the approved security plan(s). Documentation of all such assessment activities should be retained on file to demonstrate how the security plan was developed and evaluated. However, these analyses need not be included or specifically referenced in the approved plan.

4. SECURITY PLAN COMPONENTS. All security plans must include the following:

a. A listing and prioritization of the assets and security interests at the facility or site; a description of how the protection program is managed; and a description of how national and DOE S&S requirements are met, including any deviations from requirements; and

b. As required, implementation plans for meeting changes in national or DOE policies or other changes (such as the addition or removal of security interests) that may require an extended time frame to implement because of financial or other resource considerations, including an implementation schedule and planned contingency measures in case the requirements cannot be met as scheduled. Implementation plans and contingency measures may be included in the security plan by reference. DOE cognizant security offices must monitor contractors' implementation plans to ensure that requirements are implemented without unnecessary delays.

5. REVIEWS AND UPDATES. Security plans must be reviewed as required to ensure that the plans are current and reflect the actual operating conditions at the covered location. Changes to approved security plans must be approved by the DOE cognizant security office, and the Federal office may require more frequent reviews or may direct a contractor to review the contractor's plan at any time. Updates to security plans must be made whenever any of the following conditions apply:

a. Changes in baseline security requirements in national-level or DOE policy;

b. Changes in facility operators/contractors;

c. Changes in assets or security interests;

d. Changes in facilities included in a site security plan;

e. Changes in the security posture of a facility or site;

f. Planned changes to the security program at the facility or site; or

g. Changes in operations at a facility or site that require modification to approved security measures.

CHAPTER II. SECURITY CONDITIONS

1. GENERAL. DOE SECON levels reflect a multitude of conditions that may adversely impact Departmental and/or facility and site security. SECONs may include terrorist activity, continuity conditions, environmental (fire, chemical, radiological, etc.) and/or severe weather conditions. The day-to-day DOE security readiness state is informed by the Homeland Security National Terrorism Advisory System (NTAS). NTAS alerts are established based on the analysis of a continuous and timely flow of integrated, all-source threat assessments and reporting provided to Executive Branch decision-makers. This chapter details DOE requirements for responding to changes in the NTAS alerts and the Departmental SECON levels.

2. SECON LEVELS. The following are the SECON levels used by DOE to establish the current security readiness state:

   a. SECON 5, Low Condition. This condition is declared when there is a low risk of terrorist activity, continuity conditions, environmental, and/or severe weather conditions. SECON 5 exists when a minimal SECON concern exists but warrants only a routine security posture.

   b. SECON 4, Guarded Condition. This condition is declared when there is a general risk of terrorist activity, continuity conditions, environmental, and/or severe weather conditions. SECON 4 applies when there is a broad, non-specific threat of a possible event, the nature and extent of which are unpredictable. All measures selected for use under SECON 4 must be capable of being maintained indefinitely.

   c. SECON 3, Elevated Condition. SECON 3 is declared when there is a significant risk of terrorist activity, continuity conditions, environmental, and/or severe weather conditions. SECON 3 applies when an increased and more predictable threat against DOE facilities exists. The measures used in SECON 3 must be capable of being maintained for lengthy periods without causing undue hardship, affecting operational capability, or aggravating relations with the local community.

   d. SECON 2, High Condition. SECON 2 is declared when there is a high risk of terrorist activity, continuity conditions, environmental, and/or severe weather conditions. This condition may apply when an incident occurs or intelligence is received indicating that some form of action against DOE personnel and facilities is imminent. Implementation of measures in this security condition for more than a short period will probably create hardship and affect the routine activities of the facility/site and its personnel.

e. SECON 1, Severe Condition. This condition reflects a severe risk of terrorist activity, continuity conditions, environmental, and/or severe weather conditions. SECON 1 applies in the immediate area where conditions have occurred that may affect a DOE facility/site or when an attack is initiated on the facility/site. Implementing SECON 1 will create hardship and affect the activities of the location and its personnel. Normally, this condition will be declared as a localized response.

3. SECON PLANNING. Both contractor and Federal site security offices must develop SECON response plans that can be immediately implemented when there is a change in either the Department's or a specific facility/site's SECON status. Each facility or site must identify the specific measures that will most efficiently and effectively implement the required increases in readiness at each SECON level. Protection measures listed in HSPD-3 and the DOE SECON Quick Reference tool (http://www.hss.energy.gov/Referencebook/secon.html) may be used to develop response plans, which must describe the specific actions to be taken for each SECON level. SECON response plans must be made a part of the facility or site security plan.

4. ESTABLISHMENT OF SECON LEVEL.

a. Departmental SECON Level. Department-wide SECON levels are established by the Deputy Secretary of Energy in consultation with the Under Secretaries, the Director, Office of Intelligence and Counterintelligence, and the Chief Health, Safety and Security Officer. Departmental SECON levels will be determined using existing threat, environmental, COGCON levels as specified in DOE O 150.1, *Continuity Programs*, and/or other program considerations/factors for Headquarters and field activities. Changes in the COGCON level may require concurrent changes in the SECON level.

b. Local SECON Levels. Local SECON levels may differ from the Departmental SECON level and are established by site/facility management with the concurrence of the cognizant Under Secretary or, in the case of DOE Headquarters, the Chief Health, Safety and Security Officer.

5. COORDINATION. If the determination is made that a site/facility SECON level should differ from the Departmental SECON, site/facility management must immediately notify the Operations Center, Office of Emergency Operations, Office of the Associate Administrator for Emergency Operations, NNSA, of the changed condition and keep the Operations Center informed of the status of the facility and the SECON response plan implementation.

CHAPTER III. PERFORMANCE ASSURANCE

1. GENERAL. An acceptable level of performance must be established and maintained to ensure that all elements of a facility/site protection program are workable and function as designed and in accordance with the overall protection goals established by local facility/site management. A performance assurance program must be developed that identifies the essential elements of the protection program and establishes monitoring and testing activities with sufficient rigor to ensure that the program elements are at all times operational, functioning as intended, and interacting in such a way as to identify and preclude the occurrence of adverse activity before security is irreversibly compromised. The intent of the performance assurance program is not to duplicate monitoring and testing activities conducted under ongoing quality assurance and S&S operations, but to include them in a comprehensive approach to assuring system effectiveness. Implementation activities and schedules for performance assurance plans must be included in the facility or site security plan.

2. APPLICABILITY. All facilities with assets requiring a facility security clearance must conduct performance assurance activities. These activities must be tailored to the assets at the location and the elements that compose the total system in place at the location. At all locations, testing will include at a minimum the following:

   a. Operability tests to confirm, without any indication of effectiveness, that a system element or total system is operating as expected; and

   b. Effectiveness tests to provide assurance that essential elements of the system are working as expected, separately or in coordination, to meet protection program objectives.

3. PERFORMANCE ASSURANCE PLANNING. Facilities and sites must implement and maintain a program that ensures that essential elements used to protect DOE S&S interests meet established requirements for reliability, operability, readiness, and performance prior to and during operational use. The assurance plan must:

   a. Encompass all S&S topical areas relating to Program Management Operations, Physical Protection, Protective Force, Information Security, Personnel Security, and Materials Control and Accountability that are relevant to protection of assets at the facility/site;

   b. Identify the essential elements relevant to protection of assets at the facility/site;

   c. Describe how essential elements relevant to the protection of assets were determined;

   d. Describe how each essential element and the facility/site security program as a whole will be tested, including type of test, evaluation criteria (test objectives and

performance criteria that define both success and failure), frequency, and number of tests;

e. Establish the testing schedule for essential elements and note whether any testing requirements established in other applicable DOE directives are to be integrated with this schedule;

f. Describe the process for managing, tracking, and integrating results and addressing any deficiencies identified during the tests; and

g. Describe actions that must be initiated in the event of a failure of any essential element or the program as a whole.

4. TEST SCHEDULES.

a. Essential elements must be periodically tested to verify their continued functionality, operability, effectiveness, and/or performance. Testing frequency may be based as applicable on manufacturer's recommendations, consensus standards, facility-/site-specific conditions and operational needs, or other criteria that will ensure program effectiveness. Testing of elements that are not prone to failure and that are not subject to compromise without noticeable tampering, such as walls and fences, is not required as long as it can be documented that tampering with such elements would be detected in time to prevent compromise of overall protection.

b. In addition to the testing of essential elements, at least once every 12 months, a comprehensive facility or site threat scenario test must be performed at facilities/sites with Category I special nuclear material (SNM); with identified credible radiological, biological, or chemical sabotage targets; or that have been identified as critical national security facilities/assets to demonstrate overall facility/site S&S system effectiveness. Comprehensive threat scenarios must be consistent with DOE O 470.3B, *Graded Security Protection (GSP) Policy*.

c. Facilities/sites with denial protection strategies must conduct, in addition to the tests noted above, protective force exercises quarterly with a rotational schedule for multiple facilities requiring denial protection strategies. One of these quarterly tests may be combined with the annual comprehensive threat scenario test.

5. RESULTS ANALYSIS AND DOCUMENTATION. Each test must be documented in a test report that includes a narrative description of the testing activity and an analysis of test results. Issues requiring corrective action must be documented and tracked until resolved. When unsatisfactory results of a test indicate that national security and/or the health and safety of facility/site employees or the public is jeopardized, immediate compensatory measures must be taken until the issue is resolved and normal reporting procedures must be followed.

6. SYSTEM DEGRADATION. When an essential element is under repair or is in an inoperative or ineffective state, the overall S&S program must be considered to be in a degraded mode until testing confirms that all applicable elements have returned to full operability. The facility or site must implement compensatory measures during such degraded modes adequate to ensure that protection of assets is maintained.

7. REVIEWS AND UPDATES. Performance assurance plans must be reviewed and updated when essential elements are affected due to:

   a. Changes in facility/site mission, programmatic activities, or S&S interests and/or assets;

   b. Changes in the operation or physical configuration of a facility or site, such as a building addition; new work processes or systems; construction of fences, roads, buildings, etc.; demolition of buildings; or reconfigurations of fences, roads, etc.;

   c. Completion of S&S upgrades or downgrades;

   d. Changes in protection strategy, risk or vulnerability analysis, protective force deployment, or other significant revisions to the applicable security plan; or

   e. Changes in S&S policies, including DOE Order 470.3B, *Graded Security Protection (GSP) Policy*.

SECTION 2. SURVEY, REVIEW, AND SELF-ASSESSMENT PROGRAMS

1. OBJECTIVE.

   a. Provide assurance to the Secretary, Departmental Elements, and other government agencies that S&S interests and activities are protected at the required levels.

   b. Provide DOE line management with the information necessary to make informed decisions regarding the allocation of resources, acceptance of risk, and mitigation of S&S vulnerabilities.

2. PURPOSE. Surveys, self-assessments, and review programs are conducted to ensure that S&S systems and processes at facilities/sites are operating in compliance with Departmental and national-level policies, requirements, and standards for the protection of security assets and interests. These programs provide the means for timely identification and correction of deficiencies and noncompliant conditions to prevent adverse events, and validate the effectiveness of corrective actions implemented to address identified deficiencies.

3. DEFINITIONS.

   a. Safeguards and Security Survey. An integrated performance and compliance based evaluation of all applicable topics to determine the overall status of the S&S program at a facility or site and to ensure that S&S systems and processes at the location are operating in compliance with Departmental and national-level policies, requirements, and standards. Surveys are conducted or supervised by Federal security personnel.

   b. Initial Survey. A comprehensive review of the security status at a facility that is a candidate for an FCL, conducted to determine whether the facility in question meets established standards for the protection of the security interests and activities to be covered by the FCL.

   c. Periodic Survey. A survey conducted for all cleared facilities in accordance with established schedules that covers all applicable topics to meet the objectives of the S&S survey.

   d. Termination Survey. A survey of a cleared facility conducted to verify the termination of Departmental activities and the appropriate disposition of S&S interests at that facility. The termination survey confirms that all S&S activities have been terminated or awarded to another contractor, that access authorizations have been properly terminated or dispositioned, and that no DOE property, classified information or matter, and nuclear and other hazardous material presenting a potential radiological or toxicological sabotage threat remains.

e. Self-Assessment. An internal integrated evaluation of all applicable S&S topical areas at a contractor facility or site, conducted by contractor security personnel at intervals consistent with risk management principles, to determine the overall status of the S&S program at that location and verify that S&S objectives are met. The DOE cognizant security office may direct a specific self-assessment interval and may direct that self assessment reports be provided to DOE.

f. Finding. A factual statement of identified issues and deficiencies (failure to meet a documented legal, regulatory, performance, compliance, or other applicable requirement) in the S&S program at a facility, resulting from an inspection, survey, self-assessment, or any other S&S review activity.

4. REFERENCES.

a. E.O. 13526, *Classified National Security Information*, dated 12-29-09.

b. E.O. 12829, *National Industrial Security Program*, dated 01-26-93.

c. DoD 5220.22-R, *Industrial Security Regulation*.

d. DoD 5220.22-M, *National Industrial Security Program Operating Manual (NISPOM)*.

e. DoD Defense Security Service (DSS) Industrial Security Letters (ISLs), available at http://www.dss.mil/isp/fac_clear/download_nispom.html (Note: ISLs do not automatically impose requirements, but may contain useful clarifications of existing NISPOM provisions.).

f. 10 CFR Part 1016, *Safeguarding of Restricted Data*.

g. 10 CFR Part 824, *Procedural Rules for the Assessment of Civil Penalties for Classified Information Security Violations*.

h. 32 CFR Part 2001, *Classified National Security Information*.

i. 48 CFR Chapter 9, *Department of Energy Acquisition Regulation*.

j. DOE P 226.1B, *Department of Energy Oversight Policy, dated 4-25-11*.

k. DOE O 226.1B, *Implementation of Department of Energy Oversight Policy*, dated 4-25-11.

l. DOE O 475.1, *Counterintelligence Program*, dated 10-04-04.

5. REQUIREMENTS. DOE cognizant security offices, as designated by the Program Secretarial Office, or for NNSA, the Office of the Administrator through the Chief, Defense Nuclear Security, are responsible for ensuring that the following activities are

accomplished for the surveys and self-assessments program for facilities and sites under their cognizance and for ensuring that contractors under their cognizance accomplish their responsibilities under this program at contractor facilities. Procedures applicable to the surveys and self-assessments program must be documented in facility or site security plans. Identified interfaces and integration with the contractor assurance system must also be documented in facility or site security plans.

a. Establish and maintain a schedule for conducting surveys in accordance with applicable national and DOE policy standards.

b. Ensure that surveys are conducted as scheduled and/or as required for security activities such as the granting or termination of an FCL.

c. Ensure that contractors issued an FCL review their security programs on a continuing basis and conduct formal self-assessments at intervals consistent with risk management principles.

d. Ensure that contractors under their cognizance prepare formal reports of self-assessments and related findings and corrective actions.

e. Advise contractors under their cognizance of the appropriateness of the self-assessment and its expected coverage and use.

f. Provide an evaluation of contractor self-assessment processes and recommend changes as necessary to ensure that DOE objectives are met.

g. Ensure that both surveys and contractor self-assessments evaluate all S&S topics relating to Program Management Operations, Physical Protection, Protective Force, Information Security, Personnel Security, and Materials Control and Accountability that are applicable at the facility/site being surveyed.

h. Ensure that all findings identified during surveys and self-assessments are tracked until the issues are resolved.

i. Ensure that the results of surveys are reported in the DOE Safeguards and Security Information Management System (SSIMS).

j. Ensure that corrective actions for issues identified in surveys and self-assessments are implemented in a timely and effective manner, and validate the effectiveness of corrective actions to prevent recurrence of the issues.

6. SURVEYS. Surveys are conducted to confirm that a Federal or contractor facility meets all security requirements appropriate to the activities conducted at that facility, to inform Federal line management of the effectiveness of the facility security program, to identify any issues or concerns with the security program so that these can be addressed and corrected, and to allow both contractor and Federal managers to manage risk in an informed and rational manner.

a. Initial Surveys. A favorable survey is required as one of the conditions for granting a facility security clearance. This initial survey must be completed not more than 6 months prior to the granting of the FCL if the facility will possess classified information or matter or SNM, or will have a facility importance rating of "PP".

b. Periodic Surveys. Periodic surveys must be conducted for all cleared facilities to ensure that S&S measures employed by the facility are adequate for the protection of security assets and interests. The National Industrial Security Program specifies that surveys of contractor facilities will be conducted not more often than once every 12 months unless special circumstances exist. 32 CFR Part 2001.60 establishes a requirement for an annual survey specifically for the assessment of activities related to classified information. At the discretion of the DOE cognizant security office, other topics may be combined with this requirement to meet the periodic survey requirement. For facilities which do not have classified interests or SNM, the frequency of the periodic survey may be established consistent with risk management principles and documented in the applicable security plan with a description of the reasons for the schedule (e.g., good performance on past surveys and self-assessments, regular satisfactory performance assurance testing, non-possessing facilities, etc.).

c. Termination Surveys. When a contract for which an FCL has been granted is terminated or otherwise ended (e.g., suspended), a termination survey must be conducted to verify the termination of security activities and the appropriate disposition of S&S interests. Examples of survey activities include: the appropriate disposition, destruction, or return of classified information or matter, SNM, hazardous material, or property; the signing of a certificate of possession if classified is to be retained by the contractor for the allowable period; security badge retrieval; verification of debriefings or verification of the transfer of access authorizations to other DOE interests. Surveys must be conducted onsite at facilities possessing Top Secret classified information or matter, Restricted Data, Sensitive Compartmented Information or special access program information or matter, or SNM. For all other facilities, termination surveys may be conducted either onsite or through any other means established by the cognizant security office.

7. SELF-ASSESSMENTS. Self-assessments are conducted by contractors at their facilities to ensure that at any point the facility is in compliance with all security requirements appropriate to the activities, information, and conditions at the location. Assessments are conducted at intervals consistent with risk management principles and/or as directed by the DOE cognizant security office, and reports are provided to that office. Federal facilities are not required to conduct self-assessments in addition to surveys under this Order.

8. REPORTS AND RATINGS. For each rated area, the survey report must contain a description of each element reviewed, how the review was conducted including any

samples and tests used in the evaluation, a summary of the observations made, and an analysis of the results that support the ratings awarded. Ratings must be based upon the effectiveness and adequacy of the security programs at the subject facility. The ratings listed below must be used for all surveys, self-assessments, and reviews. When a topic does not apply at a given facility, or if a topic is not rated, the survey report must contain this information. All ratings must be supported and documented with the rating justification and rationale.

a. Satisfactory. The element being evaluated meets protection objectives or provides reasonable assurance that protection objectives are being met.

b. Marginal. The element being evaluated partially meets protection objectives or provides questionable assurance that protection objectives are being met.

c. Unsatisfactory. The element being evaluated does not meet protection objectives or does not provide adequate assurance that protection objectives are being met.

9. FINDINGS AND CORRECTIVE ACTIONS.

a. All open S&S findings from any source (previous surveys and assessments; inspections, reviews, and reports by other organizations such as the Government Accountability Office or the Office of the Inspector General; etc.) must be reviewed during surveys to validate the status of corrective actions and to evaluate the impact on the current operation of the facility's S&S program. Findings closed during the survey period must be reviewed for sustainability of the closing action.

b. Findings from all surveys must be documented in the associated report and entered into SSIMS in accordance with guidelines issued by the SSIMS database manager. Findings must be tracked until closed and monitored on an established schedule to ensure that corrective action plans to address the issue are being implemented in a timely and effective manner. Trending assessment activities based on findings must be conducted to establish if findings represent an isolated issue or a systemic problem with a specific topical element or with the S&S program as a whole.

c. Corrective action plans must be developed for all open survey findings. For all identified findings, corrective actions must be implemented in a timely and effective manner. The effectiveness of corrective actions must be validated during subsequent surveys to ensure that the action taken has been sufficient to prevent recurrence of the issue that resulted in the finding. Corrective actions must be reported in SSIMS and the current status of the action must be reported in SSIMS until the associated finding is closed.

10. DOCUMENTATION. Reports of surveys, self-assessments, and review activities must be maintained in accordance with *DOE Administrative Records Schedule 18*, paragraphs 9 and 10.

APPENDIX B. SAFEGUARDS AND SECURITY PROGRAM MANAGEMENT OPERATIONS

This appendix establishes the U.S. Department of Energy (DOE) requirements for conducting management activities connected with the operation of cleared facilities within the DOE complex. Section 1 addresses obtaining a facility clearance (FCL) and establishing the safeguards and security (S&S) activities connected with that facility. Section 2 covers the foreign ownership, control, or influence determinations that are necessary to establish and maintain a facility clearance. Section 3 covers security awareness activities, including required personnel briefings. Section 4 addresses the handling of classified visits to and from DOE facilities, including foreign classified visits. Section 5 deals with S&S training to be provided for employees at cleared facilities. Section 6 covers restrictions imposed on the transfer of security funded technologies outside the United States.

SECTION 1. FACILITY CLEARANCES AND REGISTRATION OF SAFEGUARDS AND SECURITY ACTIVITIES

1. OBJECTIVE. To ensure that DOE, DOE contractor, and other (Federal) government agency (OGA) facilities and their contractors engaged in DOE activities are eligible for access to, and meet the requirements to possess and secure, classified information or matter or special nuclear material (SNM); and, as applicable, to protect other assets and conduct other security activities on behalf of DOE.

2. PURPOSE. The FCL program regulates DOE approval of a Federal or contractor facility's eligibility to access, receive, generate, reproduce, store, transmit, or destroy classified information or matter; SNM; other hazardous material presenting a potential radiological, chemical, or biological sabotage threat; and/or DOE property of significant monetary value, exclusive of facilities and land values (hereinafter referred to as security assets and activities). DoD 5220.22-M, *National Industrial Security Program Operating Manual (NISPOM),* serves as a national standard to establish the baseline requirements for contractor FCLs when contractors are engaged in activities requiring the protection of national security information classified at the Confidential, Secret, or Top Secret level. The NISPOM requirements are incorporated in this directive and are supplemented with requirements for the protection of DOE-specific assets, Restricted Data, SNM, and other security activities not covered by the NISPOM.

3. FACILITY DEFINITION. For purposes of granting and registering an FCL code under this program, an entity (contractor or Federal) and its classified or high value security activities will be registered with one FCL code if the following criteria are met:

   a. A centrally directed security program is maintained that covers all security activities (i.e., under the same name, single mailing address, single security plan applicable at all locations, and all security matters under single management control).

   b. The distance between the security activities is such that the contractor or Federal entity is able to maintain daily supervision of its operations, including day-to-day observations of the security program.

4. REFERENCES.

   a. E.O. 12829, *National Industrial Security Program*, dated 01-26-93.

   b. E.O. 13549, *Classified National Security Information Program for State, Local, Tribal, and Private Sector Entities*, dated 8-18-10.

   c. 42 U.S.C. Sections 2011 through 2296, *Atomic Energy Act of 1954*.

   d. 32 CFR Part 2001, *Classified National Security Information*.

e. 32 CFR Part 2004, *National Industrial Security Program Directive No. 1*.

f. 10 CFR Part 1016, *Safeguarding of Restricted Data*.

g. 10 CFR Part 1045, *Nuclear Classification and Declassification*.

h. DoD 5220.22-R, *Industrial Security Regulation*.

i. DoD 5220.22-M, *National Industrial Security Program Operating Manual (NISPOM)*.

j. DoD Defense Security Service (DSS) Industrial Security Letters (ISLs), available at http://www.dss.mil/isp/fac_clear/download_nispom.html (Note: ISLs do not automatically impose requirements, but may contain useful clarifications of existing NISPOM provisions.)

k. Directive-Type Memoranda (DTM) issued by the Office of the Under Secretary of Defense, (e.g., DTM 09-019, "Policy Guidance for Foreign Ownership, Control, or Influence (FOCI" available at http://www.dtic.mil/whs/directives/corres/dir3.html. Note: DTMs, which may be issued periodically on a variety of topics, do not automatically impose requirements, but may contains useful information applicable to existing NISP programs.)

l. 10 U.S.C. Section 2536, *Award of certain contracts to entities controlled by a foreign government: prohibition.*

m. 48 CFR Chapter 9, *Department of Energy Acquisition Regulation*.

n. DOE O 475.2A, *Identifying Classified Information*, dated 2-1-11.

5. REQUIREMENTS. DOE cognizant security offices, as designated by the Program Secretarial Office, or for NNSA, the Office of the Administrator through the Chief, Defense Nuclear Security, are responsible for ensuring that the following activities are accomplished for the FCL program for facilities and sites under their cognizance and for ensuring that contractors under their cognizance accomplish their responsibilities under this program at contractor facilities. Procedures applicable to the FCL program must be documented in facility or site security plans.

a. Establish and maintain FCLs by registering, updating, suspending, reinstating, and terminating FCLs and related security activities under their cognizance in accordance with the requirements contained in this Order.

b. Ensure that organizations seeking FCLs meet all the eligibility requirements applicable to the type of organization prior to being processed for an FCL.

c. Ensure that all items required by the DEAR as the basis for approval of a contractor FCL have been completed and favorably adjudicated/approved prior to granting the final FCL.

d. Ensure that accurate facility importance ratings are assigned and that ratings are updated as necessary to reflect changes in security activities.

e. Establish and apply procedures to ensure that coordination is accomplished between the FCL and Foreign Ownership, Control, or Influence (FOCI) programs for all contractor FCLs.

f. Determine on a case-by-case basis the necessity for branch offices of a multiple-facility organization to be cleared, based upon the performance of security activities.

g. Determine the necessity for the corporate tier parent in a parent-subsidiary relationship to be excluded or cleared as a possessing or non-possessing facility.

h. Ensure that prime contractors have appropriately implemented provisions pertaining to subcontractors and that all subcontractors are processed for FCLs when required and terminated or transferred to the cognizance of a new management and operations contractor as appropriate.

i. Ensure that all key management personnel (KMP) are properly identified, processed for, and granted access authorizations at the appropriate level or are formally excluded from access, duties, and influence that would otherwise cause them to be identified as KMP prior to granting a final FCL.

j. Ensure that procedures are in place to verify changes in an organization's KMP as they occur and that access authorizations are immediately processed for new KMP.

k. Receive and evaluate contractor reports of changes that may impact the FCL, and take any necessary action to suspend or terminate the FCL if such action is warranted.

l. Notify the appropriate DOE contracting officer, the contractor, and/or the Federal entity applying for or holding an FCL in writing of the level of FCL granted.

m. In conjunction with the responsible surveying offices, as identified by DOE Federal management, ensure that the S&S Information Management System (SSIMS) database accurately reflects established facilities, security assets, and activities under their jurisdiction; ensure that updates and changes to such information are recorded in SSIMS immediately; and ensure that accurate forms are submitted for this purpose.

n. When a contract ends and/or an FCL is no longer necessary, complete a termination survey and ensure that appropriate forms are submitted and SSIMS is updated to enact the termination.

o. Ensure that upon termination of a contract, all security clearances (access authorizations) connected to the FCL are terminated and all DOE property; classified information; and/or nuclear and other hazardous material presenting a potential radiological, chemical or biological sabotage threat is appropriately reallocated, disposed of, destroyed, or returned to an appropriate DOE or cleared DOE contractor organization.

CHAPTER I. FACILITY CLEARANCE PROGRAM

1. GENERAL.

a. Facilities Eligible for the FCL Program.

(1) An industrial, educational, commercial, or other contractor entity will require an FCL if the terms of a contract awarded under the DEAR include the security activities described in paragraph 2 of Section 1 above. A contractor requiring an FCL must be sponsored by:

(a) a Government Contracting Activity (GCA; i.e., a contracting officer); or

(b) a cleared contractor acting as the prime contractor for an uncleared subcontractor. A contractor cannot sponsor itself for an FCL.

(2) OGAs may be registered as having a DOE FCL when a mission or programmatic need for such an action has been established by DOE line management. Verification of the clearance and security capability of an OGA must be based on a written statement of security assurance from that agency submitted to the DOE cognizant security office. State, local, tribal, and other similar governmental authorities do not have authority to self-certify clearance and security capability for handling classified information; therefore, they must not be registered as OGAs. These entities must be handled in accordance with E.O. 13549, *Classified National Security Information Program for State, Local, Tribal, and Private Sector Entities*, and its implementing directives.

(3) DOE Federal facilities are registered with a facility code under the FCL program and are subject to survey requirements.

b. In accordance with the DEAR, section 952.204-2(l), FCLs are required for subcontractors requiring personnel security clearances. The prime contractor is responsible for implementation of the provisions of DoD 5220.22-M, N*ational Industrial Security Program Operating Manual (NISPOM)* (Chapter 7, "Subcontracting"), all DOE security requirements for their subcontractors, and for termination of the subcontracts upon completion of activities. Prime contractors must ensure that all subcontracts are terminated if the prime contract is terminated, or for management and operations subcontracts, transferred to the cognizance of the new management and operations contractor as appropriate.

c. All company officials who occupy positions with the authority to affect the organization's policies or practices in security activities conducted under the contract, as determined by the DOE cognizant security office, must be designated

as KMP. As a minimum, KMP must include the senior management official responsible for all aspects of contract performance and the designated facility security officer (FSO). KMP must be in process for or possess active security clearances in order for a contractor to be eligible for an FCL involving classified information or matter, or SNM. Until all investigative requirements have been completed and final security clearances have been granted to the designated KMP, only an interim facility clearance can be granted.

d. In accordance with the DEAR, section 952.204-73(e), a contractor that will not possess or handle classified information or matter, or SNM, at the contractor's place of business but will require DOE personnel security clearances for the contractor's employees to perform work at other cleared facilities must be processed for an FCL as a non-possessing facility. Employees of a non-possessing contractor must adhere to the security plans of the facilities where they are afforded access to classified information or matter, or SNM.

e. A self-employed individual not doing business as a company, or a consultant who will not retain classified information or matter at his/her place of business, does not require an FCL provided the individual or consultant is the sole employee requiring a security clearance. For security administration activities, to include processing for a personnel security clearance, the individual will be considered an employee of the possessing facility where he/she is afforded access to classified information or matter. These individuals are required to complete the same security awareness briefings and requirements as other cleared employees. A self-employed individual or consultant who will retain classified information or matter at their place of business must be processed for and granted an FCL that applies to the premises where the individual or consultant will store, handle, or process classified information or matter.

f. For Multiple Facility Organizations (MFOs), the home office facility must have an FCL at the same or higher level as that of any cleared facility within the MFO.

g. In a corporate tier parent-subsidiary relationship, the parent and each of its subsidiaries are separate legal entities and must be processed separately for an FCL. Because the parent controls the subsidiary, the general rule in the U.S. Government is that the parent must have an FCL at the same or higher level as that of the subsidiary. However, DOE will determine the necessity for the parent to be cleared or excluded from access. DOE will advise the companies as to what action is necessary for processing the FCL. When a parent or its cleared subsidiaries are collocated, a formal written agreement to use common security services may be executed by the two firms, subject to DOE approval.

h. A contractor granted an FCL by an OGA may be granted a DOE FCL for receiving, processing, using, or storing classified information or matter under a DOE contract at the same clearance level, based on reciprocity.

2. ELIGIBILITY REQUIREMENTS. The following eligibility requirements must be met prior to being processed for an FCL.

a. A contractor or prospective contractor must:

(1) Be selected to perform tasks under a contract containing the DEAR security clauses found at 48 CFR Part 952;

(2) Be organized under the laws of one of the 50 States, the District of Columbia, or Puerto Rico and must be located in the United States or a U.S. territorial area or possession;

(3) Have a reputation for integrity and lawful conduct in its business dealings;

(4) Not have been barred from participating in U.S. Government contracts (this includes KMP on the contract); and

(5) Not be under FOCI to a degree that the granting or continuation of the FCL would be inconsistent with the national interest.

b. An OGA must:

(1) Have a documented need for an FCL as established in writing by DOE line management;

(2) Submit a written statement of security assurance to the DOE cognizant security office, verifying the security capability of the agency as it applies to the DOE activity; and

(3) When Restricted Data (RD) or Formerly Restricted Data (FRD) is involved, include in the written statement of security assurance procedures to limit the manner in which the RD or FRD is to be disseminated and ensure that appropriate clearances for access to RD or FRD are in place.

c. For DOE facilities, cognizant security offices for DOE Federal activities must establish and document a security plan describing an adequate level of protection for DOE security interests.

CHAPTER II. IMPORTANCE RATINGS

1. FACILITY IMPORTANCE RATINGS. Importance ratings are used to establish a risk-based system for identifying the level of protection applicable to security assets and activities of facilities. Each facility granted an FCL must be assigned an importance rating. Each facility's assigned importance rating must be recorded on DOE F 470.2, *Facility Data and Approval Record (FDAR)*. Importance rating criteria are as follows.

   a. "A" Importance Ratings. An "A" importance rating must be assigned to those facilities that meet any of the following criteria:

      (1) Engaged in administrative activities considered essential to the direction and continuity of the overall DOE nuclear weapons program, as determined by the Program Secretarial Office or for NNSA, the Office of the Administrator;

      (2) Authorized to possess Top Secret RD/FRD or Top Secret national security information, or possess Special Access Program (SAP) matter, or designated as Field Intelligence Elements;

      (3) Authorized to possess Category I quantities of SNM (including facilities with credible rollup quantities of SNM to a Category I quantity); or

      (4) Operate critical infrastructure programs determined to be essential by DOE line management.

   b. "B" Importance Ratings. A "B" importance rating must be assigned to those facilities that meet any of the following criteria:

      (1) Engaged in activities other than those categorized as "A" and authorized to possess Secret RD and/or weapon data matter;

      (2) Authorized to possess Category II quantities of SNM; or

      (3) Authorized to possess certain categories of biological agents.

   c. "C" Importance Ratings. A "C" importance rating must be assigned to those facilities that meet any of the following criteria:

      (1) Authorized to possess Categories III and IV quantities of SNM or other nuclear materials requiring safeguards controls or special accounting procedures; or

      (2) Authorized to possess classified information or matter other than the type categorized for "A" and "B" facilities.

d. "D" Importance Ratings. A "D" importance rating must be assigned to those facilities that provide common carrier, commercial carrier, or mail service and are not authorized to store classified information or matter, or nuclear material during non-working hours. (Carriers who store classified information or matter, or nuclear material must be assigned an "A," "B," or "C" importance rating.)

e. "E" (Excluded Parent) Importance Ratings. An "E" importance rating must be assigned to a corporate tier parent of a contractor organization when the parent has been barred from participation in the activities related to a contract with DOE.

f. "PP" (Property Protection) Importance Ratings. A "PP" importance rating must be assigned to those facilities that meet any of the following criteria:

(1) Government property of a significant monetary value (suggested threshold of $5 million);

(2) Nuclear materials requiring safeguards controls or special accounting procedures other than those categorized as types "A," "B," or "C";

(3) Responsibility for DOE program continuity;

(4) National security considerations; or

(5) Responsibilities for protection of the health and safety of the public and employees.

g. "NP" (Non-Possessing) Importance Ratings. An "NP" rating must be assigned to those facilities whose staff have authorized access to classified information or matter, or SNM at other approved locations, but which do not themselves possess any classified information or matter, or SNM, or meet any of the other criteria listed for the other ratings above.

2. UPGRADING AND DOWNGRADING A FACILITY'S ASSIGNED IMPORTANCE RATING. As security activities are added or changed, the importance rating of the approved facility may change (i.e., it may be either upgraded or downgraded). Upgrading or downgrading a facility's importance rating may also require transfer of the DOE cognizant security office functions. Changes to the facility importance rating must be registered in SSIMS by the submission of DOE F 470.2, *Facility Data and Approval Record (FDAR).*

CHAPTER III. FACILITY CLEARANCE APPROVAL REQUIREMENTS

1. ISSUANCE OF FCLs. All eligibility requirements listed below must be satisfied prior to the issuance of an FCL. The DEAR prohibits the award of a classified contract until an FCL has been granted and issued. When an existing unclassified contract is modified to require classified work, the contract modification cannot take effect until an FCL is issued and the appropriate DEAR security clause is inserted in the contract.

2. CONTRACTOR FACILITIES. In accordance with the provisions of the DEAR, approval of a contractor final FCL must be based on the following items:

   a. A favorable FOCI determination based upon all information available to the cognizant security office including information on Standard Form (SF) 328 and any required supporting documentation;

   b. A contract or proposed contract containing the appropriate security clauses found in the DEAR;

   c. S&S plans, developed in accordance with DOE policy in Attachment 2 of this Order, that describe protective measures appropriate to the activities being performed at the facility and approved by the DOE cognizant security office;

   d. If access to nuclear material is involved, an established Reporting Identification Symbol code for the Nuclear Materials Management and Safeguards Reporting System (NMMSS);

   e. A comprehensive survey conducted no more than 6 months before the FCL approval date with a composite facility rating of satisfactory, if the facility will possess classified information or special nuclear material at its location or if the facility has an importance rating of "PP";

   f. Appointment of an FSO, who must possess or be in the process of obtaining an access authorization (security clearance) equivalent to the level of the facility clearance (note that only an interim FCL can be granted until the FSO's access authorization is finalized);

   g. If applicable, appointment of a Materials Control and Accountability Representative; and

   h. Access authorizations for KMP who will be determined on a case-by-case basis and must possess or be in the process of obtaining access authorizations equivalent to the level of the facility clearance. (NOTE: until the required KMP access authorizations are finalized, only an interim FCL can be granted.)

3. FACILITY CLEARANCES FOR OGAs. Federal government facilities are eligible to be registered with a DOE FCL if the OGA is involved in activities that impact DOE security

interests such as possession and/or storage of RD or other mission or programmatic needs as identified and documented by DOE line management. Approval of an OGA FCL must be based upon a written statement of security assurance from the OGA that protection of DOE security interests is adequately ensured. The statement of security interest must include the following information:

a. An approved classified mailing address for the facility;

b. The highest level and most restrictive category of classified information the facility is authorized to receive and store;

c. A statement that national security classified information will be afforded protection according to E.O. 13526, *Classified National Security Information*, and all implementing directives issued by the Information Security Oversight Office (ISOO), to include the requirements of 32 CFR Part 2001, *Classified National Security Information*;

d. A statement that the requirements of 10 CFR Part 1045, *Nuclear Classification and Declassification*, will be met for RD and FRD; and

e. Assurance that the requirements of the Atomic Energy Act, including the mandatory access authorization requirements, will be met for access to RD and FRD.

4. RECORDS. For DOE Federal and contractor facilities, the DOE cognizant security office must maintain a copy of the facility's S&S plans, survey reports, FOCI documentation including notification of a favorable FOCI determination if applicable, pertinent correspondence, and copies of DOE F 470.2, *Facility Data and Approval Record (FDAR)*, created for the facility. For FCL termination of all registered facilities, a copy of the certificate of non-possession or security certification must be maintained.

CHAPTER IV. INTERIM AND LIMITED FACILITY CLEARANCES

1. INTERIM FCLs. Interim FCLs are granted on a temporary basis, pending completion of full investigative and approval requirements, including but not limited to the completion of background investigations for final access authorizations for those individuals required to be cleared in connection with the FCL (such as KMP). Interim FCLs may be granted only to avoid unacceptable delays in pre-contract negotiation or in performance on a contract, and must be granted only after DOE has made a FOCI determination and granted interim access authorizations to KMP and other facility personnel requiring immediate access to classified information or matter.

   a. When final access authorizations have been granted to all facility employees, a final FCL must be granted and registered in SSIMS via an updated DOE F 470.2, *Facility Data and Approval Record (FDAR).*

   b. When an interim access authorization for an individual KMP is withdrawn, the interim FCL must also be withdrawn unless action is taken to remove the individual from the position requiring access.

   c. Foreign owned or controlled companies and those with non-U.S. citizens as KMP are not eligible for interim FCLs.

2. LIMITED FCLs. The United States has entered into agreements with certain foreign governments that establish arrangements whereby a foreign-owned U.S. company may be considered eligible for an FCL without any additional FOCI negation or mitigation instrument. To ensure that release of information or access to SNM is in accordance with the U.S. National Disclosure Policy, a limited FCL must be restricted to one security activity involving classified information or SNM. Award of another security activity to the same facility involving such information requires separate FCL registration, under another limited FCL or under an FCL without restrictions, if appropriate. Issuance of a limited FCL requires imposing strict access restrictions to limit access to the scope of the contract. The clearance and exclusion requirements for KMP apply to all FCLs, including a limited FCL.

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

      (1) Verification of an agreement authorizing the exchange of the classified information or matter involved to the country from which the foreign ownership is derived.

         (a) Access to classified information or matter will be limited to performance on a contract, subcontract, or program involving the government of the country from which foreign ownership is derived.

(b) Release of classified information or matter must be in conformity with the U.S. National Disclosure Policy.

(2) In extraordinary circumstances, a limited FCL may also be granted when the criteria listed above cannot be satisfied, provided there exists a compelling need to do so consistent with national security interests.

b. Limited FCL Compelling Need Statement. Each request for clearance under a limited FCL must be accompanied by a statement of compelling need from the GCA. The GCA's compelling need statement must be signed by the head of the cognizant DOE program office and include the following:

(1) Acknowledgment that the company will be under FOCI (i.e., FOCI will not be mitigated);

(2) Acknowledgment that the GCA/Departmental element accepts the risks inherent in the granting of an FCL where FOCI is not mitigated; and

(3) A foreign disclosure determination stating the basis for determining that release of classified to the foreign government involved is in conformity with U.S. National Disclosure Policy.

CHAPTER V. PERSONNEL SECURITY CLEARANCES AND EXCLUSION PROCEDURES REQUIRED IN CONNECTION WITH CONTRACTOR FACILITY CLEARANCES

1. SECURITY CLEARANCES REQUIRED IN CONNECTION WITH THE FCL. Certain officials (typically the owners, officers, directors, partners, regents, trustees, and/or executive personnel [KMP]) with the ability to affect the organization's policies or practices in security activities conducted under the contract must be cleared to the level of the FCL or formally excluded from access as appropriate. For multiple facility organizations, each subordinate cleared facility's KMP must also be cleared or excluded. Changes in an organization's KMP must be reported as they occur, and access authorizations must be processed for new KMP immediately.

2. EXCLUSION PROCEDURES. When officials are to be excluded from or cleared at a level not commensurate with the FCL, compliance with one or both of the exclusion actions listed below is mandatory before issuance of an FCL. Exclusion actions must be made a matter of record by the organization's executive body. A copy of the resolution must be provided to the DOE cognizant security office.

   a. When formal exclusion action is required, the organization's governing body must affirm that specific KMP (designated by name) will not require, will not have, and can be effectively excluded from access to all classified information or matter, or nuclear or other hazardous material presenting a potential radiological, chemical, or biological sabotage threat, that is entrusted to or held by the organization. Additionally, the governing body must affirm that the specific KMP (designated by name) do not occupy positions that would enable them to adversely affect the organization's policies or practices in the performance of classified contracts.

   b. When officials are to be cleared at a level below that of the FCL, the organization's governing body must affirm that such KMP (designated by name) will not require, will not have, and can be effectively denied access to higher-level classified information (specified by level), and do not occupy positions that would enable them to adversely affect the organization's policies or practices in the performance of higher-level classified contracts.

3. SECURITY CLEARANCES CONCURRENT WITH THE FCL. Contractors may designate employees who require access to classified information or matter during the negotiation of a contract or the preparation of a bid or quotation pertaining to a prime contract or a subcontract to be processed for security clearances concurrent with the FCL. The granting of an FCL is not dependent on the security clearance of such employees.

CHAPTER VI. FACILITY CLEARANCES GRANTED BY OTHER GOVERNMENT AGENCIES

1. ACCEPTING OGA FCLs.

a. General. A contractor with an equal or higher FCL granted by another Federal government agency under the National Industrial Security Program (NISP) may be accepted by DOE for accessing, receiving, generating, reproducing, storing, transmitting, or destroying classified information or matter, contingent on the conditions listed below. Reciprocity between DOE and the OGA must be documented in a written letter or memorandum of agreement (MOA) between the DOE cognizant security office and the cognizant OGA that establishes the responsibilities of each party for assurance and verification of the protection afforded the DOE assets.

(1) Classification Level/Category and Special Conditions. The FCL granted by the OGA must be at the appropriate classification level and category and must encompass the DOE activity.

(a) Limited or interim FCLs granted by an OGA cannot be accepted.

(b) If cleared under a Voting Trust Agreement, Proxy Agreement, Special Security Agreement, or Security Control Agreement, the DOE cognizant security office must obtain a copy of the FOCI mitigation plan from the cognizant OGA. The mitigation plan must be submitted to the DOE Office of Health, Safety and Security or, for NNSA activities, to the Office of Defense Nuclear Security, for review.

(c) For DOE contracts involving proscribed information (i.e., Top Secret, COMSEC, RD/FRD), the following requirements, as appropriate, must be met before accepting an FCL granted in conjunction with a Special Security Agreement or Security Control Agreement.

1 When the company is controlled by a foreign government:

a DOE must have entered into an agreement with the foreign government involved that covers the proscribed information to be released under the contract; and

b A waiver must be granted by the cognizant Secretary (i.e., the Secretary of Energy and/or the Secretary of Defense) in accordance with the

provisions of 10 U.S.C. Section 2536, *Award of certain contracts to entities controlled by a foreign government: prohibition*, which prohibits contract awards involving proscribed information to foreign government-controlled companies unless such a waiver is granted.

2 When a company is not controlled by a foreign government a national interest determination (NID) for the specific program/project/contract must be approved by DOE and/or the OGA as appropriate.

3 For contracts involving RD/FRD, the additional requirements set forth below in paragraphs (6)(a)–(d) must be met or addressed as appropriate.

(d) An OGA Top Secret facility clearance transfers to a DOE Secret/RD possessing interest, and an OGA Secret facility clearance transfers to a DOE Secret/RD non-possessing interest as long as DOE grants the security clearances to KMPs and all individuals requiring access to Secret/RD under the DOE contract(s).

(e) Final FCLs granted by OGAs for access to national security information (NSI), when no proscribed information is involved, will be accepted by DOE on a reciprocal basis with no additional requirements.

(2) Notification of Cancellation. An assurance must be obtained from the OGA that the FCL will not be canceled prior to the DOE cognizant security office being notified.

(3) Protective Measures. Confirmation must be obtained from the OGA that the facility's protective measures and procedures are adequate for the protection of the DOE activity, and results of the agency's last survey of the facility are satisfactory in those areas that could affect the DOE interest.

(4) Surveys. The facility's survey frequency must be confirmed by the OGA, and assurance must be obtained that copies of each of the OGA's periodic survey reports or memoranda covering the status of the protection of the DOE activity will be furnished to the DOE cognizant security office following each scheduled survey.

(5) Access authorizations. Each employee to be granted access to RD or SNM must have an appropriate access authorization.

(6) RD/FRD. If RD or FRD is involved, the following must be considered:

(a) An assurance must be obtained from the OGA that the facility complies with the requirements of 10 CFR Part 1045, *Nuclear Classification and Declassification*.

(b) When the DOE contract involves RD, an assurance must be obtained from the OGA that the facility's protective measures and procedures meet the requirements of DoD 5220.22-M, N*ational Industrial Security Program Operating Manual (NISPOM)*, including any appendices or supplements applicable to RD.

(c) FCLs not meeting the requirements in (a) and (b) above may be accepted if the DOE activity requires that the contractor establish upgraded protective measures that meet DOE requirements. For FCL upgrades, the agreement between DOE and the OGA must cover reimbursement for upgrade costs incurred by the OGA or contractor.

(d) When DOE accepts an FCL based on an OGA-approved Voting Trust Agreement, Proxy Agreement, Special Security Agreement, or Security Control Agreement, an assurance must be obtained from the OGA that it will invite and permit DOE to attend the annual meeting if such attendance is determined necessary by either the OGA or DOE.

b. Contractor's Tier Parent(s). If the parent(s) of a company that DOE is processing for an FCL holds an FCL granted by another Federal agency, the tier parent(s) does not need to provide DOE with a FOCI package, provided reciprocity is accomplished with the OGA. Reciprocity between the DOE cognizant security office and the OGA must be documented in a written agreement with the appropriate provisions as outlined above. The written agreement must contain an assurance from the OGA that security cognizance will be transferred to DOE for any tier parent no longer requiring the OGA FCL.

2. OGA VERIFICATION REQUESTS. If an OGA requests verification of an existing DOE FCL, a copy of the facility's current DOE F 470.2, *Facility Data and Approval Record (FDAR),* must be provided.

3. OGA CONTRACTORS WITH NO DOE CONTRACTS. Classified mail channels must be registered in SSIMS for an OGA contractor organization where the Department does not have a contractual interest but must communicate or exchange classified information with the OGA contractor. To establish an address for the classified mail channel, a statement of security assurance or a form comparable in content must be completed and signed by the DOE cognizant security office and by the authorizing government official

for the OGA contractor. The establishment of this type of registration in SSIMS cannot be used as a basis for registering additional security activities.

CHAPTER VII. DOCUMENTATION AND REGISTRATION OF FACILITY CLEARANCES AND RELATED SECURITY ACTIVITIES

1. DOCUMENTATION OF FCLs. SSIMS must be used by all DOE cognizant security offices to register FCL information for which they have cognizant security authority, survey cognizance, or responsibility for registered security activities. Each registered FCL must identify the highest security activity approved for the registered facility.

   a. DOE F 470.1, *Contract Security Classification Specification (CSCS)*, is used to register information in SSIMS concerning contract vehicles; a DD 254 used by an OGA sponsoring an activity can be submitted in lieu of the DOE F 470.1 if it is annotated with the DOE facility code. DOE F 470.2, *Facility Data and Approval Record (FDAR)*, is used to record approvals, changes, and deletions of facility security information and other facility changes for entry into SSIMS. These forms are available on the website of the DOE Office of the Chief Information Officer (http://cio.energy.gov/records-management/forms.htm).

   b. If more than one Departmental element has a registered security activity at a facility, the element responsible for the security activity involving the highest classification level and category is the responsible DOE cognizant security office, to include being the processing personnel security office. This responsibility may be delegated, by mutual agreement, to another Departmental element with a registered security activity at that facility. The Special Security Officer, Office of Intelligence and Counterintelligence, must also sign the DOE F 470.1 for contracts involving access to Sensitive Compartmented Information.

   c. Any change in the responsible DOE cognizant security office or survey office must include a transfer of appropriate documentation (e.g., S&S plans; construction project status; FOCI files; etc.).

2. REGISTRATION OF SECURITY ACTIVITIES. Security activities are specific, unrelated tasks or contract elements involving S&S interests at a facility. Security activities must be registered in association with a specific FCL.

   a. Security Activities for Existing FCLs. The DOE cognizant security office must:

      (1) Determine and validate the security requirements, including personnel security clearances, for the proposed security activity.

      (2) Determine the FCL status through SSIMS or the Defense Security Service/Industrial Security Facilities Database (DSS/ISFD).

      (3) Compare the security requirements for the activity to the approved FCL in the following situations and ensure that:

(a) When the contractor FCL is granted by an OGA, the requirements for accepting an OGA FCL are met.

(b) When the contractor FCL is granted by DOE:

1 The new activity will be protected adequately under the facility's existing S&S program as outlined in the facility's approved security plan.

2 The existing FCL is compatible with the level and category of the new security activity.

3 The facility holds a composite facility rating of satisfactory on the basis of the last S&S survey report.

4 If applicable, coordination is accomplished with the DOE and/or OGA cognizant security agency for any tier parent(s) of the contractor holding a DOE or OGA FCL to ensure compliance with national requirements (e.g., FOCI determination, exclusion resolutions for KMP, etc.).

b. Registering New Security Activities. The procurement request originator will submit a DOE F 470.1, *Contract Security Classification Specification (CSCS)*, or DD 254 to the DOE contracting official, who will forward the completed DOE F 470.1 to the DOE cognizant security office. The DOE cognizant security office will verify the information and ensure that the new security activity can be performed within the existing FCL. If no issues are identified, the cognizant security office will approve the form and return it to the contracting officer so that the contract can be awarded. When a new activity will exceed the current FCL, or if there is no FCL, all actions required to upgrade the current level or obtain an FCL must be completed prior to contract award.

c. Terminating Security Activities. When a registered security activity is terminated, the organization that established the security activity must ensure that all access authorizations associated with the activity are terminated and all DOE property, classified information or matter, and/or nuclear and other hazardous material is appropriately reallocated, disposed of, destroyed, or returned to the appropriate DOE or cleared DOE contractor organization. A certificate of non-possession must be obtained from the organization responsible for the terminating activity and must be maintained by the DOE cognizant security office that established the security activity. A final CSCS form must be submitted and SSIMS must be updated to show the termination.

3. REGISTERING WORK FOR OTHERS (WFO) ACTIVITIES. The requirements of DOE O 481.1C, *Work for Others (Non-Department of Energy Funded Work)*, dated 1-24-

05 must be met before a WFO project or any "out of scope" modifications to existing WFO agreements are accepted. WFO activities must be registered in SSIMS.

a. WFO Performed at DOE-Owned or DOE-Operated Facilities. Before acceptance of WFO activities, the DOE and the requesting agency must exchange classification and protection information, including the DOE F 470.1, *Contract Security Classification Specification (CSCS)* or DD Form 254. The exchange of classification and protection information must be documented and may also include a formal agreement that includes reimbursement of any additional S&S costs (above minimum security requirements) incurred by the Department.

b. WFO Performed at Other Than DOE-Owned or DOE-Operated Facilities. When an OGA stipulates that WFO activities are to be performed by a DOE contractor at locations other than DOE-owned or DOE-operated facilities, an FCL is required. If the FCL is issued by an OGA, the requirements for accepting OGA FCLs apply. The WFO activity must be registered in SSIMS. Before the activity can be registered, all applicable requirements of DOE O 481.1C, *Work for Others (Non-Department of Energy Funded Work)*, must be met, and the DOE cognizant security office must review and certify that the sponsoring organization has complied with the applicable provisions of DOE O 475.2A, *Identifying Classified Information*.

c. Subcontracting in Connection with WFO. When subcontracting is required in connection with WFO, the subcontractor can be registered based on DOE F 470.2, *Facility Data and Approval Record (FDAR)*, and verification of the FCL. In this instance, a security cognizance agreement is not required. If the subcontractor has a DOE FCL at the appropriate level, the WFO activity must be registered. If the subcontractor has an FCL issued by an OGA, the considerations for the acceptance of OGA FCLs, as outlined in Chapter VI of this Section, apply. A separate letter or memorandum of understanding between DOE and the OGA is not required provided that all considerations are addressed in the WFO agreement.

4. EXCEPTIONS TO REGISTRATION IN SSIMS. Foreign intelligence information, SCI, SAPs, and other sensitive activities requiring special access or procedures associated with receipt, storage, processing, and/or handling must conform to the applicable protection provisions of Executive Orders and to applicable Director of Central Intelligence directives. Because these activities are not regulated under S&S policy, they are not registered in SSIMS. Exceptions to the registration requirements are identified below.

a. SAPs. SAPs are not registered in SSIMS. SAPs are registered in accordance with DOE O 471.5, *Special Access Programs*, dated 3-29-11.

b. SCI. SCI security activities are not registered in SSIMS; however, each accredited SCI facility (SCIF) must be registered in SSIMS using DOE F 470.2, *Facility Data and Approval Record (FDAR).*

c. Classified or Sensitive Activities. Details concerning sensitive or classified activities the publication of which in SSIMS would compromise mission completion of such activities or classified information are not registered in SSIMS. The DOE cognizant security office must notify the appropriate Program Secretarial office or, for NNSA, the Office of the Administrator before granting the FCL.

CHAPTER VIII. SUSPENSIONS

1. REASONS FOR SUSPENSION. When the following conditions occur, the DOE cognizant security office must suspend the FCL, document the action on an updated DOE F 470.2 (*Facility Data and Approval Record [FDAR]),* and immediately update SSIMS to reflect the suspension:

   a. When a company with an FCL is determined to be under FOCI that has not been mitigated, the FCL must be suspended. Contract performance on activities involving proscribed information may not continue until all applicable FOCI requirements are met.

   b. When findings or other deficiencies in a survey, self-assessment, inquiry, inspection, or evaluation indicate suspension of an FCL is necessary, the DOE cognizant security office will determine whether the FCL must be suspended pending validated corrective actions.

2. ACTIONS. When a decision is made to suspend the FCL of a company that has current access to classified information or SNM, the following actions must be taken:

   a. The facility subject to the suspension action must be notified in writing that its FCL has been suspended, including the reason for the suspension; that award of new contracts to the facility will not be permitted until the facility has been restored to a fully valid status; and that termination of the FCL may result if the issues causing the suspension are not rectified within a time frame and manner specified by DOE. Notification must include instructions for immediately securing classified material and/or SNM at an approved cleared facility pending restoration of the suspended facility to a fully valid status.

   b. GCAs must be notified and must make the final decision regarding a contractor's continued performance on existing contracts other than the contract activity for which the suspension is in effect. Continued possession of classified information or SNM associated with those contracts retained under GCA authorizations must be evaluated by the DOE cognizant security office to determine whether appropriate security requirements are being met.

   c. All affected DOE elements and, if applicable, affected OGAs must be notified by the DOE cognizant security office of the suspension action.

3. NON-COMPLIANCE WITH MITIGATION PLANS. When the DOE cognizant security office determines that a cleared contractor or its tier parent is out of compliance with an approved FOCI mitigation plan, the DOE cognizant security office must analyze the non-compliance and evaluate the overall impact to the protection of security interests. The cognizant contracting officer must be notified immediately and one or more of the following actions must be taken:

a. Request a corrective action and implementation plan from the contractor to bring it into compliance with the approved mitigation plan.

b. Suspend the FCL.

c. Terminate the FCL.

4. CONTINUATION OF CONTRACT PERFORMANCE UNDER FOREIGN GOVERNMENT OWNERSHIP. In accordance with the intent of 10 U.S.C. Section 2536, *Award of certain contracts to entities controlled by a foreign government: prohibition*, when an existing contractor becomes foreign-government owned but execution of a novation agreement is not required by the DEAR clause, the continued performance by that contractor on existing classified contracts or contracts for environmental restoration, remediation, or waste management that involve proscribed information may only continue under FCL suspension if:

a. The contractor is eligible for continuation on such work by Secretarial and/or OGA Secretarial waiver under 10 U.S.C. Section 2536(b)(1)(A) or 10 U.S.C. Section 2536(b)(1)(B), as applicable;

b. Each GCA takes immediate action to request a waiver under 10 U.S.C. Section 2536(b)(1)(A) or 10 U.S.C. Section 2536(b)(1)(B), as applicable, and also takes interim actions to safeguard the classified information associated with its classified contracts.

5. REINSTATEMENT OF A SUSPENDED FCL. When the conditions that resulted in the suspension have been resolved in a manner determined acceptable by DOE management, the FCL may be reinstated. The reinstatement must be based on the necessity to complete or continue work associated with the original FCL.

CHAPTER IX. FACILITY CLEARANCE TERMINATION AND CLOSE OUT

1. CONTRACT CLOSEOUT/FACILITY CLEARANCE TERMINATION.

   a. General. When a contract ends and/or an FCL is no longer necessary, the DOE cognizant security office must complete a termination survey, a DOE F 470.2, *Facility Data and Approval Record (FDAR)*, and update SSIMS to enact the termination. All security clearances connected to the facility clearance must be terminated and all DOE property, classified information or matter, and/or nuclear and other hazardous material presenting a potential radiological, chemical or biological sabotage threat must be appropriately reallocated, disposed of, destroyed, or returned to an appropriate DOE or cleared DOE contractor organization.

   b. Contract Completion. Upon completion or termination of a contract, the possessing contractor must submit to the DOE cognizant security office either a certificate of non-possession or a certificate of possession (of classified matter). A non-possessing contractor must submit a security activity closeout certification. Closure of the contract must be documented with a final DOE F 470.1, *Contract Security Classification Specification (CSCS)*. Forms and certificates must be maintained with the records pertaining to the facility clearance.

2. REACTIVATION. Reactivations of terminated FCLs must be based on programmatic or mission need and the implementation of current security requirements. The DOE cognizant security office must validate that all security requirements have been implemented, must complete a DOE F 470.2, *Facility Data and Approval Record (FDAR)*, and must update SSIMS to complete the reactivation.

SECTION 2. FOREIGN OWNERSHIP, CONTROL, OR INFLUENCE PROGRAM

1. OBJECTIVE. Foreign investment can play an important role in maintaining the vitality of the U.S. industrial base. Therefore, it is the policy of the U.S. Government to allow foreign investment consistent with the national security interests of the United States. The DOE Foreign Ownership, Control, or Interest (FOCI) policy for U.S. companies subject to an FCL determination is intended to facilitate foreign investment by ensuring that foreign firms cannot undermine U.S. security and export controls to gain unauthorized access to critical technology and/or classified information or matter, including RD, FRD, and SNM.

2. PURPOSE. The FOCI program regulates DOE determinations of the degree to which a contractor facility is under foreign ownership, control, or influence. In accordance with 48 CFR Chapter 9, the DOE Acquisition Regulation (DEAR), DOE must obtain information about FOCI that is sufficient to help the Department determine whether award of a contract to a person or firm, or the continued performance of a contract by a person or firm, may pose undue risk to the common defense and security. A contractor cannot be under FOCI to such a degree that granting or continuing an FCL would be inconsistent with U.S. national security interests. The requirements of the National Industrial Security Program (NISP) form the baseline for this program, supplemented with requirements for the protection of DOE-specific assets, Restricted Data, SNM, and other security activities.

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

4. REFERENCES.

   a. E.O. 12829, *National Industrial Security Program*, dated 01-26-93.

   b. 32 CFR Part 2004, *National Industrial Security Program Directive No. 1*.

   c. DoD 5220.22-R, *Industrial Security Regulation*.

   d. DoD 5220.22-M, *National Industrial Security Program Operating Manual (NISPOM)*.

   e. DoD Defense Security Service (DSS) Industrial Security Letters (ISLs), available at http://www.dss.mil/isp/fac_clear/download_nispom.html (Note: ISLs do not automatically impose requirements, but may contain useful clarifications of existing NISPOM provisions.).

f. Directive-Type Memorandum 09-019 (DTM) "Policy Gudance for Foreign Ownership, Control, or Influence," issued by the Office of the Under Secretary of Defense, available at http://www.dtic.mil/whs/directives/corres/dir3.html. (Note: DTMs, which may be issued periodically on a variety of topics, do not automatically impose requirements, but may contains useful information applicable to existing NISP programs.)

g. 10 U.S.C. Section 2536, *Award of certain contracts to entities controlled by a foreign government: prohibition.*

h. 48 CFR Chapter 9, *Department of Energy Acquisition Regulation.*

i. DOE Order 475.1, *Counterintelligence Program*, dated 10-04-04.

5. REQUIREMENTS. DOE cognizant security offices, as designated by the Program Secretarial Office or, for NNSA, the Office of the Administrator through the Chief, Defense Nuclear Security, are responsible for ensuring that the following activities are accomplished under the FOCI program for facilities and sites under their cognizance and for ensuring that contractors under their cognizance accomplish their responsibilities under this program at contractor facilities. Procedures applicable to the FOCI program must be documented in facility or site security plans.

a. Ensure that determinations are rendered under the FOCI program concerning foreign ownership, control or influence factors on all contractors and their tier parents as applicable, in accordance with national and DOE requirements when the contract will involve or is likely to involve classified information or SNM.

b. Establish and apply procedures to ensure that coordination is accomplished between the FCL and FOCI programs for all contractor FCLs.

c. Ensure that all relevant aspects of FOCI are resolved and, if necessary, appropriately mitigated prior to the granting of an interim or final FCL.

d. Ensure that contractors under their cognizance meet reporting requirements as established in DOE directives and national standards.

e. Establish and determine the circumstances under which a contractor will be requested to complete a new FOCI package.

f. Ensure that contractors under FOCI mitigation comply with all requirements imposed by the mitigation instrument.

g. Ensure that procedures are in place for verification of the original signature on the Standard Form (SF) 328, Certificate Pertaining to Foreign Interest, prior to finalizing a FOCI determination.

h. Ensure that counterintelligence threat and technology transfer risk assessments and updates are obtained and evaluated as necessary in the administration of the FOCI program.

i. Ensure that annual review and certification requirements established in DoD 5220.22-M, N*ational Industrial Security Program Operating Manual (NISPOM),* or alternative methods as permitted by this Order, for contractors under a FOCI mitigation instrument, are met for all such contractors under their cognizance.

j. Ensure that when factors not related to ownership are present, contractors take appropriate positive measure to assure that the foreign interest can be effectively mitigated and cannot otherwise adversely affect performance on contracts.

k. Approve trustees, proxy holders, and outside directors nominated by contractors in connection with FOCI mitigation plans, and approve specific measures such as technology control plans developed and implemented by contractors as part of FOCI mitigation plans.

l. Evaluate changes in FOCI information submitted by contractors holding an FCL, and make changes in mitigation methods or security requirements, or suspend or terminate the facility clearance, as warranted to address changed conditions.

CHAPTER I. GENERAL FOCI PROGRAM INFORMATION

1. GENERAL.

a. An FCL must not be granted until all relevant aspects of FOCI have been resolved and, if necessary, appropriately mitigated. Appropriate procedures must be in place to ensure coordination between the FOCI and FCL programs under the jurisdiction of each DOE program office.

b. The determination of whether a U.S. company is under FOCI must be made on a case-by-case basis. In instances where the company is unable to identify a foreign owner (e.g., the participating investors in a foreign investment or hedge fund cannot be identified), DOE may determine that the company is not eligible for an FCL. The following are examples of factors that must be considered to determine whether a company is under FOCI, is eligible for an FCL in spite of FOCI issues, and the protective measures required to mitigate FOCI:

(1) Foreign intelligence threat, including record of economic and government espionage against U.S. targets;

(2) Risk of unauthorized technology transfer;

(3) Type and sensitivity of classified information or matter, or special nuclear material (SNM) to be accessed;

(4) The nature, source, and extent of FOCI, including whether foreign interests hold a majority or substantial minority position in the company, taking into consideration all immediate, intermediate, and ultimate parent companies;

(5) Record of compliance with pertinent U.S. laws, regulations, and contracts;

(6) Nature of bilateral and multilateral security and information exchange agreements that may be relevant;

(7) Whether the government of the foreign interest has industrial security and export control regimes in place that are comparable to those of the United States; and

(8) Ownership or control, in whole or in part, by a foreign government.

c. Development of security measures to mitigate the impact of unacceptable FOCI must be based on the concept of risk management.

d. If there is a change in a company with an existing FCL that impacts a favorable FOCI determination, the FCL must be suspended or terminated unless security measures are taken to remove the possibility of unauthorized access or adverse impacts to contract performance.

e. Any doubt that unacceptable FOCI can be effectively mitigated to the point that affording the applicant access to classified information or matter is clearly consistent with national security must be resolved in favor of the national security.

2. APPLICABILITY.

a. FOCI determinations must be rendered on the following:

(1) Applicants, including industrial; educational; commercial; or any other entity, grantee, or licensee that have or anticipate executing a contract requiring access authorizations, including individuals contracting as a business. This includes subcontractors of any tier, consulting firms, agents, grantees, and cooperative research and development agreement participants who require security clearances.

(2) All tier parents of applicants when the parent is located in the United States, Puerto Rico, or a U.S. possession or trust territory (DEAR, section 925.204-73[f]).

b. A FOCI determination is not required for an individual performing work under a consulting agreement (e.g., an individual awarded a contract who has not contracted as a business). Foreign involvement for such individuals is determined and adjudicated through the background investigation conducted for the security clearance.

c. When a local, State, or Federal agency or department is granted an FCL, there must be an agreement containing a security clause, which must state that if the government agency or department subcontracts any work requiring access to classified information or matter by a commercial entity in connection with the FCL, a FOCI determination is required. If the government agency or department does not have its own FOCI policies or an agreement with the Secretary of Defense for industrial security services, DOE will render the FOCI determination.

d. Contractors with existing U.S. Government FCLs are identified in SSIMS and/or DSS/ISFD. No further FOCI review is required for an applicant registered in either of these systems holding an equal or higher U.S. Government FCL based upon a favorable FOCI determination.

3. ELECTRONIC SUBMISSION/PROCESSING WEB SITE. The Department has an electronic system for submission of FOCI information to DOE. To ensure confidentiality

of the information submitted and stored on the system, the site is protected with 128-bit encryption.

a. Applicants must use this system for the submission of FOCI packages, including changes to update their FOCI information. The FOCI Web site may be accessed via an Internet browser at https://foci.anl.gov. Electronic signatures are not accepted; therefore, a signed original SF 328, Certificate Pertaining to Foreign Interests, executed in accordance with the instructions on the certification section of the SF 328, must either be submitted to the DOE cognizant security office, or retained by the applicant and inspected by the DOE cognizant security office at the applicant's place of business prior to rendering the final FOCI determination.

b. Federal employees and supporting contractors use the Electronic Submission Processing System Web site at https://doefoci.anl.gov.

CHAPTER II. FOCI PROCESSING

1. DETERMINING THE REQUIREMENTS FOR A FOCI DETERMINATION. If the procurement request requires security clearances, the DEAR security clauses found at 48 CFR Part 952.204-2, *Security*, will be included in the contract. For all such contracts a DOE F 470.1, *Contract Security Classification Specification (CSCS)*, must be completed by the procurement request originator. A DD Form 254 may be used by a Federal agency sponsoring a contract activity, provided it is annotated with the DOE facility code. FOCI information and forms required under the security clauses will be submitted via the electronic FOCI website.

2. FINAL FOCI DETERMINATIONS.

   a. When insufficient lead time is expected between selection and contract award for the processing of the FOCI determination, the contracting officer may request a preliminary review, not a final FOCI determination, of the SF 328 submissions of each applicant in the competitive range.

   b. A final FOCI determination will only be rendered for the successful applicant.

3. ADJUDICATION.

   a. Adjudication Level.

      (1) The DOE cognizant security office renders the FOCI determination under the following conditions:

         (a) the responses to the FOCI questions do not exceed the thresholds in the FOCI Implementation reference tool in the e-FOCI system;

         (b) exclusion procedures are invoked when the applicant is controlled by a parent(s) not requiring security clearances or requiring a lower level of access to classified information or matter.

      (2) The Office of Health, Safety, and Security (HSS), or for NNSA the Office of Defense Nuclear Security, will render FOCI determinations that exceed established thresholds. The DOE cognizant security office will forward the FOCI submission(s) to HSS or NNSA with:

         (a) the justification for clearance or exclusion, including full details pertaining to the proposed contract, and

         (b) the DOE cognizant security office's analysis, including a clear statement of the reason why a Headquarters determination is required. The Headquarters office, in coordination with the Office

of General Counsel when appropriate, will provide a final FOCI determination to the submitting office.

b. Counterintelligence (CI) Threat Assessment and Technology Transfer Risk Assessment. A counterintelligence threat assessment and technology transfer risk assessment must be obtained and considered prior to a final decision to grant an FCL to an applicant under FOCI or to restore an FCL previously suspended because of unacceptable FOCI. The DOE cognizant security office must coordinate with the appropriate counterintelligence office to ensure that the threat assessment and technology transfer risk assessments and updates are accomplished.

4. COMMITTEE ON FOREIGN INVESTMENT IN THE UNITED STATES.

a. The Committee on Foreign Investment in the United States (CFIUS) is an interagency committee chaired by the Department of the Treasury under Section 721 of the *Defense Production Act of 1950* (50 U.S.C. App. 2170). CFIUS review is a voluntary process which affords an opportunity for foreign investors and U.S. persons entering into a covered transaction to submit the transaction for review by CFIUS to assess the impact of the transaction on national security. DOE policy with regard to CFIUS is found in DOE O 142.5, *Committee on Foreign Investment in the United States*, dated 10-8-10.

b. The CFIUS review and the FOCI and FCL processing actions are carried out in two parallel but separate processes with different time constraints and considerations.

5. CONTRACTING OFFICERS. Contracting officers must provide electronic or written notification to the DOE cognizant security office when:

a. they become aware of any changes to an applicant's FOCI status;

b. a requested FOCI review is no longer needed;

c. a FOCI determination was rendered on an applicant that was not awarded a contract;

d. all work on a contract for which a FOCI determination was rendered is within 30 days of termination or completion;

e. security clearances are no longer required in performance of the contract.

CHAPTER III. CHANGES TO FOCI INFORMATION

1. FOCI CHANGES THAT OCCUR FOLLOWING SUBMISSION OF AN SF 328 AND BEFORE CONTRACT AWARD. When an applicant has submitted a comprehensive FOCI package to the contracting officer and changes have occurred in the FOCI of the company prior to contract award, the applicant must submit an updated SF 328 and associated documents. DOE cognizant security offices must review the updated information and take any necessary steps to resolve FOCI concerns before the contract is awarded.

2. UPDATES. Changed conditions, such as a change in ownership, indebtedness, or foreign intelligence threat, may justify adjustments to the security requirements under which a company is operating or require that a different FOCI mitigation method be used. A changed condition may result in a determination that a company is no longer considered to be under FOCI or, conversely, that a company is no longer eligible for an FCL. Contractors holding an FCL based upon a favorable FOCI determination must submit written reports of changed conditions and anticipated changes which affect the FCL. Changes must be analyzed by the DOE cognizant security office to ensure that the contractor continues to meet the standards for holding an FCL. DOE cognizant security offices may request updated information, including the submission of a new FOCI package, at any time outside the normal cycle of package submission requirements. Significant changes that warrant a new FOCI determination include the following:

   a. a new threshold or factor exists that did not exist when the previous determination was made;

   b. a previously reported threshold or factor that was favorably adjudicated by the DOE cognizant security office has increased to a level requiring a determination by HSS or NNSA;

   c. a previously reported financial threshold or factor that was favorably adjudicated has increased by 5 percent or more; or a shift has occurred of 5 percent or more by country location, end user, or lenders;

   d. a previously reported foreign ownership threshold or factor that was favorably adjudicated has increased to the extent that a FOCI mitigation method or a different FOCI mitigation method is required; and

   e. any changes in ownership or control.

   f. Incidents of counterintelligence interest or concern identified and reported to the cognizant security office by the servicing counterintelligence office after the initial FOCI determination may also warrant a new determination.

3. ANNUAL REVIEW AND CERTIFICATION. The DOE cognizant security office will develop procedures to ensure that contractors provide adequate information to enable the DOE office to conduct a meaningful evaluation of compliance with annual review and certification requirements.

a. Each contractor holding an FCL under a FOCI mitigation instrument must provide written annual certification to the DOE cognizant security office that no changes have occurred which would impact the contractor's ability to protect classified information or matter or otherwise impact the national security. The certification report must include:

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

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

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

(4) any changes or impending changes of key management personnel or key board members, including the reasons for the changes'

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

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

b. Any contractor controlled by a parent organization(s) that has/have been excluded by formal resolution must provide written certification on an annual basis to the DOE cognizant security office acknowledging the continued effectiveness of the resolution.

c. Any contractor that has executed a Board Resolution to reduce FOCI in non-controlling foreign ownership situations must provide annual written certification to the DOE cognizant security office acknowledging that the resolution remains in effect.

d. Representatives of the DOE cognizant security office must meet annually (at least every 12 months) with the senior management officials who comprise the Government Security Committee (GSC) of organizations operating under a Voting Trust Agreement, Proxy Agreement, Special Security Agreement, or Security Control Agreement to review the effectiveness of the pertinent security arrangement and to establish a common understanding of the operating requirements and their implementation. If annual meetings cannot be conducted,

DOE cognizant security offices must establish other methods, such as the submission of a new FOCI package for review, to accomplish the same ends. Reviews must include examination of the following:

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

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

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

CHAPTER IV. FOCI MITIGATION

1. GENERAL. If DOE determines that a company is under FOCI, DOE will determine the extent to which and the manner in which the FOCI may result in unauthorized access to classified information or SNM and the types of actions that will be necessary to mitigate the associated risks to a level deemed acceptable to DOE. DOE cognizant security offices will ensure that the following are considered in every FOCI evaluation:

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

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

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

   d. Type and sensitivity of the information to be accessed;

   e. Source, nature, and extent of FOCI, including but not limited to whether foreign persons hold a majority or substantial minority position in the company, taking into consideration all immediate, intermediate, and ultimate parent companies;

   f. Nature of any bilateral and multilateral security and information exchange agreements that may pertain;

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

   h. Any other factor that indicates or demonstrates a capability on the part of the foreign interests to control or influence the operations or management of the business organization concerned.

2. MITIGATION ACTION PLANS. If there are any affirmative answers on the Certificate Pertaining to Foreign Interests, or other information is received which indicates that the applicant may be under FOCI, the DOE cognizant security office must review the case to determine the relative significance of the information in regard to the following factors:

   a. Whether the applicant is under FOCI;

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

   c. The type of actions, if any, that would be necessary to mitigate or negate the effects of the FOCI to a level deemed acceptable to the Federal Government.

3. FOCI MITIGATION INSTRUMENTS. The affected organization or its legal representatives may propose a plan to negate or reduce unacceptable FOCI; however,

DOE has the right and obligation to impose any security method, safeguard, or restriction it believes necessary to ensure that unauthorized access to classified information or matter, or SNM, is precluded. An organization that will not implement the security measures determined necessary by DOE to mitigate its foreign involvement to an acceptable level is ineligible for a FOCI determination and an FCL. Under all methods of FOCI mitigation, management positions requiring security clearances in conjunction with the FCL must be filled by U.S. citizens residing in the United States.

a. Secretarial Waiver Authority. In accordance with 10 U.S.C. Section 2536, a contract under a national security program may not be awarded to an entity controlled by a foreign government if it is necessary for the entity to be given access to proscribed information unless a waiver has been granted by the Secretary concerned (i.e., the Secretary of Energy or the Secretary of Defense). Further, if the Secretary decides to grant a waiver under 10 U.S.C. Section 2536(b)(1)(B) for an environmental restoration, remediation, or waste management contract, the Secretary must notify Congress of this decision. The contract may be awarded or the novation agreement executed only after the end of a 45-day period, beginning on the date notification is received by the Senate Committee on Armed Services and the House Committee on National Security.

b. Controlling Foreign Ownership. A controlling foreign ownership is one in which a non-U.S. citizen(s) owns a majority of the voting securities of the U.S. organization or, if less than 50 percent is foreign-owned, it can be reasonably determined that non-U.S. citizens or their representatives are in a position to effectively control the business management of the U.S. organization. Where the FOCI stems from majority foreign ownership or control, a FOCI mitigation plan may consist of one of the following methods:

(1) Voting Trust Agreement. Under this type of agreement, the foreign owner relinquishes most rights associated with ownership of the company to cleared U.S. citizens approved by the U.S. Government. Foreign owners must transfer legal title of the company to the Trustees. The Voting Trust Agreement does not impose any restrictions on the organization's eligibility to have access to classified information or matter or to compete for classified contracts. A Government Security Committee (GSC) must be established under the Voting Trust to oversee classified, SNM, and export control activities.

(a) All Trustees must become members of the company's governing board

(b) The arrangement must provide for the exercise of all prerogatives of ownership by the Trustees with complete freedom to act independently from the foreign owners, except as provided in the agreement, which may limit the authority of the Trustees by

requiring approval from the foreign owners with respect to matters such as:

1 the sale or disposal of the company's assets or a substantial part thereof;

2 pledges, mortgages, or other encumbrances on the company's assets, capital stock or ownership interests;

3 mergers, consolidations, or reorganizations;

4 dissolution of the company; and,

5 filing of a bankruptcy petition.

(c) The Trustees assume full responsibility for the foreign owner's voting interests and for exercising all management prerogatives relating thereto in such a way as to ensure that the foreign owner will be insulated from the company and will solely retain the status of a beneficiary.

(d) The company must be organized, structured, and financed to be capable of operating as a viable business entity independent from the foreign owner.

(2) Proxy Agreement. Like the Voting Trust Agreement, under this arrangement, the foreign owner relinquishes most rights associated with ownership of the company to cleared U.S. citizens approved by the U.S. Government. Under a Proxy Agreement, the foreign owner's voting rights are conveyed to the Proxy Holders by the irrevocable Proxy Agreement. Legal title to the shares remains with the non-U.S. citizen(s). All provisions of a Voting Trust Agreement applicable to Trustees, including authorized limitations on the powers of the Trustees, must apply to the Proxy Holders. The Proxy Agreement does not impose any restrictions on the organization's eligibility to have access to classified information or matter or to compete for classified contracts. The company must be organized, structured, and financed to be capable of operating as a viable entity independent from the foreign owner. Use of a Proxy Agreement requires the establishment of a GSC to oversee classified, SNM, and export control activities.

(3) Special Security Agreement. A Special Security Agreement may be considered when a U.S. organization is effectively owned or controlled by a foreign interest and the Federal Government has entered into a general security agreement with the foreign government involved. The Special Security Agreement preserves the foreign shareholder's right to be

represented on the governing body with a direct voice in the business and management of the company while denying unauthorized access to classified information or matter, or SNM by imposing substantial security and export control measures within an institutionalized set of corporate practices and procedures. SSAs must:

(a) require active involvement in security matters of senior management and certain Board members (outside directors), who must be cleared U.S. citizens;

(b) provide for the establishment of a GSC to oversee classified, SNM, and export control activities;

(c) be based on a Secretarial Waiver as described above if the contract will require access to proscribed information; and

(d) require a National Interest Determination (NID) prior to release of proscribed information to the contractor or its cleared employees to certify that release of such information is consistent with the national security interests of the United States. The NID can be program, project, or contract specific.

c. Non-controlling Foreign Ownership. A non-controlling foreign ownership is one in which a non-U.S. citizen(s) owns less than a majority of the voting securities of the U.S. organization and/or is not in a position to effectively control the business management of the U.S. organization. Where the FOCI stems from non-controlling foreign ownership or control, a FOCI mitigation plan must consist of either Board Resolution or Security Control Agreement methods.

(1) Board Resolution. When a foreign interest does not own voting interests sufficient to elect, or otherwise is not entitled to representation on the company's governing board, a resolution by the governing board will normally be adequate to mitigate the FOCI concerns. The resolution must identify the foreign shareholder and describe the type and number of foreign-owned shares; acknowledge the company's obligation to comply with all security and export control requirements; and certify that the foreign owner does not require, will not have, and can be effectively precluded from unauthorized access to all classified and export-controlled information entrusted to or held by the contractor. Annual certifications must be provided to the DOE cognizant security office acknowledging the continued effectiveness of the resolution. The company must distribute to members of its governing board and to its KMP copies of such resolutions, and report in its corporate records the completion of this distribution.

(2) Security Control Agreement. When a company is not effectively owned or controlled by a foreign interest and the foreign interest is nevertheless

entitled to representation on the company's governing board, a Security Control Agreement may be used. There are no access limitations under this type of agreement. However, the SCA requires the imposition of substantial security and export control measures in order to preserve the foreign interest's right to be represented on the board while denying unauthorized access to classified information or matter, or SNM. The SCA requires the same active involvement in security matters of senior management and certain Board members, and the establishment of a GSC, as are required when the Special Security Agreement is used.

d. Limited FCL. A limited FCL may be granted to certain contractors (e.g., a sole source contractor) which are controlled or owned by a foreign interest where FOCI mitigation is not able to be implemented. Access limitations are inherent with granting limited FCLs. Full requirements for granting a limited FCL are set forth in the Facility Clearance section of this appendix.

e. Factors Not Related to Foreign Ownership. When factors not related to ownership are present, positive measures must be put in place to assure that the foreign interest can be effectively mitigated and cannot otherwise adversely affect performance on classified contracts. Examples of such measures include:

(1) modification or termination of loan agreements, contracts and other understandings with foreign interests;

(2) diversification or reduction of foreign-source income;

(3) demonstration of financial viability independent of foreign interests;

(4) elimination or resolution of problem debt;

(5) assignment of specific oversight duties and responsibilities to board members;

(6) formulation of special executive-level security committees to consider and oversee matters that affect the performance of classified contracts;

(7) physical or organizational separation of the contractor component performing on classified contracts;

(8) the appointment of a technology control officer;

(9) adoption of special Board Resolutions; and,

(10) other actions that negate or mitigate foreign influence.

4. NONCOMPLIANCE WITH MITIGATION PLANS. When the DOE cognizant security office determines that a cleared contractor or its tier parent is out of compliance with an

approved FOCI mitigation plan, the cognizant security office must analyze the noncompliance and evaluate the overall impact to the protection of security interests. Depending on the severity of the noncompliance issue and the willingness or unwillingness of the organization to correct the problem and return to compliance, one or more of the following actions must be taken and the cognizant contracting officer notified immediately:

a. request a corrective action and implementation plan from the contractor to bring it into compliance with the approved mitigation plan;

b. suspend the facility clearance;

c. terminate the facility clearance. An existing FCL must be revoked if security measures cannot be taken to remove the possibility of unauthorized access or adverse effect on contract performance.

SECTION 3. SAFEGUARDS AND SECURITY AWARENESS

1. OBJECTIVE. To inform individuals of their safeguards and security (S&S) responsibilities and to promote continuing awareness of good security practices.

2. PURPOSE. The safeguards and security awareness program is responsible for communicating their personal security responsibilities to all individuals at a facility or site. In addition, for individuals who are granted access to classified information or matter, or special nuclear material (SNM), the security awareness program provides the means to instruct these individuals in their duties and responsibilities related to the access afforded to them and reiterate those duties and responsibilities upon termination of access. The program also provides, through supplementary awareness activities, a method to continuously reinforce good security practices.

3. DEFINITION. For purposes of this directive, the term "safeguards and security awareness" refers to all site introductory briefings on security topics, briefings conducted for access to classified information or matter or special nuclear material, formal refresher briefings covering access to classified or SNM and/or other security topics, termination briefings provided upon termination of access to classified or SNM, and all other activities, presentations, and materials intended to educate or raise the awareness of individuals as to their responsibilities within the facility/site security program.

4. REFERENCES.

   a. E.O. 13526, *Classified National Security Information*, dated 12-29-09.

   b. 10 CFR Part 1017, *Identification and Protection of Unclassified Controlled Nuclear Information*.

   c. 32 CFR Part 2001, *Classified National Security Information*, Subpart G, "Security Education and Training."

   d. 32 CFR Part 2001, *Classified National Security Information*, Subpart H, "Standard Forms."

   e. E.O. 12829, *National Industrial Security Program*, dated 01-26-93.

   f. DoD 5220.22-M, *National Industrial Security Program Operating Manual (NISPOM)*.

   g. Information Security Oversight Office (ISOO) Classified Information Non-Disclosure Agreement (Standard Form 312) Briefing Booklet.

   h. DOE O 475.2A, *Identifying Classified Information*, dated 2-1-11.

i. DOE O 471.1B, *Identification and Protection of Unclassified Controlled Nuclear Information*, dated 3-1-2010.

j. DOE O 471.3, *Identifying and Protecting Official Use Only Information*, dated 1-13-11.

k. DOE O 475.1, *Counterintelligence Program*, dated 10-4-04.

5. REQUIREMENTS. DOE cognizant security offices, as designated by the Program Secretarial Office or, for NNSA, the Office of the Administrator through the Chief, Defense Nuclear Security, are responsible for ensuring that the following activities are accomplished for the security awareness program for facilities and sites under their cognizance and for ensuring that contractors under their cognizance accomplish their responsibilities under this program at contractor facilities. Procedures applicable to the security awareness program must be documented in facility or site security plans.

a. Ensure that security briefings are conducted in accordance with the requirements of this section for all covered individuals.

b. Ensure that, if briefings are conducted through electronic means, a method exists to ascertain and verify that the individual completes all required content prior to receiving credit for the briefing.

c. Ensure that all individuals granted DOE security clearances (access authorizations) execute a Standard Form (SF) 312, Classified Information Nondisclosure Agreement, prior to being granted access to classified information or matter, or SNM.

d. Ensure that non-DOE personnel granted unescorted access to a facility or site security area receive appropriate awareness information (e.g., information on prohibited and controlled articles).

e. Develop and issue supplemental awareness materials, tailored to local facility/site conditions and issues and appropriate for both cleared and non-cleared employees and visitors, to make them aware of their security responsibilities.

f. Ensure that executed SF 312 forms and other records related to the security awareness program are maintained in accordance with ISOO and DOE records requirements.

g. Ensure that individuals are appropriately authorized to witness and accept the SF 312 on behalf of the United States and that such designations of authority are documented in the current facility/site security plan.

h. Determine administrative actions to be taken when individuals fail to complete the requirement for annual refresher briefings.

i. Ensure that information of counterintelligence concern is reported to the supporting counterintelligence office.

6. BRIEFINGS. Safeguards and security awareness programs must include an initial briefing for all individuals who are issued a DOE security badge; comprehensive, refresher, and termination briefings for all individuals with a DOE security clearance for access to classified information or matter, or SNM; and appropriate site-specific awareness information for non-DOE personnel granted unescorted access to Departmental security areas. S&S awareness refresher briefings must address site-specific knowledge and needs, S&S interests, and potential threats to the facility/organization. Contents must be reviewed regularly and updated as necessary. Contents of briefings concerning incidents of counterintelligence concern, deliberate compromises, and foreign interactions must be coordinated with the supporting counterintelligence office. Records must be maintained in a manner that provides an audit trail that verifies an individual's receipt of the briefings.

a. Initial Briefing. DOE Federal and contractor employees who receive a DOE security badge must receive an initial briefing before they are given unescorted access to other than public areas of the facility/site.

(1) Content.

(a) overview of the DOE facility/organization's mission;

(b) overview of facility/organization's major S&S program responsibilities;

(c) access control;

(d) escort procedures;

(e) protection of Government property and badge procedures;

(f) identification of controlled and prohibited articles;

(g) protection of controlled unclassified information (CUI), including official use only information;

(h) procedures for reporting incidents of security concern (e.g., attempts to gain unauthorized access to the facility or to classified information or matter); and

(i) identification of classification markings.

(2) Scheduling. The initial briefing must be completed before personnel assume their duties. A transferred individual must complete a site-specific initial briefing before assuming duties at the new site.

(3) Documentation. Initial briefing records must be maintained. Records may be maintained in conjunction with badging records or other records pertaining to access control.

b. Comprehensive Briefing. An individual must receive a comprehensive briefing upon receipt of a security clearance and before receiving initial access to classified information or matter, or special nuclear material (SNM).

(1) Content. The content for the comprehensive briefing must include the following items.

(a) Basic classification security policies and principles:

1 definition of classified information or matter;

2 purpose of DOE classification program;

3 levels and categories of classified information or matter;

4 damage criteria associated with each classification level;

5 classification awareness requirements contained in DOE O 475.2A, *Identifying Classified Information*.

(b) Classified information or matter protection elements:

1 procedures for protecting classified information and matter;

2 definition of unauthorized disclosures;

3 penalties for unauthorized disclosures;

4 conditions and restrictions for access to classified information or matter;

5 individual's S&S reporting requirements;

6 legal and administrative sanctions for security infractions and violations of law;

7 protection and control of classified information or matter, and controlled unclassified information, including telecommunications and electronic transmissions and official use only information;

8 information pertaining to security badges, security clearance levels, and access controls;

9 responsibilities associated with escorting;

10 targeting and recruitment methods of foreign intelligence services;

11 general information concerning the protection of SNM, if applicable; and

12 purpose and requirements of, and responsibilities for, the SF 312.

(c) Personnel security elements:

1 purpose of the personnel security program;

2 sources of legal authority and guidance;

3 the access authorization process;

4 key terms associated with adjudications;

5 adjudication factors;

6 due process; and

7 individual reporting requirements.

(2) Scheduling. Comprehensive briefings must be completed before individuals are granted access to classified information or matter, or SNM. A comprehensive briefing is also required when a security clearance is extended or transferred to another DOE facility/organization. Initial and comprehensive briefings may be combined at the discretion of facility/site security management. Under such circumstances, the briefing must include information prescribed for both initial and comprehensive briefings.

(3) Documentation. Documentation of the comprehensive briefing must be maintained. The SF 312 must be used to document the first comprehensive briefing after the grant of a security clearance, and may be used to document subsequent comprehensive briefings.

c. Refresher Briefing. Cleared individuals must receive annual refresher briefings. Agreements between DOE elements and/or contractor organizations may be established to ensure that individuals temporarily assigned to other DOE locations receive refresher briefings on schedule. Failure to complete the annual refresher briefing by an individual who holds a security clearance will result in administrative actions determined by the cognizant security office, including

possible administrative termination of the security clearance, until such time as the individual has complied with the briefing requirement. The processing personnel security office responsible for the clearance must be notified in accordance with paragraph d(3) below when a clearance is terminated for this reason.

(1) Content. Refresher briefings must selectively reinforce the information provided in the comprehensive briefing based upon current facility/site-specific security issues as well as counterintelligence (CI) awareness, and address the classification refresher requirements contained in DOE O 475.2A.

(2) Scheduling. Refresher briefings must be conducted each calendar year at approximately 12-month intervals.

(3) Documentation. Documentation of refresher briefings must be maintained for individuals until their next briefing. Documentation may be in electronic or hard copy format. Documentation must include the ability to identify individuals who have not met the refresher briefing requirement.

d. Termination Briefing. A termination briefing is required whenever a security clearance has been or will be terminated. Termination briefings must reiterate to the individual the continuing responsibility not to disclose classified information or matter to which they had access, the potential penalties for noncompliance, and the obligation to return all unclassified controlled and classified documents and materials in the individual's possession to the cognizant security office or to the DOE.

(1) Content. The content for the termination briefing must include:

(a) information contained in the numbered items of the Security Termination Statement Form (DOE F 5631.29 or successor form);

(b) information contained in items 3, 4, 5, 7, and 8 of the SF 312;

(c) penalties for unauthorized disclosure of classified information or matter as specified in the Atomic Energy Act and pertinent sections of 18 U.S.C.;

(d) penalties for unauthorized disclosure of Unclassified Controlled Nuclear Information (UCNI).

(2) Scheduling. The termination briefing must be conducted on the individual's last day of employment, the last day the individual possesses a security clearance, or the day it becomes known that the individual no longer requires access to classified information or matter, or SNM, whichever is sooner. If the individual is not available for the termination

briefing, the completed but unsigned security termination statement and an explanation of the circumstances surrounding the termination and why the signature could not be obtained must be submitted to the processing personnel security office.

(3) Required notification. When an individual no longer requires a security clearance/access authorization, or when a clearance/access authorization is administratively terminated, the processing personnel security office must be notified electronically or verbally within two working days to be followed by submission to that office of a completed DOE F 5631.29, *Security Termination Statement*.

(4) Documentation. Records documenting receipt of the termination briefing must be maintained. This briefing must be documented by completing DOE F 5631.29 or by written notice.

7. CLASSIFIED INFORMATION NONDISCLOSURE AGREEMENT (SF 312).

a. Administration.

(1) As a condition of access, a cleared individual must complete an SF 312 either at the time of, or after, the comprehensive briefing and before accessing classified information or matter, or SNM.

(2) Any individual who refuses to execute an agreement must be denied access to classified information or matter, or SNM and reported to the DOE cognizant security office. The processing personnel security office responsible for the clearance must be notified of the refusal to sign the SF 312 within 48 hours of the refusal.

(3) In most cases, the same person may serve as both the witness and acceptor of the SF 312 as long as that person has been authorized to accept the signed form on behalf of the United States. Any DOE Federal employee may witness the execution of the SF 312 by a Government or non-Government employee. A DOE Federal employee specifically authorized to do so may accept on behalf of the United States an SF 312 executed by either an employee of DOE or a contractor employee whose clearance is granted by DOE. An authorized representative of a contractor who has been specifically designated to act as an agent of the United States may witness and accept an SF 312 executed by an employee of the same organization.

b. Retention. The original SF 312 or a legally enforceable facsimile must be retained in accordance with General Records Schedule (GRS) 18, item 25, published by the National Archives and Records Administration (NARA), as supplemented by the DOE Administrative Records Schedule (ARS) 18. The

cognizant DOE security office must ensure SF 312s retained by contractors are sent to DOE upon the terminations of employment of contractor employees, in accordance with 32 CFR Part 2003.20.

c. Storage. The SF 312 must be stored in accordance with 32 CFR Section 2001.80(d)(2) and *DOE Administrative Records Schedule 18*. Personnel security files must not be used as a storage location for the agreements. Contractors are not permitted to provide storage for retired SF 312s on behalf of the DOE unless their facilities are approved in accordance with NARA standards for records storage facilities. The originals or legally enforceable facsimiles of the executed agreements must be retained in a file system from which they can be expeditiously retrieved if the U.S. Government seeks enforcement or subsequent employers require confirmation of execution.

8. SUPPLEMENTARY AWARENESS ACTIVITIES.

a. Purpose. Supplementary security awareness activities must be conducted to ensure that individuals, whether cleared or uncleared, are aware of their S&S responsibilities and good security practices. These awareness activities may be carried out in any form which meets the needs of the facility/site, including but not limited to briefings, presentations, posters, newsletters, token items such as badge lanyards, employee recognition, computer notices, fliers, tabletop cards, etc. Activities may address general security concerns or may be tailored to specific problems or issues as indicated by incident reports, employee questions, or management communications.

b. Records Retention. All programmatic records must be maintained in accordance with the NARA/DOE-approved records retention and disposition schedules.

SECTION 4. CONTROL OF CLASSIFIED VISITS

1. OBJECTIVE. Classified information and matter must be protected by ensuring that only persons with the appropriate security clearances, need-to-know, and programmatic authorizations are afforded access during visits where the release or exchange of such information is involved.

2. PURPOSE. Control of classified visits ensures that access to classified information by cleared U.S. citizens or individuals from foreign governments visiting DOE facilities is controlled in accordance with the mission of the Department and is consistent with national laws and regulations and international treaties and agreements.

3. DEFINITIONS.

   a. Classified visit. A visit that will involve or is expected to involve access to, or an exchange of, classified information.

   b. Foreign national. Any person who is not a U.S. citizen.

   c. Visitor. An individual who is not an employee or contractor of the facility/site and does not work full or part-time at the facility/site.

   d. Restricted Data access authorization. For purposes of classified visits by individuals from Other Government Agencies (OGA) other than DoD, NASA, and NRC, this term identifies access granted in connection with a visit to a cleared individual who has an official government need to access Restricted Data (RD) or special nuclear material (SNM) as defined in the Atomic Energy Act of 1954, as amended. This access does not require conversion of the prospective visitor's existing security clearance to a DOE L or Q access authorization, provided that: an authorized DOE official has verified the individual's OGA security clearance through DOE and national-level personnel security electronic databases, and made a need-to-know determination with respect to the specific RD and/or SNM to be disclosed during the visit; and the individual has executed an acknowledgement of receipt of a briefing on safeguarding RD and/or SNM.

4. REFERENCES.

   a. 42 U.S.C. Chapter 23, *Atomic Energy Act of 1954, as amended*.

   b. 42 U.S.C. Section 2455(b) (Section 304[b] of the *National Aeronautics and Space Act of 1958*).

   c. 10 CFR Part 1016, *Safeguarding of Restricted Data*.

   d. 10 CFR Part 1045, *Nuclear Classification and Declassification*.

e. 32 CFR Part 2001, *Classified National Security Information*, Subpart E, "Safeguarding."

f. E.O. 13526, *Classified National Security Information*, dated 12-29-09.

g. E.O. 12968, *Access to Classified Information*, dated 8-4-95.

h. E.O. 12829, *National Industrial Security Program*, dated 01-26-93.

i. DoD 5220.22-M, *National Industrial Security Program Operating Manual (NISPOM)*.

j. DoD Defense Security Service (DSS) Industrial Security Letters (ISLs), available at http://www.dss.mil/isp/fac_clear/download_nispom.html (Note: ISLs do not automatically impose requirements, but may contain useful clarifications of existing NISPOM provisions.).

k. DOE O 457.1, *Counterintelligence Program*, dated 10-4-04.

5. REQUIREMENTS. DOE cognizant security offices, as designated by the Program Secretarial Office or, for NNSA, the Office of the Administrator through the Deputy Administrator for Defense Programs, are responsible for ensuring that the following activities are accomplished for the classified visits program at facilities and sites under their cognizance and for ensuring that contractors under their cognizance accomplish their responsibilities under this program at contractor facilities. Procedures applicable to classified visits must be documented in facility or site security plans.

a. Ensure that local procedures are established for processing and handling classified visits to DOE Federal and contractor facilities under their cognizance by cleared U.S. citizens and for processing requests for classified visits by cleared individuals from their facilities to other locations.

b. Ensure that procedures are established for processing and handling visits by foreign nationals to facilities under their cognizance in accordance with governing international agreements or treaties.

c. Ensure that, for visits by foreign nationals, appropriate procedural limitations are developed and followed for the visit to preclude access to information not related to the visit and the scope of the international treaty or agreement governing the visit.

d. Ensure that responsibility for operational approval of classified visits, including delegations of authority as necessary, is established in writing and documented in the appropriate security plan.

e. Ensure that, when continuing visitor access approval is necessary for individuals who frequently visit DOE facilities, the access approval does not exceed a period

of 1 year (or for contractors, the final day of a contract if less than one year) and that approval is renewed annually if necessary.

f. Establish procedures to ensure that classified visit requests are sent and received through the DOE cognizant security office and the appropriate security offices of other Federal government agencies.

g. Establish procedures to ensure that, for classified visits involving access to RD or SNM by cleared U.S. citizens other than representatives of DoD, NASA, and NRC who are not otherwise authorized for such access: a senior Federal official at the site verifies through DOE and national-level personnel security electronic databases the individual's possession of a security clearance at the requisite level , and makes an affirmative documented determination that such access will not endanger the common defense and security; such individuals are given an appropriate briefing concerning the protection of RD and SNM prior to being given access; and the individuals sign an acknowledgement that they have received this briefing.

h. Establish procedures to ensure that access granted under paragraph g. above is tracked and maintained as part of the site classified visits file, and is not entered into any clearance tracking database or extended for any purpose outside the approved classified visit.

i. Establish procedures to ensure that all classified information or matter, including the individual's personal notes, to be removed from DOE's control by individuals granted access under paragraph g. above is sent through the DOE cognizant security office to the established classified mailing address listed in SSIMS for the OGA or OGA contractor facility which the individual represents. If no classified mailing address is registered in SSIMS, one must be established in accordance with the requirements in Section 1 of this Appendix before the material is released. Hand-carrying of classified information from DOE premises by individuals granted access in connection with a classified visit is strictly prohibited.

6. VISITS TO DOE FACILITIES BY CLEARED U.S. CITIZENS OTHER THAN DOE PERSONNEL.

a. For all classified visits to DOE and DOE contractor facilities, the following must be established and verified:

(1) the identity of the visitor;

(2) the level and type of clearance held by the visitor, which must allow access to the information to be disclosed;

(3) that the visit is for an official purpose for which the individual has a legitimate need to know and to access the classified information or matter to be disclosed.

b. Appropriate procedural limitations (e.g., use of escorts in limited/restricted areas) must be in place to ensure that the visitor has access only to information for which the individual has a verified need, and that access to other classified information or matter is precluded.

c. Requests for visits and access to specific types of facilities and information must be referred to and approved by the appropriate office:

(1) for weapons programs, nuclear materials production facilities, or sensitive nuclear materials production information, the Deputy Administrator for Defense Programs;

(2) for uranium enrichment plants or facilities engaged in uranium enrichment technology development, including advanced isotope separation technology, the Office of Nuclear Energy;

(3) for Naval Nuclear Propulsion facilities, the Deputy Administrator for Naval Reactors.

d. Visits involving access to Restricted Data (RD) or special nuclear material (SNM) when the visitor does not hold a DOE access authorization require specific approval by DOE/NNSA Federal officials authorized to give such approval. Approval must be based upon verification through DOE and national-level personnel security electronic databases that the individual holds an appropriate final security clearance, unless the individual is in one of the categories described below. If access to Nuclear Weapon Data Sigma information is required, the visit request must be submitted on DOE F 5631.20, *Request for Visit or Access Approval*, or successor form, and the form must specifically indicate the requirement for such access.

(1) DOE accepts the Q and L access authorizations granted by the Nuclear Regulatory Commission (NRC) as valid for access to RD. Visits by NRC employees, consultants, contractors, or subcontractors who require access to weapon data, sensitive nuclear materials production information, atomic vapor laser isotope separation technology, or uranium enrichment technology or entry into a DOE classified weapon or production facility must be approved by the appropriate Departmental element office. Visits may be requested using either the DOE F 5631.20 or NRC Form 277. NRC identification badges cannot be used as authority for visits.

(2) For DoD and NASA employees, consultants, contractors, or subcontractors, access to RD must be requested on a DOE F 5631.20 or

successor form. Individuals from NASA may also use NASA Form 405, Request for Access Approval. A memorandum or electronic message signed by the certifying official may be used unless access to Nuclear Weapon Data is required. For NASA, the visit request must include a certification that the matter to which access is requested relates to aeronautical and space activities. Requests must be forwarded for approval to the appropriate Departmental element with jurisdiction over the information to which access is requested. Access to critical nuclear weapon design information must be specifically requested.

(3) Prior to being given access, OGA employees and their contractors who are granted access to RD and SNM in connection with a classified visit must receive an appropriate briefing concerning the protection of RD and SNM and must sign an acknowledgement indicating his/her understanding that access will be terminated at the end of the visit period.

(4) RD and/or SNM access granted in connection with a classified visit must be tracked as part of the local site classified visit tracking process, and records of such access must be maintained in the classified visit files. This type of access will not be identified as a Q or L access authorization, will not be entered in the DOE Central Personnel Clearance Index or other clearance tracking databases, and cannot be extended for any purpose outside the approved classified visit.

(5) This process does not apply to classified visits by non-U.S. citizens.

7. VISITS BY CLEARED DOE PERSONNEL TO OTHER DOE FACILITIES.

a. Unless local site procedures require, or access to certain facilities or programs as described below will take place, formal visit requests are not required for visits by DOE Federal and contractor personnel to other DOE sites. The DOE security badge will serve as evidence of DOE security clearance/access authorization for internal DOE visits.

b. Visitors who require access to weapon data (classified Secret or Top Secret), sensitive nuclear materials production information, inertial confinement fusion data, atomic vapor laser isotope separation technology, uranium enrichment technology, or facilities specifically designated by a Departmental element, must obtain approval from the responsible office prior to the visit.

c. DOE F 5631.20 must be used by DOE Federal and contractor employees to obtain programmatic approval for access to Sigmas 14, 15, and/or 20. Approval for access must be obtained from the Deputy Administrator for Defense Programs.

d. Cleared DOE Federal or contractor employees who are foreign nationals may visit other facilities only under the access restrictions which apply to their clearances.

8. CLASSIFIED VISITS TO DOE FACILITIES BY NON-U.S.CITIZENS.

a. For all classified visits by non-U.S. citizens to DOE facilities, the following must be established and verified:

(1) the identity of the visitor;

(2) assurance that the sharing of specific classified information with the foreign national is covered by an existing treaty or agreement;

(3) receipt of security assurances from the appropriate foreign embassy;

(4) verification that the appropriate DOE Federal official has approved the sharing of the specific information to be disclosed during the classified visit.

b. DOE Federal or contractor employees may be designated to serve as hosts for classified visits by non-U.S. citizens. A host must be a U.S. citizen with an access authorization equal to or higher than the overall classification level of the visit. The host must ensure that:

(1) foreign nationals are not granted access to classified information before approval is received from the appropriate designated authority with programmatic responsibility;

(2) foreign nationals are precluded from any access to classified information outside the scope of the international agreement or treaty governing the visit and/or any limitations set by the approval authority with programmatic responsibility, and sharing of classified information is in accordance with the protocols specifically outlined in the agreement or treaty governing the visit (e.g., level, category, and type of classified information, protection procedures for incoming classified foreign government information, security clearance verification, transmission protocols for classified information during and after the visit, post-visit documentation, etc) ;

(3) appropriate procedural limitations (e.g., use of escorts in limited/restricted areas) are in place to ensure that the foreign visitor has access only to information permitted by the applicable international agreement or treaty for which the individual has a verified need, and that access to all other classified information or matter is precluded.

c. Requests for visits and access by foreign nationals to specific types of facilities and information must be referred to and approved by the appropriate Headquarters office:

(1) for visits to uranium enrichment plants or facilities and access to classified information on uranium enrichment technology development, including advanced isotope separation technology, the Office of Nuclear Energy;

(2) for visits and access to classified information in connection with the military application of atomic energy under 42 U.S.C. Section 2164, and 42 U.S.C. Section 2121, the Deputy Administrator for Defense Programs;

(3) for visits and access to classified information in connection with nonproliferation, international security, or International Atomic Energy Agency requirements, the Deputy Administrator for Defense Nuclear Nonproliferation;

(4) for visits and access to classified information in connection with naval nuclear propulsion, the Deputy Administrator for Naval Reactors;

(5) for visits and access to classified information in connection with Sensitive Compartmented Information, the Office of Intelligence and Counterintelligence.

9. DOCUMENTATION. Reports of classified visits must be maintained in accordance with *DOE Administrative Records Schedule 18*, paragraph 17.1.

SECTION 5. SAFEGUARDS AND SECURITY TRAINING PROGRAM

1. OBJECTIVE. To establish programs that ensure personnel are trained to a level of proficiency and competence that ensures they are qualified to perform assigned safeguards and security (S&S) tasks and/or responsibilities.

2. PURPOSE. The DOE Quality Assurance Program, as established in DOE O 414.1D, *Quality Assurance*, mandates that all DOE facilities and sites train and qualify their personnel to be capable of performing assigned work, and that continuing training be provided to maintain job proficiency. This section describes the requirements for establishing training for personnel working in S&S programs.

3. DEFINITION. As used in this section, training means the process of providing for and making available to an employee a planned, prepared, and coordinated program, system, or routine of instruction in S&S topical areas applicable to the employee's position that will improve individual and organizational performance and assist in achieving the Department's mission and performance goals.

4. REFERENCES.

   a. 5 U.S.C. Subpart C, *Employee Performance*, Chapter 41, "Training".

   b. DOE O 226.1B, *Implementation of Department of Energy Oversight Policy*, dated 4-25-11.

   c. DOE O 350.1 chg 3, *Contractor Human Resource Management Programs*, dated 9-30-96.

   d. DOE O 360.1B, *Federal Employee Training*, dated 10-11-01.

   e. DOE M 360.1-1B, *Federal Employee Training Manual, dated 10-11-01*.

   f. DOE O 413.3B, *Program and Project Management for the Acquisition of Capital Assets*, dated 11-29-10.

   g. DOE O 414.1D, *Quality Assurance*, dated 4-25-11.

   h. DOE-STD-1171-2009, *Safeguards and Security Functional Area Qualification Standard*.

   i. DOE-STD-1123-2009, *Safeguards and Security General Technical Base Qualification Standard*.

5. REQUIREMENTS. DOE cognizant security offices, as designated by the Program Secretarial Office or, for NNSA, the Office of the Administrator through the Chief, Defense Nuclear Security, are responsible for ensuring that security training activities are

accomplished at facilities and sites under their cognizance and for ensuring that contractors under their cognizance accomplish their responsibilities under this program at contractor facilities. Procedures applicable to S&S training must be documented in facility or site security plans.

a. The S&S training program for each facility must encompass all program elements which are performed by employees working at that location. The content of training (initial, refresher, and on-the-job) must be consistent with the knowledge and skills required to perform assigned S&S tasks and/or responsibilities as determined by valid and complete job analyses.

b. Individual training needs must be evaluated against a job or functional analysis of the position to ensure that appropriate job-related training is identified. Training requirements must be determined by analyzing needs, the job or function, and/or desired performance. Analyses must be conducted to ensure that training courses identify and address the requirements of the job competencies.

c. Training courses must be produced using a systematic approach that includes at least analysis, design, development, implementation, and evaluation phases.

d. Training that meets analysis requirements can be provided by external resources such as commercial vendors or other government training agencies. Training products procured from these resources must be evaluated at the site level for consistency with DOE policy and needs.

e. Evaluation of training must be performed to ensure that instructional objectives are met and to determine overall effectiveness. Knowledge and/or performance-based testing must be used to measure the knowledge and/or skills acquired from training programs.

f. Accurate and complete employee training records that contain dates of course attendance, course title, and scores/grades achieved (where applicable) must be maintained in accordance with DOE Administrative Records Schedule 1, Personnel Records.

g. Training plans that project training derived from a valid needs analysis for the forthcoming year must be developed annually.

h. Facility Security Officers must complete training appropriate to their position and the security operations conducted at their assigned facilities. This training should be completed within 1 year of appointment to the position of FSO.

SECTION 6. RESTRICTIONS ON THE TRANSFER OF SECURITY-FUNDED TECHNOLOGIES

1. OBJECTIVE. Protect and control classified and unclassified controlled Office of Health, Safety and Security (HSS) funded technology, other Technology Development Program (TDP)-related information, and protection practices and expertise that may be provided to recipients who are not Department of Energy (DOE) Federal or contractor employees.

2. PURPOSE. This section establishes DOE policy for ensuring that safeguards and security (S&S) funded technology, TDP information, and protection practices and expertise are disseminated outside the DOE only when such dissemination is in compliance with national laws and regulations.

3. REFERENCES.

   a. E.O. 12829, *National Industrial Security Program*, dated 01-26-93.

   b. DoD 5220.22-M, *National Industrial Security Program Operating Manual (NISPOM)*.

   c. 10 CFR Part 110, *Export and Import of Nuclear Equipment and Material*.

   d. 10 CFR Part 810, *Assistance to Foreign Atomic Energy Activities*.

   e. 15 CFR Parts 730 to 780, *Export Administration Regulations*.

   f. 22 CFR Parts 120 to 130, *International Traffic in Arms Regulations*.

   g. 31 CFR Parts 500 to 598, *Office of Foreign Assets Control (OFAC), Department of the Treasury*.

4. REQUIREMENTS. DOE cognizant security offices, as designated by the Program Secretarial Office or, for NNSA, the Office of the Administrator through the Chief, Defense Nuclear Security, are responsible for ensuring that the following activities are accomplished at facilities and sites under their cognizance and for ensuring that contractors under their cognizance accomplish their responsibilities under this program at contractor facilities. Procedures applicable to the transfer of security-funded technologies must be documented in facility or site security plans.

   a. General. The dissemination in any form of HSS funded classified and/or unclassified controlled technology, other TDP S&S-related information, or protection practices/expertise to individuals or organizations outside the Department and its operational facilities is prohibited until the following has taken place:

(1) verification of the recipient's capability to protect and control the information consistent with Department S&S and classification and control policies;

(2) a determination that the intended recipient has a strict need-to-know; a security clearance or access authorization at the appropriate level for any classified information; and that the Department's ability to protect its facilities and assets will not be weakened or degraded by the transfer in question; and

(3) approval of the transfer is obtained in accordance with the requirements for a risk assessment and the review and approval process set forth below, and with applicable Export Control laws and regulations.

b. Risk Assessment. An assessment of the risks for unauthorized use/transfer of classified technology, information, or practices must be conducted before release of the technology/information. The risk assessment must be used as the basis for approving or denying proposed transfers. Proposed release must be handled on a case-by-case basis because eligibility criteria are determined by both the type of information or technology and the intended recipient. The following factors must be addressed:

(1) a determination as to whether the applicant is eligible to receive a specific type of information and/or technology. No person is entitled solely by virtue of rank, position, or access authorization or security clearance to have access to classified or unclassified controlled HSS-funded technology, information or protection practices/expertise;

(2) relevance of and impact on the subject information or technology to the protection of Departmental facilities and assets;

(3) ability of the intended recipient to protect the information and/or technology in a manner equivalent to minimum security standards required by the Department.

c. Review and Approval Process. Reviews to determine if Export Control laws and processes apply must be conducted and the general and/or specific authorization (including any required license) from the appropriate authority must be obtained. Coordination and approval must include the Departmental element and the Chief Health, Safety, and Security Officer. Reports must be made in accordance with Export Control laws as applicable.

ATTACHMENT 1. CONTRACTOR REQUIREMENTS DOCUMENT DOE O 470.4B, *SAFEGUARDS AND SECURITY PROGRAM*

This Contractor Requirements Document (CRD) establishes Safeguards and Security requirements for Department of Energy (DOE) contractors, including National Nuclear Security Administration (NNSA) contractors.

In addition to the requirements set forth in this CRD, contractors are responsible for complying with Attachments 2, 3, 4, and 5 to DOE O 470.4B referenced in and made a part of this CRD and which provide program requirements and/or information applicable to contracts in which this CRD is inserted.

Regardless of the performer of the work, site/facility contractors with the CRD incorporated into their contracts are responsible for compliance with the CRD. Affected site/facility contractors are responsible for flowing down the requirements of the CRD to subcontracts at any tier to the extent necessary to ensure compliance with the requirements.

A violation of the provisions of the CRD relating to the safeguarding or security of Restricted Data or other classified information may result in a civil penalty pursuant to subsection a of section 234B of the *Atomic Energy Act of 1954* (42 U.S.C. Section 2282b). The procedures for the assessment of civil penalties are set forth in 10 CFR Part 824, *Procedural Rules for the Assessment of Civil Penalties for Classified Information Security Violations*.

1. REQUIREMENTS. Contractors must comply with the following requirements:

   a. Safeguards and security programs must be developed and maintained that incorporate the requirements contained in this CRD and its associated attachments.

   b. Programs associated with each topical area found in the attachments to this CRD must be implemented in accordance with the requirements stated for that topic.

   c. Contractors at facilities/sites that possess nuclear weapons and components, Category I special nuclear material, or targets subject to radiological or toxicological sabotage must develop defensive plans that apply the DOE Tactical Doctrine as set forth in Attachment 4. Defensive plans must focus on the protection of sensitive assets while assuring the maximum survivability of protective force (PF) personnel.

   d. Incidents of security concern must be addressed in accordance with the requirements found in Attachment 5 and reported in accordance with applicable laws and regulations.

   e. Interfaces and necessary interactions between S&S programs and other disciplines such as safety, emergency management, classification, counterintelligence, facility operations, cyber system operations and security, and business and budget

operations including property management must be identified and clearly defined; and must be maintained throughout the lifecycle of protective measures to ensure that S&S planning and operations work together effectively with these disciplines. Sensitive Compartmented Information is under the purview of the Office of Intelligence and Counterintelligence; necessary interfaces and interactions between that office and S&S programs must also be identified, defined, and maintained

f. S&S programs must incorporate a risk-based approach to protect assets and activities against the consequences of attempted theft, diversion, terrorist attack, industrial sabotage, radiological sabotage, chemical sabotage, biological sabotage, espionage, unauthorized access, compromise, and other acts that may have an adverse impact on national security, the environment, or pose significant danger to the health and safety of Department of Energy (DOE) Federal and contractor employees or the public.

g. S&S programs must be tailored to address site-specific characteristics and requirements, current technology, ongoing programs, and operational needs to achieve acceptable protection levels that reduce risks in a cost-effective manner.

2. EQUIVALENCIES AND EXEMPTIONS. Requests by contractors for equivalencies and exemptions to requirements contained in the CRD must be submitted through Federal channels approved by the cognizant Program Secretarial Office or the Administrator, National Nuclear Security Administration. When submitting a request for an equivalency or exemption, the contractor must specify, in writing, the reasons why it is impractical, unreasonable, or otherwise undesirable to comply with the requirement in question.

a. Equivalencies are alternatives to how a requirement in this CRD is fulfilled, where the CRD specifies the "how." An equivalency represents an alternate approach to achieving the goal of the CRD that results in no increased risk to public health and safety, the environment, workers, or national security.

b. Exemptions are a release from one or more requirements in this CRD without the identification of an equivalent means of meeting the requirement. The level of additional risk being accepted must be identified, and any measures implemented to compensate for the identified additional risk must be specified. Any increase in risk to public health and safety, the environment, workers, or national security must be justified.

c. When submitting a request for an equivalency or exemption, the request must be supported by a vulnerability assessment (VA) when required by the assets being protected, or by sufficient analysis to form the basis for an informed risk management decision; and the analysis must identify compensatory measures, if applicable, or alternative controls to be implemented.

3. DEFINITIONS.

a. Cognizant security office means the office assigned responsibility for a given security program or function. Where DOE cognizant security office is stated, the reference is to a Federal activity.

b. Definitions applicable to each topical area are found in the attachments. Definitions for terms used in a general S&S context are available through the Safeguards and Security Policy Information Resource (PIR) tool at http://pir.pnl.gov/.

ATTACHMENT 2. CONTRACTOR REQUIREMENTS DOCUMENT SAFEGUARDS AND SECURITY PROGRAM PLANNING

This Attachment provides information and/or requirements applicable to contracts in which the CRD (Attachment 1 to DOE O 470.4B) is inserted.

This attachment establishes the DOE requirements for developing facility and site security plans and for ensuring that plans are current and address the actual operating conditions at the covered location through performance assurance testing and a program of contractor self-assessments. Section 1 addresses planning activities. Section 2 covers activities to be implemented in connection with self-assessments and DOE surveys.

SECTION 1. SAFEGUARDS AND SECURITY PROGRAM PLANNING

1. OBJECTIVE. To establish a safeguards and security (S&S) planning approach that will provide facilities and sites with a consistent method for identifying, developing and documenting sound risk mitigation strategies by identifying all critical S&S performance, technical, schedule, and cost elements.

2. PURPOSE. Safeguards and security planning activities are conducted to ensure that an S&S plan describing the assumptions and approved operating conditions necessary to protect national security and property assets, as well as the public, DOE employees, and contractor employees from malevolent actions by adversaries, is prepared for each facility and site and approved by an appropriate Federal authority.

3. DEFINITIONS.

   a. Facility. A facility consists of one or more security interests under a single security management responsibility or authority and a single facility security officer within a defined boundary that encompasses all the security assets at that location, operating under a security plan that allows security management to maintain daily supervision of its operations, including day-to-day observations of the security program.

   b. Site. A site consists of one or more facilities operating under a centralized security management, including a site security officer with consolidated authority and responsibility for the facilities, and covered by a site security plan that may consolidate or replace, wholly or partially, individual facility plans.

   c. S&S Interest(s) and/or assets. A general term for any Departmental resource or property that requires protection from malevolent acts. It includes but is not limited to Federal and contractor personnel; classified information and/or matter; sensitive compartmented information facilities; automated data processing centers; facilities storing, processing, and transmitting classified information; vital equipment; special nuclear material (SNM); other nuclear materials; certain radiological, chemical or biological materials; sensitive unclassified information; or other Departmental property.

   d. Essential Elements. Protection and assurance elements necessary for the overall success of the safeguards and security program at a facility or site, the failure of any one of which would result in protection effectiveness being significantly reduced or which would require performance of other elements to be significantly better than expected in order to mitigate the failure. Essential elements can include but are not limited to equipment, procedures, and personnel.

4. REFERENCES.

a. DOE P 470.1A, *Safeguards and Security Program*, dated 12-29-10.

b. DOE O 470.3B, *Graded Security Program (GSP) Policy*, contractor requirements document, dated 8-12-08.

c. 48 CFR Section 952.204-2, *Security*, and Section 952.204-73(c), *Facility Clearance*.

d. E.O. 12977, *Interagency Security Committee*, dated 10-19-95.

e. Interagency Security Committee (ISC) Standard, *Physical Security Criteria for Federal Facilities*.

f. ISC Standard, *Facility Security Level Determinations for Federal Facilities*.

g. ISC Report, *The Design Basis Threat (DBT)*.

h. DOE-STD-1192-2010, *Vulnerability Assessment Standard*.

i. PDD 39, *U.S. Policy on Counterterrorism*.

j. HSPD 3, *Homeland Security Advisory System*.

k. DoD 5220.22-M, *National Industrial Security Program Operating Manual (NISPOM)*.

l. DOE O 150.1, *Continuity Programs*, dated 5-8-08.

5. REQUIREMENTS. Contractors are responsible for ensuring that the following security planning activities are accomplished for the facilities and sites under their cognizance.

a. Perform planning activities that support the Department's Strategic Plan, the facility/site's mission, forecasts of significant changes to facility/site operations, and current and projected operational and fiscal constraints.

b. Submit all contractor security plans for review and approval by DOE cognizant security offices, establishing a Federally-approved authorization for site security operations as well as the Federal acceptance of any residual risk involved in operations under the requirements of the approved security plans.

c. Maintain accurate and current approved security plans that continue to accurately describe site/facility S&S procedures and requirements.

d. Conduct site operations in compliance with approved security plans.

e. Monitor progress on completion of implementation plans to ensure that approved actions are completed within the approved time frames.

f. Develop and implement defense strategies and Security Incident Response Plans in accordance with the DOE Tactical Doctrine contained in Attachment 4 for facilities/sites that possess nuclear weapons and components, Category I SNM, or targets subject to radiological or toxicological sabotage .

g. Conduct assessments of protection effectiveness at a level of detail and at a level of rigor appropriate to the assets and security interests being protected and in accordance with national standards and DOE directives, and maintain documentation of such analyses in support of the security plan.

h. Provide assurances for safeguarding against loss, theft, diversion, unauthorized access, misuse or sabotage of radioactive materials and radioactive sealed sources that could adversely affect national security and the health and safety of employees, the public, and the environment in accordance with all safety and security requirements applicable to the contract, including the CRD to DOE O 470.3B, *Graded Security Protection (GSP) Policy*, the CRD to DOE M 231.1A chg 2, *Environment, Safety and Health Reporting Manual*, and 10 CFR Part 835, *Occupational Radiation Protection,* Subpart M and Appendix E.

i. Develop SECON response plans that can be immediately implemented when there is a change in either the Department's or a specific facility/site's SECON status.

CHAPTER I. SECURITY PLANS

1. GENERAL. All facilities and sites under DOE cognizance must have a security plan which reflects the assets, security interests, approved S&S program implementation at that location, and any residual risks associated with operation under the security plan.

   a. DOE cognizant security offices, in consultation with contractor security offices, will determine and define the facilities under their cognizance and how or if a group of facilities will be consolidated into a site. This decision is made locally in order to facilitate the security management at each location.

   b. For those facilities which do not have security assets (e.g., classified information or matter, SNM, or other assets requiring a facility security clearance (FCL) in accordance with the Facility Clearance section of this directive), the security plan must be developed to address the protection of employees and contractor property.

   c. For all U. S. Government owned or leased properties which do not have security assets (e.g., classified information or matter, SNM, or other assets requiring an FCL in accordance with the Facility Clearance section of this directive), but to which DOE Federal employees are assigned, the standards set forth by the Interagency Security Committee (ISC) under E.O. 12977, *Interagency Security Committee*, must be used as the baseline for developing the security plan.

   d. While the ISC standards do not apply to contractor owned or leased facilities in which government employees are not routinely assigned, they should be used to establish the basis for planning for the protection of employees and contractor property at contractor facilities which do not have security assets (e.g., classified information or matter, SNM, or other assets requiring an FCL in accordance with the Facility Clearance section of this directive).

   e. Facilities with security interests which require an FCL but which do not fall under the provisions of the CRD to DOE O 470.3B (*Graded Security Protection [GSP] Policy)* must develop security plans which, in addition to the protection of employees and property, address the protection of security interests at the location and meet the requirements in national-level policy and DOE directives for the protection of those interests. Non-possessing facilities must develop a security plan in sufficient detail to address how the contractor will fulfill its responsibilities (reporting requirements, management of employee clearances, etc.) under the FCL.

   f. Facilities with security interests to which GSP performance standards or other requirements apply must develop security plans which comply with the requirements in the GSP and incorporate the DOE Tactical Doctrine in addition to

complying with the requirements in national-level policy and DOE directives for the protection of any security interests not covered by the GSP performance standards, and in addition to the protection of employees and property.

2. SECURITY PLAN. The security plan is the approved method for conducting security operations at a facility or site and therefore must reflect security operations at that facility or site at all times. The plan must describe in detail, either in its content or in combination with other explicitly referenced documents, all aspects of safeguards and security operations occurring at the location and must include documentation of any deviations from national or DOE requirements. At those locations where management has determined that several facilities can be consolidated into a site, the site security plan may consolidate or replace individual facility security plans in whole or in part, but must establish a unified approach to conducting site operations. Security plans must be based on in-depth analysis of considerations specific to the location and the assets and interests to be protected.

3. ASSESSMENTS AND ANALYSES. Security plans must be supported by a sufficient analytical basis to establish that protection requirements will be met if the plan is completely and effectively executed. The analytical basis must include, as applicable, qualitative and quantitative simulations, performance test results, and/or expert analysis that reflect the complexity of facility/site operations and the consequences of loss or unauthorized access or use of the security assets present.

When facility/site security assets include Category I (or credible rollup to Category I) Special Nuclear Material (SNM), vulnerability assessments (VA), force-on-force system performance tests, other applicable performance tests, and expert analysis must be used in combination to establish the requirements for specific security measures and equipment, the effectiveness of the proposed security posture, and the requirements for improvements in the protection of Category I SNM documented in the approved security plan(s). Documentation of all such assessment activities should be retained on file to demonstrate how the security plan was developed and evaluated. However, these analyses need not be included or specifically referenced in the approved plan.

4. SECURITY PLAN COMPONENTS. All security plans must include the following:

a. a listing and prioritization of the assets and security interests at the facility or site; a description of how the protection program is managed; and a description of how applicable national and DOE S&S requirements are met, including any deviations from requirements; and

b. as required, implementation plans for meeting changes in applicable national or DOE policies or other changes (such as the addition or removal of security interests) which may require an extended time frame to implement because of financial or other resource considerations, including an implementation schedule and planned contingency measures in case the requirements cannot be met as

scheduled. Implementation plans and contingency measures may be included in the security plan by reference.

5. REVIEWS AND UPDATES. Security plans must be reviewed as required to ensure that the plans are current and reflect the actual operating conditions at the covered location. Changes to approved security plans must be approved by the DOE cognizant security office, and the Federal office may require more frequent reviews or may direct a contractor to review the contractor's plan at any time. Updates to security plans must be made whenever any of the following conditions apply:

   a. Changes in baseline security requirements in applicable national-level or DOE policy;

   b. Changes in facility operators/contractors;

   c. Changes in assets or security interests;

   d. Changes in facilities included in a site security plan;

   e. Changes in the security posture of a facility or site;

   f. Planned changes to the security program at the facility or site; or

   g. Changes in operations at a facility or site that require modification to approved security measures.

CHAPTER II. SECURITY CONDITIONS

1. GENERAL. DOE SECON levels reflect a multitude of conditions that may adversely impact Departmental and/or facility and site security. SECONs may include terrorist activity, continuity conditions, environmental (fire, chemical, radiological, etc.) and/or severe weather conditions. The day-to-day DOE security readiness state is correlated to the Homeland Security National Terrorism Advisory System (NTAS). NTAS alerts are established based on the analysis of a continuous and timely flow of integrated, all-source threat assessments and reporting provided to Executive Branch decision-makers. This chapter details DOE requirements for responding to changes in the NTAS alerts and the Departmental SECON levels.

2. SECON LEVELS. The following are the SECON levels used by DOE to establish the current security readiness state:

   a. SECON 5, Low Condition. This condition is declared when there is a low risk of terrorist activity, continuity conditions, environmental, and/or severe weather conditions. SECON 5 exists when a minimal SECON concern exists, but warrants only a routine security posture.

   b. SECON 4, Guarded Condition. This condition is declared when there is a general risk of terrorist activity, continuity conditions, environmental, and/or severe weather conditions. SECON 4 applies when there is a broad non-specific threat of a possible event, the nature and extent of which are unpredictable. All measures selected for use under SECON 4 must be capable of being maintained indefinitely.

   c. SECON 3, Elevated Condition. A SECON 3 is declared when there is a significant risk of terrorist activity, continuity conditions, environmental, and/or severe weather conditions. SECON 3 applies when an increased and more predictable threat against DOE facilities exists. The measures used in SECON 3 must be capable of being maintained for lengthy periods without causing undue hardship, affecting operational capability, or aggravating relations with the local community.

   d. SECON 2, High Condition. A SECON 2 is declared when there is a high risk of terrorist activity, continuity conditions, environmental, and/or severe weather conditions. This condition may apply when an incident occurs or intelligence is received indicating that some form of action against DOE personnel and facilities is imminent. Implementation of measures in this security condition for more than a short period will probably create hardship and affect the routine activities of the site and its personnel.

e. SECON 1, Severe Condition. This condition reflects a severe risk of terrorist activity, continuity conditions, environmental, and/or severe weather conditions. SECON 1 applies in the immediate area where conditions have occurred that may affect a DOE facility/site or when an attack is initiated on the site. Implementing SECON 1 will create hardship and affect the activities of the site and its personnel. Normally, this condition will be declared as a localized response.

3. SECON PLANNING. Contractor site security offices must develop SECON response plans that can be immediately implemented when there is a change in either the Department's or a specific facility/site's SECON status. Each facility or site must identify the specific measures that will most efficiently and effectively implement the required increases in readiness at each SECON level. Protection measures listed in HSPD-3 and the DOE SECON Quick Reference tool (http://www.hss.energy.gov/Referencebook/secon.html) may be used to develop response plans, which must describe the specific actions to be taken for each SECON level. SECON response plans must be made a part of the facility or site security plan.

4. ESTABLISHMENT OF SECON LEVEL.

a. Departmental SECON Level. Department-wide base SECON level is established by the Deputy Secretary of Energy in consultation with the Under Secretaries, the Director, Office of Intelligence and Counterintelligence, and the Chief Health, Safety and Security Officer. Departmental SECON levels will be determined using existing threat, environmental, COGCON levels as specified in DOE O 150.1, *Continuity Programs*, and/or other program considerations/factors for Headquarters and field activities. Changes in the COGCON level may require concurrent changes in the SECON level.

b. Local SECON Levels. Local SECON levels may differ from the Departmental SECON level and may be established by the DOE cognizant security office in consultation with contractor site/facility management. The DOE cognizant security office must obtain the concurrence of the cognizant Under Secretary or, in the case of DOE Headquarters, the Chief Health, Safety and Security Officer.

5. COORDINATION. If contractor facility/site management determines that a site/facility SECON level should differ from the Departmental SECON, contractor facility/site management must immediately notify the DOE cognizant security office so that appropriate notifications can be made to the Operations Center (OC), Office of Emergency Operations, Office of the Associate Administrator for Emergency Operations, NNSA, of the changed condition, the status of the facility, and the SECON response plan implementation.

CHAPTER III. PERFORMANCE ASSURANCE

1. GENERAL. An acceptable level of performance must be established and maintained to ensure that all elements of a facility/site protection program are workable and function as designed and in accordance with the overall protection goals established by local facility/site management. A performance assurance program must be developed which identifies the essential elements of the protection program and establishes monitoring and testing activities of sufficient rigor to ensure that the program elements are at all times operational, functioning as intended, and interacting in such a way as to identify and preclude the occurrence of adverse activity before security is irreversibly compromised. The intent of the performance assurance program is not to duplicate monitoring and testing activities conducted under ongoing quality assurance and safeguards and security operations, but to include them in a comprehensive approach to assuring system effectiveness. Implementation activities and schedules for performance assurance plans must be included in the facility or site security plan.

2. APPLICABILITY. All facilities with assets requiring a facility security clearance must conduct performance assurance activities. These activities must be tailored to the assets at the location and the elements which compose the total system in place at the location. At all locations, testing will include at a minimum the following:

   a. operability tests to confirm, without any indication of effectiveness, that a system element or total system is operating as expected;

   b. effectiveness tests to provide assurance that essential elements of the system are working as expected, separately or in coordination, to meet protection program objectives.

3. PERFORMANCE ASSURANCE PLANNING. Facilities and sites must implement and maintain a program that ensures that essential elements used to protect DOE S&S interests meet established requirements for reliability, operability, readiness, and performance prior to and during operational use. The assurance plan must:

   a. encompass all S&S topical areas relating to Program Management Operations, Physical Protection, Protective Force, Information Security, Personnel Security, and Materials Control and Accountability which are relevant to protection of assets at the facility/site;

   b. identify the essential elements relevant to protection of assets at the facility/site;

   c. describe how essential elements relevant to the protection of assets were determined;

   d. describe how each essential element and the facility/site security program as a whole will be tested, including type of test, evaluation criteria (test objectives and

performance criteria that define both success and failure), frequency, and number of tests;

e. establish the testing schedule for essential elements and whether any testing requirements established in other applicable DOE directives are to be integrated with this schedule;

f. describe the process for managing, tracking, and integrating results and addressing any deficiencies identified during the tests;

g. describe actions that must be initiated in the event of a failure of any essential element or the program as a whole.

4. TEST SCHEDULES.

a. Essential elements must be periodically tested to verify their continued functionality, operability, effectiveness and/or performance. Testing frequency may be based as applicable on manufacturer's recommendations, consensus standards, facility/site-specific conditions and operational needs, or other criteria that will ensure program effectiveness. Testing of elements which are not prone to failure and which are not subject to compromise without noticeable tampering, such as walls and fences, is not required as long as it can be documented that tampering with such elements would be detected in time to prevent compromise of overall protection.

b. In addition to the testing of essential elements, at least once every 12 months, a comprehensive facility or site threat scenario test must be performed at facilities/sites with Category I special nuclear material (SNM), identified credible radiological, biological or chemical sabotage targets, or identified as critical national security facilities/assets, to demonstrate overall facility/site S&S system effectiveness. Comprehensive threat scenarios must be consistent with the GSP.

c. Facilities/sites with denial protection strategies must conduct, in addition to the tests above, protective force exercises quarterly with a rotational schedule for multiple facilities requiring denial protection strategies. One of these quarterly tests may be combined with the annual comprehensive threat scenario test.

5. RESULTS ANALYSIS AND DOCUMENTATION. Each test must be documented in a test report which includes a narrative description of the testing activity and an analysis of test results. Issues requiring corrective action must be documented and tracked until resolved. When unsatisfactory results of a test indicate that national security and/or the health and safety of facility/site employees or the public is jeopardized, immediate compensatory measures must be taken until the issue is resolved, and normal reporting procedures must be followed.

6. SYSTEM DEGRADATION. When an essential element is under repair or is in an inoperative or ineffective state, the overall S&S program must be considered to be in a degraded mode until testing confirms that all applicable elements have returned to full operability. The facility or site must implement compensatory measures during such degraded modes adequate to ensure that protection of assets is maintained.

7. REVIEWS AND UPDATES. Performance assurance plans must be reviewed and updated when essential elements are affected due to:

   a. changes in facility/site mission, programmatic activities, or S&S interests and/or assets;

   b. changes in the operation or physical configuration of a facility or site, such as a building addition; new work processes or systems; construction of fences, roads, buildings, etc.; demolition of buildings; or reconfigurations of fences, roads, etc.;

   c. completion of S&S upgrades or downgrades;

   d. changes in protection strategy, risk or vulnerability analysis, protective force deployment, or other significant revisions to the applicable security plan;

   e. changes in S&S policies, including DOE Order 470.3B, *Graded Security Protection (GSP) Policy*,.

SECTION 2. SURVEY, REVIEW AND SELF-ASSESSMENT PROGRAMS

1. OBJECTIVE.

   a. Provide assurance to the Secretary, Departmental Elements, and other government agencies that safeguards and security (S&S) interests and activities are protected at the required levels.

   b. Provide DOE Federal and contractor line management with the information necessary to make informed decisions regarding the allocation of resources, acceptance of risk, and mitigation of S&S vulnerabilities.

2. PURPOSE. Surveys, self-assessments, and review programs are conducted to ensure that S&S systems and processes at facilities/sites are operating in compliance with Departmental and national-level policies, requirements, and standards for the protection of security assets and interests. These programs provide the means for timely identification and correction of deficiencies and noncompliant conditions to prevent adverse events, and validate the effectiveness of corrective actions implemented to address identified deficiencies.

3. DEFINITIONS.

   a. Safeguards and Security Survey. An integrated performance and compliance based evaluation of all applicable topics to determine the overall status of the S&S program at a facility or site and ensure that safeguards and security systems and processes at the location are operating in compliance with Departmental and national-level policies, requirements, and standards. Surveys are conducted or supervised by Federal security personnel.

   b. Initial Survey. A comprehensive review of the security status at a facility which is a candidate for a facility clearance (FCL), conducted to determine whether the facility in question meets established standards for the protection of the security interests and activities to be covered by the FCL.

   c. Periodic Survey. A survey conducted for all cleared facilities in accordance with established schedules and covering all applicable topics to meet the objectives of the S&S survey.

   d. Termination Survey. A survey of a cleared facility conducted to verify the termination of Departmental activities and the appropriate disposition of S&S interests at that facility. The termination survey confirms that all S&S activities have been terminated or awarded to another contractor, that access authorizations have been properly terminated or dispositoned, and that no DOE property, classified information or matter, and nuclear and other hazardous material presenting a potential radiological or toxicological sabotage threat remains.

e. Self-Assessment. An internal integrated evaluation of all applicable S&S topical areas at a contractor facility or site, conducted by contractor security personnel at intervals consistent with risk management principles, to determine the overall status of the S&S program at that location and verify that S&S objectives are met. The DOE cognizant security office may direct a specific self-assessment interval and may direct that self-assessment reports be provided to DOE.

f. Finding. A factual statement of identified issues and deficiencies (failure to meet a documented legal, regulatory, performance, compliance, or other applicable requirement) in the safeguards and security program at a facility, resulting from an inspection, survey, self assessment, or any other S&S review activity.

4. REFERENCES.

a. E.O. 13526, *Classified National Security Information*, dated 12-29-09.

b. E.O. 12829, *National Industrial Security Program*, dated 01-26-93.

c. DoD 5220.22-R, *Industrial Security Regulation*.

d. DoD 5220.22-M, *National Industrial Security Program Operating Manual (NISPOM)*.

e. DoD Defense Security Service (DSS) Industrial Security Letters (ISLs), available at http://www.dss.mil/isp/fac_clear/download_nispom.html (Note: ISLs do not automatically impose requirements, but may contain useful clarifications of existing NISPOM provisions.)

f. 10 CFR Part 1016, *Safeguarding of Restricted Data*.

g. 10 CFR Part 824, *Procedural Rules for the Assessment of Civil Penalties for Classified Information Security Violations*.

h. 32 CFR Part 2001, *Classified National Security Information*.

i. 48 CFR Chapter 9, *Department of Energy Acquisition Regulation*.

j. DOE P 226.1B, *Department of Energy Oversight Policy*, dated 4-25-11.

k. CRD to DOE O 226.1B, *Implementation of Department of Energy Oversight Policy*, dated 4-25-11.

l. CRD to DOE O 475.1, *Counterintelligence Program*, dated 10-04-04.

5. REQUIREMENTS. Contractors are responsible for ensuring that the following activities related to program reviews and self-assessments are conducted at facilities and sites under their cognizance, and for ensuring that assistance and data are provided as directed

to Federal security personnel during survey activities. Procedures applicable to these activities must be documented in facility or site security plans.

a. Review security programs on a continuing basis.

b. Conduct formal self-assessments at intervals consistent with DOE direction and risk management principles.

c. Prepare and submit to the DOE cognizant security office formal reports of self-assessments and related findings and corrective actions.

d. Evaluate all S&S topics relating to Program Management Operations, Physical Protection, Protective Force, Information Security, Personnel Security, and Materials Control and Accountability that are applicable at the facility or site through the self-assessments.

e. Provide management support for all self-assessment activities both in execution and in remedy.

f. Implement corrective actions for issues identified in self-assessments and surveys in a timely and effective manner, and validate the effectiveness of corrective actions to prevent recurrence of the issues.

g. Cooperate with survey activities conducted by the DOE cognizant security office or other Federal authorities.

6. SURVEYS. Surveys are conducted to confirm that a Federal or contractor facility meets all security requirements appropriate to the activities conducted at that facility, to inform Federal line management of the effectiveness of the facility security program, to identify any issues or concerns with the security program so that these can be addressed and corrected, and to allow both contractor and Federal managers to manage risk in an informed and rational manner. The DOE cognizant security office will determine the frequency of surveys, which may be increased or decreased consistent with risk management principles. Surveys will be conducted not more often than once every 12 months unless special circumstances exist.

7. SELF-ASSESSMENTS. All contractors holding FCLs are required to review their security programs on a continuing basis, and must also conduct formal self-assessments at intervals consistent with risk management principles and/or as directed by the DOE cognizant security office.

a. Self-assessments must have sufficient scope, depth, and frequency to ensure that at any point the facility is in compliance with all security requirements appropriate to the activities, information, and conditions at the location.

b. Contractor management is responsible for providing full support to the self-assessment program and for addressing any deficiencies identified through the program in a timely and effective manner.

c. Contractors must prepare a formal report describing each self-assessment and its findings, with the resolution of issues found, and provide it to the DOE cognizant security office.

8. FINDINGS AND CORRECTIVE ACTIONS.

a. All open S&S findings from previous assessments must be reviewed during self-assessments to validate the status of the corrective action and to evaluate the impact on the current operation of the facility's S&S program.

b. Findings from all self-assessments must be documented in the associated report.

c. Corrective action plans must be developed for all open self-assessment and survey findings. For all identified findings, corrective actions must be implemented in a timely and effective manner.

d. Self-assessment findings are not required to be entered into SSIMS; however, SSIMS or a local system must be used to track these deficiencies and associated corrective actions until closed.

e. Trending analyses of deficiencies must be conducted to determine if systemic and systematic causal factors underlie multiple self-assessment findings and, if so, the associated corrective action plans must address these causal factors.

9. DOCUMENTATION. Reports of self-assessments must be maintained in accordance with *DOE Administrative Records Schedule 18*, paragraphs 9 and 10.

ATTACHMENT 3. CONTRACTOR REQUIREMENTS DOCUMENT SAFEGUARDS AND SECURITY PROGRAM MANAGEMENT OPERATIONS

This Attachment provides information and/or requirements applicable to contracts in which the CRD (Attachment 1 to DOE O 470.4B) is inserted.

This attachment establishes the DOE requirements for conducting management activities connected with the operation of cleared facilities within the DOE complex. Section 1 addresses obtaining a facility clearance and establishing the safeguards and security activities connected with that facility. Section 2 covers the foreign ownership, control, or influence determinations which are necessary to establish and maintain a facility clearance. Section 3 covers security awareness activities, including required personnel briefings. Section 4 addresses the handling of classified visits to and from DOE facilities, including foreign classified visits. Section 5 deals with safeguards and security training to be provided for employees at cleared facilities. Section 6 covers restrictions imposed on the transfer of security funded technologies outside the United States.

SECTION 1. FACILITY CLEARANCES AND REGISTRATION OF SAFEGUARDS AND SECURITY ACTIVITIES

1. OBJECTIVE. To ensure that DOE, DOE contractor, and other (Federal) government agency (OGA) facilities and their contractors engaged in DOE activities are eligible for access to and meet the requirements to possess and secure classified information or matter or special nuclear material (SNM), and as applicable to protect other assets and conduct other security activities on behalf of DOE.

2. PURPOSE. The FCL program regulates Department of Energy (DOE) approval of a Federal or contractor facility's eligibility to access, receive, generate, reproduce, store, transmit, or destroy classified information or matter, special nuclear material (SNM), other hazardous material presenting a potential radiological, chemical, or biological sabotage threat, and/or DOE property of significant monetary value, exclusive of facilities and land values (hereinafter referred to as security assets and activities). The National Industrial Security Program Operating Manual (NISPOM) serves as a national standard to establish the baseline requirements for contractor facility clearances when contractors are engaged in activities requiring the protection of national security information classified at the Confidential, Secret, or Top Secret level. The NISPOM requirements are incorporated in this directive, supplemented with requirements for the protection of DOE-specific assets, Restricted Data, SNM, and other security activities not covered by the NISPOM.

3. FACILITY DEFINITION. For purposes of granting and registering a facility clearance code under this program, an entity (contractor or Federal) and its classified or high value security activities will be registered with one facility clearance code if the following criteria are met:

   a. A centrally directed security program is maintained that covers all security activities (i.e., under the same name, single mailing address, single security plan applicable at all locations, and all security matters under single management control).

   b. The distance between the security activities is such that the contractor or Federal entity is able to maintain daily supervision of its operations, including day-to-day observations of the security program.

4. REFERENCES.

   a. E.O. 12829, *National Industrial Security Program*, dated 01-26-93.

   b. E.O. 13549, *Classified National Security Information Program for State, Local, Tribal, and Private Sector Entities*, dated 8-18-10.

   c. 42 U.S.C. Sections 2011 through 2296, *Atomic Energy Act of 1954*.

d. 32 CFR Part 2001, *Classified National Security Information*.

e. 32 CFR Part 2004, *National Industrial Security Program Directive No. 1*.

f. 10 CFR Part 1016, *Safeguarding of Restricted Data*.

g. 10 CFR Part 1045, *Nuclear Classification and Declassification*.

h. DoD 5220.22-R, *Industrial Security Regulation*.

i. DoD 5220.22-M, *National Industrial Security Program Operating Manual* (NISPOM).

j. DoD Defense Security Service (DSS) Industrial Security Letters (ISLs), available at http://www.dss.mil/isp/fac_clear/download_nispom.html (Note: ISLs do not automatically impose requirements, but may contain useful clarifications of existing NISPOM provisions.)

k. Directive-Type Memorandum (DTM) 09-019 issued by the Office of the Under Secretary of Defense, available at http://www.dtic.mil/whs/directives/corres/dir3.html. (Note: DTMs, which may be issued periodically on a variety of topics, do not automatically impose requirements, but may contains useful information applicable to existing NISP programs.)

l. 10 U.S.C. Section 2536, *Award of certain contracts to entities controlled by a foreign government: prohibition*.

m. 48 CFR Chapter 9, *Department of Energy Acquisition Regulation*.

n. DOE O 475.2A, *Identifying Classified Information*, dated 2-1-11, contractor requirements document.

o. 10 CFR Part 824, *Procedural Rules for the Assessment of Civil Penalties for Classified Information Security Violation*.

5. REQUIREMENTS. Contractors are responsible for ensuring that the following activities are accomplished for the facility clearance program at facilities and sites under their cognizance. Procedures applicable to the FCL program must be documented in facility or site security plans.

a. Establish and maintain facility clearance activities in accordance with the requirements contained in this directive and in national policies.

b. In all FCL activities, provide complete information to enable the DOE cognizant security office and/or other DOE Federal authorities to ascertain the attendant risk and whether classified information and other security assets are adequately

protected, including but not limited to accurate and complete submissions of DOE F 470.1, *Contract Security Classification Specification (CSCS)* and DOE F 470.2, *Facility Data and Approval Record (FDAR)*, for entry into the Safeguards and Security Information Management System (SSIMS).

c. Ensure that any change that might affect the validity of the FCL is reported to the DOE cognizant security office.

d. When a subcontract is established for work involving security clearances, classified information or matter, or nuclear and other hazardous material presenting a potential radiological, chemical or biological sabotage threat, submit a request for a subcontractor FCL and the associated DOE F 470.2, *Facility Data and Approval Record (FDAR)*, to the DOE cognizant security office.

e. Ensure that DOE F 470.2, FDA*R*, and other information pertaining to subcontracts is accurately and currently maintained.

f. Immediately and accurately comply with all reporting requirements related to the FCL.

g. Ensure that when a limited facility clearance has been granted, strict access restrictions are imposed to limit access to the scope of the contract; provide written documentation to the DOE cognizant security office stating the restrictions to be imposed and how they will be enforced.

h. Report all changes in the organization's key management personnel (KMP) as they occur and process access authorizations for new KMP immediately.

i. Ensure that exclusion actions for KMP who will not be cleared are made a matter of record by the organization's executive body, and provide a copy of the resolution to the DOE cognizant security office.

j. Establish internal procedures to ensure that cleared employees are aware of their responsibilities for reporting pertinent information to the FSO, appropriate DOE authorities (including counterintelligence), the Federal Bureau of Investigation, or other Federal authorities as required by DOE directives, the terms of the classified contract, and U.S. law.

k. Cooperate with DOE and other Federal authorities during official inspections, investigations concerning the protection of classified information and DOE security interests, and during personnel security investigations of present or former employees and others.

l. Upon receiving notification from DOE that an FCL is suspended, take immediate action to implement instructions contained in the notification package for securing classified matter and/or special nuclear material at an approved cleared facility pending restoration of the FCL.

m. Upon termination of the FCL, ensure that all security clearances (access authorizations) connected to the facility clearance are terminated and all DOE property, classified information, and/or nuclear and other hazardous material presenting a potential radiological, chemical or biological sabotage threat is appropriately reallocated, disposed of, destroyed, or returned to an appropriate DOE or cleared DOE contractor organization; and that an appropriate certification of the actions taken in connection with the termination is furnished to the DOE cognizant security office.

n. Maintain all records pertaining to the FCL, including original records as designated by the DOE cognizant security office, for the duration of the FCL.

CHAPTER I. FACILITY CLEARANCE PROGRAM

1. GENERAL.

a. An industrial, educational, commercial, or other contractor entity will require an FCL if the terms of a contract awarded under 48 CFR Chapter 9, *Department of Energy Acquisition Regulation*, include the security assets and/or activities described in paragraph 2 of Section 1 above. A contractor requiring an FCL must be sponsored by:

(1) a Government Contracting Activity (GCA) (i.e., a contracting officer); or

(2) a cleared contractor acting as the prime contractor for an uncleared subcontractor. A contractor cannot sponsor itself for an FCL.

b. In accordance with the DEAR, section 952.204-2(l), FCLs are required for subcontractors requiring personnel security clearances. The prime contractor is responsible for implementation of the provisions of the NISPOM, Chapter 7, Subcontracting, and all DOE security requirements for their subcontractors and for termination of the subcontracts upon completion of activities. Prime contractors must ensure that all subcontracts are terminated if the prime contract is terminated, or for management and operations subcontracts, transferred to the cognizance of the new management and operations contractor as appropriate.

c. All company officials who occupy positions which have the authority to affect the organization's policies or practices in security activities conducted under the contract, as determined by the DOE cognizant security office, must be designated as Key Management Personnel (KMP). As a minimum, KMP must include the senior management official responsible for all aspects of contract performance and the designated facility security officer (FSO). KMP must be in process for or possess active security clearances in order for a contractor to be eligible for an FCL involving classified information or matter, or special nuclear material (SNM). Until all investigative requirements have been completed and final security clearances have been granted to the designated KMP, only an interim facility clearance can be granted.

d. In accordance with the DEAR clause, section 952.204-73(e), a contractor that will not possess or handle classified information or matter, or SNM at the contractor's place of business, but will require DOE personnel security clearances for the contractor's employees to perform work at other cleared facilities, must be processed for an FCL as a non-possessing facility. Employees of a non possessing contractor must adhere to the security plans of the facilities where they are afforded access to classified information or matter, or SNM.

e. A self-employed individual not doing business as a company, or a consultant who will not retain classified information or matter at his/her place of business, does not require an FCL, provided the individual or consultant is the sole employee requiring a security clearance. For security administration activities, to include processing for a personnel security clearance, the individual will be considered an employee of the possessing facility where he/she is afforded access to classified information or matter. These individuals are required to complete the same security awareness briefings and requirements as other cleared employees. A self-employed individual or consultant who will retain classified information or matter at their place of business must be processed for and granted an FCL that applies to the premises where the individual or consultant will store, handle, or process classified information or matter.

f. For Multiple Facility Organizations (MFOs), the home office facility must have an FCL at the same, or higher, level as that of any cleared facility within the MFO.

g. In a corporate tier parent-subsidiary relationship, the parent and each of its subsidiaries are separate legal entities and must be processed separately for an FCL. Because the parent controls the subsidiary, the general rule in the U.S. Government is that the parent must have an FCL at the same or higher level as that of the subsidiary. However, DOE will determine the necessity for the parent to be cleared or excluded from access, and will advise the companies as to what action is necessary for processing the FCL. When a parent or its cleared subsidiaries are collocated, a formal written agreement to use common security services may be executed by the two firms, subject to DOE approval.

h. A contractor granted an FCL by another government agency (OGA) may be granted a DOE FCL for receiving, processing, using, or storing classified information or matter under a DOE contract at the same clearance level, based on reciprocity.

2. ELIGIBILITY REQUIREMENTS. A contractor or prospective contractor must meet the following eligibility requirements prior to being processed for an FCL:

a. be selected to perform tasks under a contract containing the DEAR security clauses found at 48 CFR Part 952;

b. be organized under the laws of one of the 50 States, the District of Columbia, or Puerto Rico and must be located in the United States or a U.S. territorial area or possession;

c. have a reputation for integrity and lawful conduct in its business dealings;

d. not have been barred from participating in U.S. Government contracts (this includes key management personnel on the contract); and

e. not be under foreign ownership, control, or influence (FOCI) to a degree that the granting or continuation of the FCL would be inconsistent with the national interest.

CHAPTER II. IMPORTANCE RATINGS

1. FACILITY IMPORTANCE RATINGS. Importance ratings are used to establish a risk-based system for identifying the level of protection applicable to security assets and activities of facilities. Each facility granted an FCL must be assigned an importance rating. Contractors may recommend a facility rating based upon activities conducted; a final determination of the rating for each facility will be made by the DOE cognizant security office. Each facility's assigned importance rating must be recorded on DOE F 470.2, *Facility Data and Approval Record (FDAR)*. Importance rating criteria are as follows.

   a. "A" Importance Ratings. An "A" importance rating must be assigned to those facilities that meet any of the following criteria:

      (1) engaged in administrative activities considered essential to the direction and continuity of the overall DOE nuclear weapons program, as determined by the Program Secretarial Office or for NNSA, the Office of the Administrator;

      (2) authorized to possess Top Secret (TS) Restricted Data (RD) or Formerly Restricted Data (FRD), or TS national security information, or possess SAP matter, or designated as Field Intelligence Elements;

      (3) authorized to possess Category I quantities of SNM (including facilities with credible roll-up quantities of SNM to a Category I quantity); or

      (4) critical infrastructure programs determined to be essential by DOE line management.

   b. "B" Importance Ratings. A "B" importance rating must be assigned to those facilities that meet any of the following criteria:

      (1) engaged in activities other than those categorized as "A" and authorized to possess Secret (S) Restricted Data (RD) and/or weapon data matter;

      (2) authorized to possess Category II quantities of SNM; or

      (3) authorized to possess certain categories of biological agents.

   c. "C" Importance Ratings. A "C" importance rating must be assigned to those facilities that meet any of the following criteria:

      (1) authorized to possess Categories III and IV quantities of SNM or other nuclear materials requiring safeguards controls or special accounting procedures; or

(2) authorized to possess classified information or matter other than the type categorized for "A" and "B" facilities.

d. "D" Importance Ratings. A "D" importance rating must be assigned to those facilities that provide common carrier, commercial carrier, or mail service and are not authorized to store classified information or matter, or nuclear material during nonworking hours. (Carriers who store classified information or matter, or nuclear material must be assigned an "A," "B," or "C" importance rating).

e. "E" (Excluded Parent) Importance Ratings. An "E" importance rating must be assigned to a corporate tier parent of a contractor organization when the parent has been barred from participation in the activities related to a contract with DOE.

f. "PP" (Property Protection) Importance Ratings. A "PP" importance rating must be assigned to those facilities that meet any of the following criteria:

(1) Government property of a significant monetary value (suggested threshold of $5 million);

(2) nuclear materials requiring safeguards controls or special accounting procedures other than those categorized as types "A," "B," or "C";

(3) responsibility for DOE program continuity;

(4) national security considerations; or

(5) responsibilities for protection of the health and safety of the public and employees.

g. "NP" (Non-Possessing) Importance Ratings. An "NP" rating must be assigned to those facilities whose staff have authorized access to classified information or matter, or SNM at other approved locations, but which do not themselves possess any classified information or matter, or SNM, or meet any of the other criteria listed for the other ratings above.

2. UPGRADING AND DOWNGRADING A FACILITY'S ASSIGNED IMPORTANCE RATING. As security activities are added or changed, the importance rating of the approved facility may change (i.e., it may be either upgraded or downgraded). Upgrading or downgrading a facility importance rating may also require transfer of the DOE cognizant security office functions. Changes to the facility importance rating must be registered in SSIMS by the submission of DOE F 470.2, *Facility Data and Approval Record (FDAR).*

CHAPTER III. FACILITY CLEARANCE APPROVAL REQUIREMENTS

1. ISSUANCE OF FCLs. All eligibility requirements listed below must be satisfied prior to the issuance of an FCL. The DOE Acquisition Regulation (DEAR) prohibits the award of a classified contract until an FCL has been granted and issued. When an existing unclassified contract is modified to require classified work, the contract modification cannot take effect until an FCL is issued and the appropriate DEAR security clause is inserted in the contract.

2. CONTRACTOR FACILITIES. In accordance with the provisions of the DEAR , approval of a contractor final facility clearance must be based on the following items:

   a. A favorable foreign ownership, control, or influence (FOCI) determination based upon all information available to the DOE cognizant security office including information on the Standard Form (SF) 328 and any required supporting documentation;

   b. A contract or proposed contract containing the appropriate security clauses found in the DEAR;

   c. Approved safeguards and security plans, developed in accordance with Attachment 2 of this CRD, which describe protective measures appropriate to the activities being performed at the facility;

   d. If access to nuclear material is involved, an established Reporting Identification Symbol code for the Nuclear Materials Management and Safeguards Reporting System (NMMSS);

   e. A comprehensive survey conducted no more than 6 months before the facility clearance approval date, with a composite facility rating of satisfactory, if the facility will possess classified information or special nuclear material at its location, or if the facility has an importance rating of PP;

   f. Appointment of a Facility Security Officer(FSO), who must possess or be in the process of obtaining an access authorization (security clearance) equivalent to the level of the facility clearance (NOTE: only an interim FCL can be granted until the FSO's access authorization is finalized);

   g. If applicable, appointment of a Materials Control and Accountability Representative; and

   h. Access authorizations for key management personnel (KMP) who will be determined on a case-by-case basis and must possess or be in the process of obtaining access authorizations equivalent to the level of the facility clearance

(NOTE: until the required KMP access authorizations are finalized, only an interim FCL can be granted.)

CHAPTER IV. INTERIM AND LIMITED FCLS

1. INTERIM FCL. Interim FCLs are granted on a temporary basis, pending completion of full investigative and approval requirements, including but not limited to the completion of background investigations for final access authorizations for those individuals required to be cleared in connection with the FCL, such as key management personnel (KMP). Interim FCLs may be granted only to avoid unacceptable delays in pre-contract negotiation or in performance on a contract, and will be granted only after DOE has made a FOCI determination and granted interim access authorizations to KMP and other facility personnel requiring immediate access to classified information or matter. Interim facility clearances are granted solely at the discretion of DOE. Foreign owned or controlled companies and those with non-U.S. citizens as KMP are not eligible for interim FCLs.

2. LIMITED FCL. The United States has entered into agreements with certain foreign governments which establish arrangements whereby a foreign-owned U.S. company may be considered eligible for an FCL without any additional FOCI negation or mitigation instrument. To ensure that release of information or access to SNM is in accordance with the U.S. National Disclosure Policy, a limited FCL must be restricted to one security activity involving classified information or SNM. Award of another security activity to the same facility involving such information requires separate FCL registration, under another limited FCL or under an FCL without restrictions, if appropriate. Issuance of a limited FCL requires that strict access restrictions must be imposed to limit access to the scope of the contract. The clearance and exclusion requirements for KMP apply to all FCLs, including a limited FCL. Limited FCLs are granted solely at the discretion of DOE upon satisfaction of all criteria and requirements.

CHAPTER V. PERSONNEL SECURITY CLEARANCES AND EXCLUSION PROCEDURES REQUIRED IN CONNECTION WITH CONTRACTOR FCLS

1. SECURITY CLEARANCES REQUIRED IN CONNECTION WITH THE FCL. Certain officials [typically the owners, officers, directors, partners, regents, trustees, and/or executive personnel (KMP)] with the ability to affect the organization's policies or practices in security activities conducted under the contract must be cleared to the level of the FCL or formally excluded from access as appropriate. For multiple facility organizations, each subordinate cleared facility's KMP must also be cleared or excluded. Changes in an organization's KMP must be reported as they occur and access authorizations must be processed for new KMP immediately.

2. EXCLUSION PROCEDURES. When officials are to be excluded from or cleared at a level not commensurate with the FCL, compliance with one or both of the exclusion actions listed below is mandatory before issuance of an FCL. Exclusion actions must be made a matter of record by the organization's executive body. A copy of the resolution must be provided to the DOE cognizant security office.

   a. When formal exclusion action is required, the organization's governing body must affirm that specific KMP (designated by name) will not require, will not have, and can be effectively excluded from access to all classified information or matter, or nuclear or other hazardous material presenting a potential radiological, chemical, or biological sabotage threat, which is entrusted to or held by the organization; and do not occupy positions that would enable them to adversely affect the organization's policies or practices in the performance of classified contracts.

   b. When officials are to be cleared at a level below that of the FCL, the organization's governing body must affirm that such KMP (designated by name) will not require, will not have, and can be effectively denied access to higher-level classified information (specified by level) and do not occupy positions that would enable them to adversely affect the organization's policies or practices in the performance of higher-level classified contracts.

3. SECURITY CLEARANCES CONCURRENT WITH THE FCL. Contractors may designate employees who require access to classified information or matter during the negotiation of a contract or the preparation of a bid or quotation pertaining to a prime contract or a subcontract to be processed for security clearances concurrent with the FCL. The granting of an FCL is not dependent on the security clearance of such employees.

CHAPTER VI. REPORTING REQUIREMENTS

1 GENERAL. Contractors are required to report certain events that have an impact on the status of the facility clearance. The reporting requirements stated here pertain specifically to the FCL; additional requirements related to FOCI issues, personnel security concerns, and other security matters are also reportable and can be found in the directives applicable to those programs.

2 UPDATES. Contractors holding an FCL must submit written reports of changed conditions and anticipated changes affecting the FCL.

a. Significant changes. When changes have occurred in the extent and nature of FOCI that affect the information in a contractor's most recent FOCI submission, the contractor must provide written notification and supporting documentation relevant to the changes to the DOE cognizant security office. Significant changes include but are not limited to the following circumstances:

(1) all circumstances that would change any answer on the SF 328 from "No" to "Yes," which must be reported by submitting a changed condition SF 328;

(2) a previously reported threshold or factor that was favorably adjudicated by the DOE cognizant security office has increased to a level requiring a determination by the Office of Health, Safety, and Security or, for NNSA, the Office of Defense Nuclear Security;

(3) when a foreign interest owns five percent or more of a U.S. business organization (Questions 1a and 1b, SF 328), a five percent or greater increase in the beneficial ownership of a class of equity securities of the business organization, or a five percent increase in the beneficial ownership of the business itself, as determined by voting or investment rights, by one or more foreign interests and/or any U.S. person effectively controlled by a foreign interest;

(4) when a U.S. business organization owns ten percent or more of a foreign interest (Question 2, SF 328), any increase equivalent to ten percent or more of the tangible net worth of the business organization;

(5) when a U.S. business organization has non-U.S. citizen Key Management Personnel (KMP) (Question 3, SF 328), appointment of any additional non-U.S. citizen to a position required to be cleared in connection with the facility clearance or to any position identified in the articles of incorporation, by-laws, articles of organization, or equivalent governance documentation or charter for the business organization;

(6) when a Foreign Person has the power to control selection or tenure of KMPs/other decisions (Question 4, SF 328), any change in such power/authority except amendments or waivers to governance documentation either to correct manifest error or which are of a formal, minor, or technical nature and do not change materially any person's rights or obligations;

(7) when there are contracts, agreements, understandings, or arrangements with foreign person(s) (Question 5, SF 328), any change expected to result in annual payments to or from an entity where the payments exceed twenty percent of the U.S. business organization's annual gross revenues;

(8) when there is indebtedness, liabilities, or obligations to foreign persons (Question 6, SF 328), there is a changed condition reportable on the SF 328 whenever there is:

(a) any new indebtedness to foreign persons which results in a liability exceeding ten percent of the tangible net worth of the business organization or includes an instrument creating a mortgage, deed of trust, pledge, lien, security interest or other charge or encumbrance against (A) any of its property, assets or leasehold interests exceeding ten percent of the business organizations tangible net worth or (B) pledges five percent or more of the voting securities of the business organization as collateral, or

(b) any other new foreign indebtedness where the business organization permits to exist a leverage ratio exceeding two to one (2:1) based on the business organization's indebtedness to its tangible net worth and calculated on the basis of information set forth in its financial statement;

(9) when the business organization derives five percent or more of total revenues/net income from a single foreign person (Question 7a, SF 318), with respect to the business organization and that single foreign person, any change expected to result in annual payments to or from the business organization where the payments exceed an additional ten percent of the business organization's gross revenues;

(10) when the business organization derives thirty percent or more of total revenues/net income from foreign persons (Question 7b, SF 328), with respect to the business organization and any foreign persons, any change expected to result in annual payments to or from the business organization where the payments exceed an additional twenty percent of the business organization's annual gross revenue;

(11) when there are ten percent or more voting securities held in a method which does not identify the beneficial owner (Question 8, SF 328), any change of five percent or more in the total number of shares held in "nominee" shares, in "street names" or in some other method which does not identify the beneficial owner or any amendment to the bylaws of the business organization or its parent related specifically to voting rights of such nominee holders and any requirement regarding notice of any matter to be presented by a nominee stockholder at a shareholders meeting including any amendment affecting the voting and notice rights and obligations of nominee holders and associated persons who fail to make timely disclosures required by the U.S. Securities and Exchange Commission such as Schedule 13D;

(12) when there are KMP(s) holding positions or serving as consultants for foreign person(s) (Question 9, SF 328), any new position held by persons required to be cleared in connection with the facility clearance (excludes positions where the KMP is appointed by the U.S. parent business organization to a seat on the board or similar governing body of a foreign subsidiary, provided that the business organization promptly gives the DOE cognizant security office notice of such appointment;

(13) when there are any other factors of foreign person control or influence (Question 10, SF 328), each change qualifying as an affirmative answer to this question on the SF 328 and each change having a material effect on the ownership, control or influence of the business, operations, prospects, condition (financial or otherwise), or property of the business organization such that the security measures contemplated by an agreement with DOE to mitigate FOCI would not reasonably be expected to remove the possibility of unauthorized access to or adverse affect on the performance of classified contracts;

(14) a previously reported foreign ownership threshold or factor that was favorably adjudicated has increased to the extent that a FOCI mitigation method (if none previously existed) or a different FOCI mitigation method is required;

(15) any changes in ownership or control, including stock transfers that affect control of the company. Notice of changes includes ownership or control events that are required to be reported to the Securities and Exchange Commission (SEC), the Federal Trade Commission, or the Department of Justice (DOJ).

b. Anticipated changes. Anticipated changes are events that arise when the contractor or any of its tier parents enters into formal negotiations toward agreement, when the parties enter into a written memorandum of understanding (MOU), or in the case of financing agreements, when written application for

financing is made. The contractor must provide the DOE cognizant security office with written notification of anticipated actions, including but not limited to the following:

(1) an action to terminate business or operations of the contractor or any of its parents for any reason, including but not limited to entering into any transaction of merger, consolidation, or amalgamation with another company; conveying, selling, leasing, transferring, or otherwise disposing of all or a substantial part of company business or assets; and/or making any material change that could have an adverse effect on the contractor organization's ability to perform its contractual obligations for DOE or other contractors of DOE;

(2) legal actions taken to initiate bankruptcy proceedings involving the contractor organization or any of its tier parents;

(3) imminent adjudication of or reorganization resulting from bankruptcy actions involving the contractor organization or any of its tier parents;

(4) entry by the contractor or its tier parents into negotiations with non-U.S. citizens that may reasonably be expected to require amendment of the SF 328, including but not limited to negotiations for the sale of securities to a non-U.S. citizen or citizens.

3. OTHER REPORTABLE CHANGES.

a. Any change of operating name or address of the company or any of its cleared locations.

b. Any changes to information previously submitted for KMP, including, if appropriate, the names of the individuals they are replacing. In addition, a statement including the following information must be provided to the DOE cognizant security office:

(1) date and place of birth, social security number, citizenship, and, if appropriate, personnel security clearance level and issuing agency;

(2) whether they have been excluded from access to classified information or special nuclear material (SNM);

(3) whether they have been temporarily excluded from access to classified information or SNM pending the granting of the DOE access authorization.

c. A new complete listing of KMP will be submitted only at the discretion of the contractor and/or when requested in writing by the DOE cognizant security office.

d. Any precontract negotiation or award not placed through a government contracting authority that involves or may involve the release or disclosure of U.S. classified information to a foreign interest or access to classified information furnished by a foreign interest.

e. When requested by the DOE cognizant security office, the contractor shall provide a current list of all classified contracts as well as classified subcontracts issued to other contractors.

f. When requested by the DOE, selected contractors shall provide to the DOE cognizant security office security costs charged to the government for a specified period of time. The data points will be used by the DOE in developing the annual Report to Congress on overall National Industrial Security Program Costs.

CHAPTER VII. SUSPENSIONS

1. REASONS FOR SUSPENSION. When the following conditions occur, the DOE cognizant security office must suspend the FCL.

   a. When a company with a FCL is determined to be under FOCI that has not been mitigated, the FCL must be suspended. Contract performance on activities involving proscribed information must not continue until all applicable FOCI requirements are met.

   b. When findings or other deficiencies in a survey, self-assessment, inquiry, inspection or evaluation indicate suspension of a FCL is necessary, the DOE cognizant security office will determine whether the FCL must be suspended pending validated corrective actions.

2. ACTIONS. When a decision is made to suspend the FCL of a company that has current access to classified information or SNM, the following actions will be taken:

   a. The facility subject to the suspension action will be notified in writing that its FCL has been suspended, including the reason for the suspension; that award of new contracts to the facility will not be permitted until the facility has been restored to a fully valid status; and that termination of the FCL may result if the issues causing the suspension are not rectified within a time frame and manner specified by DOE. Notification will include instructions for immediately securing classified information or matter and/or SNM at an approved cleared facility pending restoration of the suspended facility to a fully valid status. Contractors must take immediate action to implement these instructions.

   b. GCAs will be notified and will make the final decision regarding a contractor's continued performance on existing contracts other than the contract activity for which the suspension is in effect. Continued possession of classified information or SNM associated with those contracts retained under GCA authorizations will be evaluated by the DOE cognizant security office to determine whether appropriate security requirements are being met.

   c. All affected DOE elements and, if applicable, affected OGAs will be notified by the DOE cognizant security office of the suspension action.

3. NONCOMPLIANCE WITH MITIGATION PLANS. When the DOE cognizant security office determines that a cleared contractor or its tier parent is out of compliance with an approved FOCI mitigation plan, the DOE cognizant security office will analyze and evaluate the overall impact to the protection of security interests. One or more of the following actions will be taken, and the cognizant contracting officer notified immediately:

a. Request a corrective action and implementation plan from the contractor to bring it into compliance with the approved mitigation plan. If so requested, the contractor must immediately supply the plan and all related information.

b. Suspend the FCL. If the FCL is suspended, contractors must immediately comply with all instructions from the DOE cognizant security office pertaining to the suspension.

c. Terminate the FCL. If the FCL is terminated, contractors must immediately comply with all instructions from the DOE cognizant security office and all actions listed in the termination section pertaining to the termination.

4. CONTINUATION OF CONTRACT PERFORMANCE UNDER FOREIGN GOVERNMENT OWNERSHIP. In accordance with the intent of 10 U.S.C. Section 2536, *Award of certain contracts to entities controlled by a foreign government: prohibition*, when an existing contractor becomes foreign-government owned but execution of a novation agreement is not required by the DEAR, the continued performance by that contractor on existing classified contracts or contracts for environmental restoration, remediation, or waste management that involve proscribed information may only continue under FCL suspension if:

a. the contractor is eligible for continuation on such work by Secretarial and/or OGA Secretarial waiver under 10 U.S.C. Section 2536(b)(1)(A) or 10 U.S.C. Section 2536(b)(1)(B), as applicable;

b. each GCA takes immediate action to request a waiver under 10 U.S.C. Section 2536(b)(1)(A) or 10 U.S.C. Section 2536(b)(1)(B), as applicable, and also takes interim actions to safeguard the classified information associated with its classified contracts.

5. REINSTATEMENT OF A SUSPENDED FCL. When the conditions that resulted in the suspension have been resolved in a manner determined acceptable by DOE management, the FCL may be reinstated. The reinstatement must be based on the necessity to complete or continue work associated with the original FCL.

CHAPTER VIII. FACILITY CLEARANCE TERMINATION AND CLOSE OUT

1. CONTRACT CLOSEOUT/FACILITY CLEARANCE TERMINATION.

   a. General. When a contract ends and/or a facility clearance is no longer necessary, the FCL will be terminated. All security clearances connected to the facility clearance must be terminated and all DOE property, classified information, and/or nuclear and other hazardous material presenting a potential radiological, chemical or biological sabotage threat must be appropriately reallocated, disposed of, destroyed, or returned to an appropriate DOE or cleared DOE contractor organization.

   b. Contract Completion. Upon completion or termination of a contract, the possessing contractor must submit to the DOE cognizant security office a final DOE F 470.1, *Contract Security Classification Specification (CSCS)*, and either a certificate of non-possession or a certificate of possession (of classified matter). A non-possessing contractor must submit the final CSCS and a security activity closeout certification. Certificates must be signed by the FSO.

      (1) Non-Possessing Facilities. Upon termination of security activities, the non-possessing contractor must submit a Security Activity Closeout Certification certifying that all security clearances connected with the contract have been terminated or transferred to another contract for DOE.

      (2) Certificate of Non-Possession. Upon return, reallocation, disposition, or destruction of all classified matter pertaining to a contract, the contractor must submit a certificate of non-possession to the DOE cognizant security office. The certificate must include the contract number and a statement that all classified matter has been returned to authorized representatives of DOE or destroyed.

      (3) Certificate of Possession.

         (a) Requests to retain classified matter must indicate the benefit to DOE and the intended use of the information. Certificates must specifically identify classified matter by subject, type or form, and quantity and must state that the classified matter will retain its initial classification until downgraded or declassified by DOE, will be safeguarded in accordance with DOE requirements, that any classified matter which cannot be accounted for or which has been potentially compromised will be reported immediately in accordance with DOE security requirements, and acknowledge that unauthorized disclosure of classified matter is subject to criminal penalties.

(b) If the classified matter will aid the contractor in performing another active Government contract and the matter is being transferred to the active contract, the contractor must provide the DOE cognizant security office or the OGA holding the contract a copy of the retention notification. If the contractor is not notified to the contrary, the matter may be transferred and will fall under the jurisdiction of the gaining (i.e., active) contract.

(c) When a certificate of possession is submitted, the contractor may maintain the classified matter for 24 months unless notified to the contrary by the DOE cognizant security office or OGA with jurisdiction over the classified matter.

(d) Special nuclear material may not be retained.

2. REACTIVATION. Reactivations of terminated FCLs will be based on programmatic or mission need, a classified contract, and the implementation of current security requirements.

SECTION 2. FOREIGN OWNERSHIP, CONTROL, OR INFLUENCE PROGRAM

1. OBJECTIVE. Foreign investment can play an important role in maintaining the vitality of the U.S. industrial base. Therefore, it is the policy of the U.S. Government to allow foreign investment consistent with the national security interests of the United States. The DOE Foreign Ownership, Control, or Interest (FOCI) policy for U.S. companies subject to a facility clearance determination is intended to facilitate foreign investment by ensuring that foreign firms cannot undermine U.S. security and export controls to gain unauthorized access to critical technology and/or classified information or matter, including RD, FRD, and SNM.

2. PURPOSE. The FOCI program regulates Department of Energy (DOE) determinations of the degree to which a contractor facility is under foreign ownership, control, or influence. In accordance with 48 CFR Chapter 9, *Department of Energy Acquisition Regulation*, DOE must obtain information about FOCI which is sufficient to help the Department determine whether award of a contract to a person or firm, or the continued performance of a contract by a person or firm, may pose undue risk to the common defense and security. A contractor cannot be under FOCI to such a degree that granting or continuing a facility security clearance (FCL) would be inconsistent with U.S. national security interests. The requirements of the National Industrial Security Program (NISP) form the baseline for the program, supplemented with requirements for the protection of DOE-specific assets, Restricted Data, SNM, and other security activities.

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

4. REFERENCES.

   a. E.O. 12829, *National Industrial Security Program*, dated 01-26-93.

   b. 32 CFR Part 2004, National Industrial Security Program Directive No. 1.

   c. DoD 5220.22-R, *Industrial Security Regulation*.

   d. DoD 5220.22-M, *National Industrial Security Program Operating Manual (NISPOM)*.

   e. DoD Defense Security Service (DSS) Industrial Security Letters (ISLs), available at http://www.dss.mil/isp/fac_clear/download_nispom.html (Note: ISLs do not automatically impose requirements, but may contain useful clarifications of existing NISPOM provisions.).

f. Directive-Type Memoranda (DTM) issued by the Office of the Under Secretary of Defense (e.g., DTM 09-019, "Policy Guidance for Foreign Ownership, Control, or Influence" issued 9-2-09), applicable until incorporated into DoD policy issuances.

g. 10 U.S.C. Section 2536, *Award of certain contracts to entities controlled by a foreign government: prohibition.*

h. 48 CFR Chapter 9, *Department of Energy Acquisition Regulation*.

i. The CRD to DOE O 475.1, *Counterintelligence Program*, dated 10-04-04.

5. REQUIREMENTS. Contractors are responsible for ensuring that the following activities are accomplished for the FOCI program. Procedures applicable to the FOCI program must be documented in facility or site security plans.

a. Establish and maintain activities related to FOCI in accordance with the requirements contained in this directive and in national policies.

b. In all FOCI activities, provide complete information to enable the DOE cognizant security office and/or other DOE Federal authorities to ascertain the attendant risk and whether classified information and other security assets are adequately protected, including but not limited to accurate and complete submissions of Standard Form (SF) 328, Certificate Pertaining to Foreign Interest, and information provided during annual certification and review activities.

c. Ensure that all changes that might affect the FOCI determination are reported to the DOE cognizant security office as they occur.

d. Immediately and accurately comply with all reporting requirements related to FOCI.

e. Maintain all records pertaining to FOCI, including records such as original signatures on the SF 328 if so instructed by the DOE cognizant security office, and make such records available upon request to the DOE cognizant security office.

f. Complete a new FOCI package when directed to do so by the DOE cognizant security office or on a schedule established by that office.

g. Propose appropriate FOCI mitigation instruments and work with the DOE to develop a suitable FOCI mitigation plan acceptable to the DOE.

h. Comply with all requirements and restrictions imposed by an approved FOCI mitigation plan.

i. Furnish annual review and certification information one year from the effective date of a mitigation agreement and annually thereafter.

j. When factors not related to ownership are present, take appropriate positive measures to assure that the foreign interest is effectively mitigated and cannot adversely affect security assets and performance on contracts.

k. When FOCI is mitigated through use of a Voting Trust, Proxy Agreement, Special Security Agreement or Security Control Agreement, establish a permanent committee of the organization's Board of Directors as the Government Security Committee.

CHAPTER I. GENERAL FOCI PROGRAM INFORMATION

1. GENERAL.

a. An FCL will not be granted until all relevant aspects of FOCI have been resolved and, if necessary, appropriately mitigated.

b. The determination of whether a U.S. company is under FOCI will be made on a case-by-case basis. In instances where the company is unable to identify a foreign owner (e.g., the participating investors in a foreign investment or hedge fund cannot be identified), DOE may determine that the company is not eligible for an FCL. The following are examples of factors which DOE will consider to determine whether a company is under FOCI, is eligible for an FCL in spite of FOCI issues, and the protective measures required to mitigate FOCI.

(1) foreign intelligence threat, including record of economic and government espionage against U.S. targets;

(2) risk of unauthorized technology transfer;

(3) type and sensitivity of classified information or matter, or special nuclear material (SNM) to be accessed;

(4) nature, source, and extent of FOCI, including whether foreign interests hold a majority or substantial minority position in the company, taking into consideration all immediate, intermediate, and ultimate parent companies;

(5) record of compliance with pertinent U.S. laws, regulations, and contracts;

(6) nature of bilateral and multilateral security and information exchange agreements that may be relevant;

(7) whether the government of the foreign interest has industrial security and export control regimes in place that are comparable to those of the United States;

(8) ownership or control, in whole or in part, by a foreign government.

c. If there is a change in a company with an existing FCL that impacts a favorable FOCI determination, the FCL will be suspended or terminated unless security measures are taken to remove the possibility of unauthorized access or adverse impacts to contract performance.

d. Any doubt as to whether unacceptable FOCI can be effectively mitigated to the point that affording the applicant access to classified information or matter is clearly consistent with national security will be resolved in favor of the national security.

2. APPLICABILITY.

a. FOCI determinations must be rendered on the following:

(1) Applicants, including industrial; educational; commercial; or any other entity, grantee, or licensee, that have or anticipate executing a contract requiring access authorizations, including individuals contracting as a business. This includes subcontractors of any tier, consulting firms, agents, grantees, and cooperative research and development agreement participants who require security clearances.

(2) All tier parents of applicants when the parent is located in the United States, Puerto Rico, or a U.S. possession or trust territory (48 CFR Section 925.204-73[f]).

b. A FOCI determination is not required for an individual performing work under a consulting agreement (e.g., an individual awarded a contract who has not contracted as a business). Foreign involvement for such individuals is determined and adjudicated through the background investigation conducted for the security clearance.

c. Contractors with existing U.S. Government FCLs are identified in DOE's Safeguards and Security Information Management System (SSIMS) and/or the Department of Defense (DoD) Defense Security Service/Industrial Security Facilities Database (DSS/ISFD). No further FOCI review is required for an applicant registered in either of these systems holding an equal or higher U.S. Government FCL based upon a favorable FOCI determination.

3. ELECTRONIC SUBMISSION/PROCESSING WEB SITE. The Department has an electronic system for submission of FOCI information to DOE. To ensure confidentiality of the information submitted and stored on the system, the site is protected with 128-bit encryption. Applicants must use this system for the submission of FOCI packages, including changes to update their FOCI information. The FOCI Web site may be accessed via an Internet browser at https://doefoci.anl.gov. Electronic signatures are not accepted; therefore a signed original SF 328, Certificate Pertaining to Foreign Interests, executed in accordance with the instructions on the certification section of the SF 328, must either be submitted to the DOE cognizant security office, or retained by the applicant and inspected by the DOE cognizant security office at the applicant's place of business prior to rendering the final FOCI determination.

4. COMMITTEE ON FOREIGN INVESTMENT IN THE UNITED STATES.

a. The Committee on Foreign Investment in the United States (CFIUS) is an interagency committee chaired by the Department of the Treasury under section 721 of the *Defense Production Act of 1950* (50 U.S.C. App. 2170). CFIUS review is a voluntary process which affords an opportunity for foreign investors and U.S. persons entering into a covered transaction to submit the transaction for review by CFIUS to assess the impact of the transaction on national security. DOE policy with regard to CFIUS is found in DOE O 142.5, *Committee on Foreign Investment in the United States*, dated 10-8-10.

b. The CFIUS review and the FOCI and FCL processing actions are carried out in two parallel but separate processes with different time constraints and considerations.

CHAPTER II. FOCI MITIGATION

1. GENERAL. If DOE determines that a company is under FOCI, DOE will determine the extent to which and the manner in which the FOCI may result in unauthorized access to classified information or SNM and the types of actions that will be necessary to mitigate the associated risks to a level deemed acceptable to DOE.

2. FOCI MITIGATION INSTRUMENTS. The affected organization or its legal representatives may propose a plan to negate or reduce unacceptable FOCI; however, DOE has the right and obligation to impose any security method, safeguard, or restriction it believes necessary to ensure that unauthorized access to classified information or matter, or SNM, is precluded. An organization that will not implement the security measures determined necessary by DOE to mitigate its foreign involvement to an acceptable level is ineligible for a FOCI determination and an FCL. Under all methods of FOCI mitigation, management positions requiring security clearances in conjunction with the FCL must be filled by U.S. citizens residing in the United States.

   a. Secretarial Waiver Authority. In accordance with 10 U.S.C. Section 2536, *Award of certain contracts to entities controlled by a foreign government: prohibition,* a contract under a national security program may not be awarded to an entity controlled by a foreign government if it is necessary for the entity to be given access to proscribed information[1] unless a waiver has been granted by the Secretary concerned (i.e., the Secretary of Energy or the Secretary of Defense). Further, if the Secretary decides to grant a waiver under 10 U.S.C. Section 2536(b)(1)(B) for an environmental restoration, remediation, or waste management contract, the Secretary must notify Congress of this decision. The contract may be awarded or the novation agreement executed only after the end of a 45-day period, beginning on the date notification is received by the Senate Committee on Armed Services and the House Committee on National Security.

   b. Controlling Foreign Ownership. A controlling foreign ownership is one in which a non-U.S. citizen(s) owns a majority of the voting securities of the U.S. organization or, if less than 50 percent is foreign-owned, it can be reasonably determined that non-U.S. citizens or their representatives are in a position to effectively control the business management of the U.S. organization. Where the FOCI stems from majority foreign ownership or control, a FOCI mitigation plan may consist of one of the following methods:

[1] Proscribed information is defined as Top Secret (TS); communications security (COMSEC) information, except classified keys used to operate secure telephone equipment (STE); Restricted Data/Formerly Restricted Data as defined in the Atomic Energy Act; special access program (SAP) information; transclassified foreign nuclear information; or sensitive compartmented information (SCI).

(1) Voting Trust Agreement. Under this type of agreement, the foreign owner relinquishes most rights associated with ownership of the company to cleared U.S. citizens approved by the U.S. Government. Foreign owners must transfer legal title of the company to the Trustees. The Voting Trust Agreement does not impose any restrictions on the organization's eligibility to have access to classified information or matter or to compete for classified contracts. A Government Security Committee (GSC) must be established under the Voting Trust to oversee classified, SNM, and export control activities.

(a) All Trustees must become members of the company's governing board

(b) The arrangement must provide for the exercise of all prerogatives of ownership by the Trustees with complete freedom to act independently from the foreign owners, except as provided in the agreement, which may limit the authority of the Trustees by requiring approval from the foreign owners with respect to matters such as:

1 the sale or disposal of the company's assets or a substantial part thereof;

2 pledges, mortgages, or other encumbrances on the company's assets, capital stock or ownership interests;

3 mergers, consolidations, or reorganizations;

4 dissolution of the company; and,

5 filing of a bankruptcy petition.

(c) The Trustees assume full responsibility for the foreign owner's voting interests and for exercising all management prerogatives relating thereto in such a way as to ensure that the foreign owner will be insulated from the company and will solely retain the status of a beneficiary.

(d) The company must be organized, structured, and financed to be capable of operating as a viable business entity independent from the foreign owner.

(2) Proxy Agreement. Like the Voting Trust Agreement, under this arrangement, the foreign owner relinquishes most rights associated with ownership of the company to cleared U.S. citizens approved by the U.S. Government. Under a Proxy Agreement, the foreign owner's voting rights are conveyed to the Proxy Holders by the irrevocable Proxy Agreement.

Legal title to the shares remains with the non-U.S. citizen(s). All provisions of a Voting Trust Agreement applicable to Trustees, including authorized limitations on the powers of the Trustees, must apply to the Proxy Holders. The Proxy Agreement does not impose any restrictions on the organization's eligibility to have access to classified information or matter or to compete for classified contracts. The company must be organized, structured, and financed to be capable of operating as a viable entity independent from the foreign owner. Use of the Proxy Agreement requires the establishment of a GSC to oversee classified, SNM, and export control activities.

(3) Special Security Agreement. A Special Security Agreement may be considered when a U.S. organization is effectively owned or controlled by a foreign interest and the Federal Government has entered into a general security agreement with the foreign government involved. The Special Security Agreement preserves the foreign shareholder's right to be represented on the governing body with a direct voice in the business and management of the company while denying unauthorized access to classified information or matter, or SNM by imposing substantial security and export control measures within an institutionalized set of corporate practices and procedures. SSAs must:

(a) require active involvement in security matters of senior management and certain Board members (outside directors), who must be cleared U.S. citizens;

(b) provide for the establishment of a Government Security Committee (GSC) to oversee classified, SNM, and export control activities;

(c) be based on a Secretarial Waiver as described above if the contract will require access to proscribed information; and

(d) require a National Interest Determination (NID) prior to release of proscribed information to the contractor or its cleared employees to certify that release of such information is consistent with the national security interests of the United States. The NID can be program, project, or contract specific.

c. Non-controlling Foreign Ownership. A non-controlling foreign ownership is one in which a non-U.S. citizen(s) owns less than a majority of the voting securities of the U.S. organization and/or is not in a position to effectively control the business management of the U.S. organization. Where the FOCI stems from non-controlling foreign ownership or control, a FOCI mitigation plan must consist of either Board Resolution or Security Control Agreement methods.

(1) Board Resolution. When a foreign interest does not own voting interests sufficient to elect, or otherwise is not entitled to representation on the company's governing board, a resolution by the governing board will normally be adequate to mitigate the FOCI concerns. The resolution must identify the foreign shareholder and describe the type and number of foreign-owned shares; acknowledge the company's obligation to comply with all security and export control requirements; and certify that the foreign owner does not require, will not have, and can be effectively precluded from unauthorized access to all classified and export-controlled information entrusted to or held by the contractor. Annual certifications must be provided to the DOE cognizant security office acknowledging the continued effectiveness of the resolution. The company must distribute to members of its governing board and to its KMP copies of such resolutions, and report in its corporate records the completion of this distribution.

(2) Security Control Agreement. When a company is not effectively owned or controlled by a foreign interest and the foreign interest is nevertheless entitled to representation on the company's governing board, a Security Control Agreement may be used. There are no access limitations under this type of agreement. However, the SCA requires the imposition of substantial security and export control measures in order to preserve the foreign interest's right to be represented on the board while denying unauthorized access to classified information or matter, or SNM. The SCA requires the same active involvement in security matters of senior management and certain Board members, and the establishment of a GSC, as are required when the Special Security Agreement is used.

d. Limited FCL. A limited FCL may be granted to certain contractors (e.g., a sole source contractor) which are controlled or owned by a foreign interest where FOCI mitigation is not able to be implemented. Access limitations are inherent with granting limited FCLs. Full requirements for granting a limited FCL are set forth in the Facility Clearance section of this attachment.

e. Factors Not Related to Foreign Ownership. When factors not related to ownership are present, positive measures must be put in place to assure that the foreign interest can be effectively mitigated and cannot otherwise adversely affect performance on classified contracts. Examples of such measures include:

(1) modification or termination of loan agreements, contracts and other understandings with foreign interests;

(2) diversification or reduction of foreign-source income;

(3) demonstration of financial viability independent of foreign interests;

(4) elimination or resolution of problem debt;

(5) assignment of specific oversight duties and responsibilities to board members;

(6) formulation of special executive-level security committees to consider and oversee matters that affect the performance of classified contracts;

(7) physical or organizational separation of the contractor component performing on classified contracts;

(8) the appointment of a technology control officer;

(9) adoption of special Board Resolutions; and,

(10) other actions that negate or mitigate foreign influence.

3. TRUSTEES, PROXY HOLDERS, AND OUTSIDE DIRECTORS. The contractor must nominate individuals to serve as trustees, proxy holders, or outside directors, as applicable to the FOCI mitigation plan, subject to the approval of DOE. Individuals who serve in these positions must be:

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

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

c. cleared at the level of the facility's FCL.

4. GOVERNMENT SECURITY COMMITTEE. Under a Voting Trust, Proxy Agreement, Special Security Agreement, or Security Control Agreement, the contractor must establish a permanent committee of its Board of Directors, known as the Government Security Committee (GSC).

a. Unless otherwise approved by DOE, the GSC must consist of voting trustees, proxy holders, or outside directors, as applicable, and those officers/directors who hold security clearances. The chairman of the GSC must be a trustee, proxy holder, or outside director, as applicable to the type of mitigation instrument.

b. Members of the GSC are required to ensure that the contractor maintains policies and procedures to safeguard classified information or matter, SNM, and/or export controlled information entrusted to the organization, and that violations of those

policies and procedures are promptly investigated and reported to the appropriate authority when it is determined that a violation has occurred.

c. The GSC must take the necessary steps to ensure that the contractor complies with U.S. export control laws and regulations and does not take action deemed adverse to performance on classified contracts. A technology control officer (TCO) must be appointed, and a technology control plan (TCP) must be established and implemented.

d. The facility security officer (FSO) must be designated as the principal advisor to the GSC and must attend GSC meetings. The chairman of the GSC must concur with the appointment and replacement of FSOs selected by management. The FSO and TCO functions must be carried out under the authority of the GSC.

5. TECHNOLOGY CONTROL PLAN. A TCP approved by DOE must be developed and implemented by those companies cleared under a Voting Trust Agreement, Proxy Agreement, SSA, and SCA and when otherwise deemed appropriated by DOE. The TCP must prescribe all security measures determined necessary to reasonably foreclose the possibility of inadvertent access by non-U.S. citizen employees and visitors, including the foreign shareholder(s) and affiliates, to information for which they are not authorized. The TCP must also prescribe measures designed to ensure that access by non-U.S. citizens is strictly limited to only that specific information for which the appropriate Federal Government disclosure authorization has been obtained (e.g., an approved export license or technical assistance agreement.) Use of unique badging, escort, segregated work areas, security awareness training programs, and other measures must be included as appropriate and documented in the TCP and in the facility security plan.

SECTION 3. SAFEGUARDS AND SECURITY AWARENESS

1. OBJECTIVE. To inform individuals of their safeguards and security (S&S) responsibilities and to promote continuing awareness of good security practices.

2. PURPOSE. The safeguards and security awareness program is responsible for communicating their personal security responsibilities to all individuals at a facility or site. In addition, for individuals who are granted access to classified information or matter, or special nuclear material (SNM), the security awareness program provides the means to instruct these individuals in their duties and responsibilities related to the access afforded to them and reiterate those duties and responsibilities upon termination of access. The program also provides, through supplementary awareness activities, a method to continuously reinforce good security practices.

3. DEFINITION. For purposes of this directive, the term "safeguards and security awareness" refers to all site introductory briefings on security topics, briefings conducted for access to classified information or matter or special nuclear material, formal refresher briefings covering access to classified or SNM and/or other security topics, termination briefings provided upon termination of access to classified or SNM, and all other activities, presentations, and materials intended to educate or raise the awareness of individuals as to their responsibilities within the facility/site security program.

4. REFERENCES.

   a. E.O. 13526, *Classified National Security Information*, dated 12-29-09.

   b. 10 CFR Part 1017, *Identification and Protection of Unclassified Controlled Nuclear Information*.

   c. 32 CFR Part 2001, *Classified National Security Information*, Subpart G, "Security Education and Training."

   d. 32 CFR Part 2001, *Classified National Security Information*, Subpart H, "Standard Forms."

   e. E.O. 12829, *National Industrial Security Program*, dated 01-26-93

   f. DoD 5220.22-M, *National Industrial Security Program Operating Manual (NISPOM)*.

   g. Information Security Oversight Office (ISOO) Classified Information Nondisclosure Agreement (Standard Form 312) Briefing Booklet.

   h. The CRD to DOE O 475.2A, *Identifying Classified Information*, dated 2-1-2011.

i. DOE O 471.1B, *Identification and Protection of Unclassified Controlled Nuclear Information*, contractor requirements document, dated 3-1-2010.

j. DOE O 471.3, *Identifying and Protecting Official Use Only Information*, contractor requirements document, dated 1-13-2011.

k. The CRD to DOE O 475.1, *Counterintelligence Program*, dated 10-4-04.

5. REQUIREMENTS. Contractors are responsible for ensuring that the following activities are accomplished for the security awareness program. Procedures applicable to the security awareness program must be documented in facility or site security plans.

a. Ensure that security briefings are conducted in accordance with the requirements of this section for all covered individuals.

b. Ensure that, if briefings are conducted through electronic means, a method exists to ascertain and verify that the individual completes all required content prior to receiving credit for the briefing.

c. Ensure that all individuals granted DOE security clearances (access authorizations) execute a Standard Form (SF) 312, Classified Information Nondisclosure Agreement, prior to being granted access to classified information or matter, or SNM.

d. Ensure that non-DOE personnel granted unescorted access to a facility or site security area receive appropriate awareness information (e.g., information on prohibited and controlled articles).

e. Develop and issue supplemental awareness materials, tailored to local facility/site conditions and issues and appropriate for both cleared and non-cleared employees and visitors, to make them aware of their security responsibilities.

f. Ensure that executed SF 312 forms and other records related to the security awareness program are maintained in accordance with ISOO and DOE records requirements.

g. Ensure that individuals are appropriately authorized to witness and accept the SF 312 on behalf of the United States and that such designations of authority are documented in the current facility/site security plan.

h. Determine administrative actions to be taken when individuals fail to complete the requirement for annual refresher briefings.

i. Ensure that information of counterintelligence concern is reported to the supporting counterintelligence office.

6. BRIEFINGS. Safeguards and security awareness programs must include an initial briefing for all individuals who are issued a DOE security badge; comprehensive, refresher, and termination briefings for all individuals with a DOE security clearance for access to classified information or matter, or SNM; and appropriate site-specific awareness information for non-DOE personnel granted unescorted access to Departmental security areas. S&S awareness refresher briefings must address site-specific knowledge and needs, S&S interests, and potential threats to the facility/organization. Contents must be reviewed regularly and updated as necessary. Contents of briefings concerning incidents of counterintelligence concern, deliberate compromises, and foreign interactions must be coordinated with the supporting counterintelligence office. Records must be maintained in a manner that provides an audit trail that verifies an individual's receipt of the briefings.

   a. Initial Briefing. DOE Federal and contractor employees who receive a DOE security badge must receive an initial briefing before they are given unescorted access to other than public areas of the facility/site.

      (1) Content.

         (a) overview of the DOE facility/organization's mission;

         (b) overview of facility/organization's major S&S program responsibilities;

         (c) access control;

         (d) escort procedures;

         (e) protection of Government property and badge procedures;

         (f) identification of controlled and prohibited articles;

         (g) protection of controlled unclassified information (CUI), including official use only information;

         (h) procedures for reporting incidents of security concern (e.g., attempts to gain unauthorized access to the facility or to classified information or matter); and

         (i) identification of classification markings.

      (2) Scheduling. The initial briefing must be completed before personnel assume their duties. A transferred individual must complete a site-specific initial briefing before assuming duties at the new site.

(3) Documentation. Initial briefing records must be maintained. Records may be maintained in conjunction with badging records or other records pertaining to access control.

b. Comprehensive Briefing. An individual must receive a comprehensive briefing upon receipt of a security clearance and before receiving initial access to classified information or matter, or special nuclear material (SNM).

(1) Content. The content for the comprehensive briefing must include the following items.

(a) Basic classification security policies and principles:

1 definition of classified information or matter;

2 purpose of DOE classification program;

3 levels and categories of classified information or matter;

4 damage criteria associated with each classification level; and

5 classification awareness requirements contained in the CRD to DOE O 475.2A, *Identifying Classified Information*, as applicable.

(b) Classified information or matter protection elements:

1 procedures for protecting classified information and matter;

2 definition of unauthorized disclosures;

3 penalties for unauthorized disclosures;

4 conditions and restrictions for access to classified information or matter;

5 individual's S&S reporting requirements;

6 legal and administrative sanctions for security infractions and violations of law;

7 protection and control of classified information or matter, and controlled unclassified information, including telecommunications and electronic transmissions and official use only information;

8 information pertaining to security badges, security clearance levels, and access controls;

9 responsibilities associated with escorting;

10 targeting and recruitment methods of foreign intelligence services;

11 general information concerning the protection of SNM, if applicable; and

12 purpose and requirements of, and responsibilities for, the SF 312.

(c) Personnel security elements:

1 purpose of the personnel security program;

2 sources of legal authority and guidance;

3 the access authorization process;

4 key terms associated with adjudications;

5 adjudication factors;

6 due process; and

7 individual reporting requirements.

(2) Scheduling. Comprehensive briefings must be completed before individuals are granted access to classified information or matter, or SNM. A comprehensive briefing is also required when a security clearance is extended or transferred to another DOE facility/organization. Initial and comprehensive briefings may be combined at the discretion of facility/site security management. Under such circumstances, the briefing must include information prescribed for both initial and comprehensive briefings.

(3) Documentation. Documentation of the comprehensive briefing must be maintained. The SF 312 must be used to document the first comprehensive briefing after the grant of a security clearance, and may be used to document subsequent comprehensive briefings.

c. Refresher Briefing. Cleared individuals must receive annual refresher briefings. Agreements between DOE elements and/or contractor organizations may be established to ensure that individuals temporarily assigned to other DOE locations

receive refresher briefings on schedule. Failure to complete the annual refresher briefing by an individual who holds a security clearance will result in administrative actions determined by the cognizant security office, including possible administrative termination of the security clearance, until such time as the individual has complied with the briefing requirement. The processing personnel security office responsible for the clearance must be notified in accordance with paragraph d(3) below when a clearance is terminated for this reason.

(1) Content. Refresher briefings must selectively reinforce the information provided in the comprehensive briefing based upon current facility/site-specific security issues as well as counterintelligence (CI) awareness, and address the classification refresher requirements contained in the CRD to DOE O 475.2A, as applicable.

(2) Scheduling. Refresher briefings must be conducted each calendar year at approximately 12-month intervals.

(3) Documentation. Documentation of refresher briefings must be maintained for individuals until their next briefing. Documentation may be in electronic or hard copy format. Documentation must include the ability to identify individuals who have not met the refresher briefing requirement.

d. Termination Briefing. A termination briefing is required whenever a security clearance has been or will be terminated. Termination briefings must reiterate to the individual the continuing responsibility not to disclose classified information or matter to which they had access, the potential penalties for noncompliance, and the obligation to return all unclassified controlled and classified documents and materials in the individual's possession to the cognizant security office or to the DOE.

(1) Content. The content for the termination briefing must include:

(a) information contained in the numbered items of the Security Termination Statement Form (DOE F 5631.29 or successor form);

(b) information contained in items 3, 4, 5, 7, and 8 of the SF 312;

(c) penalties for unauthorized disclosure of classified information or matter as specified in the Atomic Energy Act and pertinent sections of 18 U.S.C.;

(d) penalties for unauthorized disclosure of Unclassified Controlled Nuclear Information (UCNI).

(2) Scheduling. The termination briefing must be conducted on the individual's last day of employment, the last day the individual possesses

a security clearance, or the day it becomes known that the individual no longer requires access to classified information or matter, or SNM, whichever is sooner. If the individual is not available for the termination briefing, the completed but unsigned security termination statement and an explanation of the circumstances surrounding the termination and why the signature could not be obtained must be submitted to the processing personnel security office.

(3) Required notification. When an individual no longer requires a security clearance/access authorization, or when a clearance/access authorization is administratively terminated, the processing personnel security office must be notified electronically or verbally within two working days to be followed by submission to that office of a completed DOE F 5631.29, Security Termination Statement.

(4) Documentation. Records documenting receipt of the termination briefing must be maintained. This briefing must be documented by completing the Security Termination Statement Form (DOE F 5631.29) or by written notice.

7. CLASSIFIED INFORMATION NONDISCLOSURE AGREEMENT (SF 312).

a. Administration.

(1) As a condition of access, a cleared individual must complete an SF 312 either at the time of, or after, the comprehensive briefing and before accessing classified information or matter, or SNM.

(2) Any individual who refuses to execute an agreement must be denied access to classified information or matter, or SNM and reported to the cognizant security office. The processing personnel security office responsible for the clearance must be notified of the refusal to sign the SF 312 within 48 hours of the refusal.

(3) In most cases, the same person may serve as both the witness and acceptor of the SF 312 as long as that person has been authorized to accept the signed form on behalf of the United States. Any DOE Federal employee may witness the execution of the SF 312 by a Government or non-Government employee. A DOE Federal employee specifically authorized to do so may accept on behalf of the United States an SF 312 executed by either an employee of DOE or a contractor employee whose clearance is granted by DOE. An authorized representative of a contractor who has been specifically designated to act as an agent of the United States may witness and accept an SF 312 executed by an employee of the same organization.

b. Retention. The original SF 312 or a legally enforceable facsimile must be retained in accordance with General Records Schedule (GRS) 18, item 25, published by the National Archives and Records Administration (NARA), as supplemented by the DOE Administrative Records Schedule (ARS) 18. Contractors may retain an original SF 312 as long as the cleared individual is employed by the contractor. Original SF 312s retained by contractors must be sent to DOE upon the terminations of employment of contractor employees, in accordance with 32 CFR Part 2003.20.

c. Storage. The SF 312 must be stored in accordance with 32 CFR Section 2001.80(d)(2) and *DOE Administrative Records Schedule 18*. Personnel security files must not be used as a storage location for the agreements. Contractors are not permitted to provide storage for retired SF 312s on behalf of the DOE unless their facilities are approved in accordance with NARA standards for records storage facilities. The originals or legally enforceable facsimiles of the executed agreements must be retained in a file system from which they can be expeditiously retrieved if the U.S. Government seeks enforcement or subsequent employers require confirmation of execution.

8. SUPPLEMENTARY AWARENESS ACTIVITIES.

a. Purpose. Supplementary security awareness activities must be conducted to ensure that individuals, whether cleared or uncleared, are aware of their S&S responsibilities and good security practices. These awareness activities may be carried out in any form which meets the needs of the facility/site, including but not limited to briefings, presentations, posters, newsletters, token items such as badge lanyards, employee recognition, computer notices, fliers, tabletop cards, etc. Activities may address general security concerns or may be tailored to specific problems or issues as indicated by incident reports, employee questions, or management communications.

b. Records Retention. All programmatic records must be maintained in accordance with the NARA/DOE-approved records retention and disposition schedules.

SECTION 4. CONTROL OF CLASSIFIED VISITS

1. OBJECTIVE. Classified information and matter must be protected by ensuring that only persons with the appropriate security clearances, need-to-know, and programmatic authorizations are afforded access during visits where the release or exchange of such information is involved.

2. PURPOSE. Control of classified visits ensures that access to classified information by cleared U.S. citizens or individuals from foreign governments visiting DOE facilities is controlled in accordance with the mission of the Department and is consistent with national laws and regulations and international treaties and agreements.

3. DEFINITIONS.

   a. Classified visit. A visit that will involve or is expected to involve access to, or an exchange of, classified information.

   b. Foreign national. Any person who is not a U.S. citizen.

   c. Visitor. An individual who is not an employee or contractor of the facility/site and does not work full or part-time at the site.

   d. Restricted Data access authorization. For purposes of classified visits by individuals from Other Government Agencies (OGA) other than DoD, NASA, and NRC, this term identifies access granted in connection with a visit to a cleared individual who has an official government need to access Restricted Data (RD) or special nuclear material (SNM). This access does not require conversion of the prospective visitor's existing security clearance to a DOE L or Q access authorization, provided that: an authorized DOE official has verified the individual's OGA security clearance through DOE and national-level personnel security electronic databases, and made a need-to-know determination with respect to the specific RD and/or SNM to be disclosed during the visit; and the individual has executed an acknowledgement of receipt of a briefing on safeguarding RD and/or SNM.

4. REFERENCES.

   a. 42 U.S.C. Chapter 23, *Atomic Energy Act of 1954, as amended*.

   b. 42 U.S.C. Section 2455(b) (Section 304[b] of the *National Aeronautics and Space Act of 1958*).

   c. 10 CFR Part 1016, *Safeguarding of Restricted Data*.

   d. 10 CFR Part 1045, *Nuclear Classification and Declassification*.

e. 32 CFR Part 2001, *Classified National Security Information*, Subpart E, "Safeguarding."

f. E.O. 13526, *Classified National Security Information*, dated 12-29-09.

g. E.O. 12968, *Access to Classified Information*, dated 8-4-95.

h. E.O. 12829, *National Industrial Security Program*, dated 01-26-93.

i. DoD 5220.22-M, N*ational Industrial Security Program Operating Manual (NISPOM)*.

j. DoD Defense Security Service (DSS) Industrial Security Letters (ISLs), available at http://www.dss.mil/isp/fac_clear/download_nispom.html (Note: ISLs do not automatically impose requirements, but may contain useful clarifications of existing NISPOM provisions.).

k. The CRD to DOE O 475.1, *Counterintelligence Program*, dated 10-4-04.

5. REQUIREMENTS. Contractors are responsible for ensuring that the following activities are accomplished for the classified visits program at facilities and sites under their cognizance. Procedures applicable to classified visits must be documented in facility or site security plans.

a. Ensure that the number of classified visits is held to a minimum.

b. Ensure that each classified visit is necessary, that the purpose of the visit cannot be achieved without providing access to or a disclosure of classified information, and that any disclosure of classified information or matter during visits occurs only for a lawful and authorized U.S. Government purpose.

c. Ensure that local procedures are established for processing and handling classified visits to facilities under their cognizance by cleared U.S. citizens and for processing requests for classified visits by cleared individuals from their facilities to other locations.

d. Ensure that procedures are established for processing and handling visits by foreign nationals to facilities under their cognizance in accordance with governing international agreements or treaties.

e. Ensure that, for visits by foreign nationals, appropriate procedural limitations are developed and followed for the visit to preclude access to information not related to the visit and the scope of the international treaty or agreement governing the visit.

f. Establish procedures to ensure that classified visit requests are sent and received through the DOE cognizant security office and the appropriate security offices of other Federal government agencies.

g. Establish procedures to ensure that, for classified visits involving access to RD or SNM by cleared U.S. citizens who are not otherwise authorized for such access, the prospective visitor has been approved for such access by the facility/site's authorized DOE Federal official, has received an appropriate briefing concerning the protection of RD and/or SNM prior to being given access, and has signed an acknowledgement that the briefing has been received.

h. Establish procedures to ensure that access granted under paragraph g. above is tracked and maintained as part of the site classified visits file and is not entered into any clearance tracking database or extended for any purpose outside the approved classified visit.

i. Establish procedures to ensure that all classified information or matter, including the visitor's personal notes, to be removed by individuals granted access under paragraph g. above is sent through the DOE cognizant security office to the established classified mailing address listed in SSIMS for the facility which the individual represents. Hand-carrying of classified information from DOE premises by individuals granted RD access in connection with a classified visit is strictly prohibited.

6. VISITS TO DOE FACILITIES BY CLEARED U.S. CITIZENS OTHER THAN DOE PERSONNEL.

a. For all classified visits to DOE and DOE contractor facilities, the following must be established and verified:

(1) the identity of the visitor;

(2) the level and type of clearance held by the visitor, which must allow access to the information to be disclosed;

(3) that the visit is for an official purpose for which the individual has a legitimate need to know and to access the classified information or matter to be disclosed.

b. Appropriate procedural limitations (e.g., use of escorts in limited/restricted areas) must be in place to ensure that the visitor has access only to information for which the individual has a verified need, and that access to other classified information or matter is precluded.

c. Requests for visits and access to specific types of facilities and information must be referred to and approved by the appropriate office before any access is granted:

(1) for weapons programs, nuclear materials production facilities, or sensitive nuclear materials production information, the Deputy Administrator for Defense Programs;

(2) for uranium enrichment plants or facilities engaged in uranium enrichment technology development, including advanced isotope separation technology, the Office of Nuclear Energy;

(3) for Naval Nuclear Propulsion facilities, the Deputy Administrator for Naval Reactors.

d. Visits involving access to Restricted Data (RD) or special nuclear material (SNM) when the visitor does not hold a DOE access authorization require specific approval by DOE/NNSA Federal officials authorized to give such approval. Approval is based upon verification through DOE and national-level personnel security electronic databases that the individual holds an appropriate final security clearance, unless the individual is in one of the categories described below. If access to Nuclear Weapon Data Sigma information is required, the visit request must be submitted on DOE F 5631.20, *Request for Visit or Access Approval*, or successor form, and the form must specifically indicate the requirement for such access.

(1) DOE accepts the Q and L access authorizations granted by the Nuclear Regulatory Commission (NRC) as valid for access to RD. Visits by NRC employees, consultants, contractors, or subcontractors who require access to weapon data, sensitive nuclear materials production information, atomic vapor laser isotope separation technology, or uranium enrichment technology or entry into a DOE classified weapon or production facility must be approved by the appropriate Departmental element office. Visits may be requested using either the DOE F 5631.20 or NRC Form 277. NRC identification badges cannot be used as authority for visits.

(2) For DoD and NASA employees, consultants, contractors, or subcontractors, access to RD must be requested on a DOE F 5631.20 or successor form. Individuals from NASA may also use NASA Form 405, Request for Access Approval. A memorandum or electronic message signed by the certifying official may be used unless access to Nuclear Weapon Data is required. For NASA, the visit request must include a certification that the matter to which access is requested relates to aeronautical and space activities. Requests must be forwarded for approval to the appropriate Departmental element with jurisdiction over the information to which access is requested. Access to critical nuclear weapon design information must be specifically requested.

(3) Prior to being given access, OGA employees and their contractors who are granted access to RD and/or SNM in connection with a classified visit

must receive an appropriate briefing concerning the protection of RD and SNM and must sign an acknowledgement indicating his/her understanding that access will be terminated at the end of the visit period.

(4) RD and/or SNM access granted in connection with a classified visit must be tracked as part of the local site classified visit tracking process, and records of such access must be maintained in the classified visit files. This type of access will not be identified as a Q or L access authorization, will not be entered in the DOE Central Personnel Clearance Index or other clearance tracking databases, and cannot be extended for any purpose outside the approved classified visit.

(5) This process does not apply to classified visits by non-U.S. citizens.

7. VISITS BY CLEARED DOE PERSONNEL TO OTHER DOE FACILITIES.

a. Unless local site procedures require, or access to certain facilities or programs as described below will take place, formal visit requests are not required for visits by DOE Federal and contractor personnel to other DOE sites. The DOE security badge will serve as evidence of DOE security clearance/access authorization for internal DOE visits.

b. Visitors who require access to weapon data (classified Secret or Top Secret), sensitive nuclear materials production information, inertial confinement fusion data, atomic vapor laser isotope separation technology, uranium enrichment technology, or facilities specifically designated by a Departmental element, must obtain approval from the responsible office prior to the visit.

c. DOE F 5631.20 must be used by DOE Federal and contractor employees to obtain programmatic approval for access to Sigmas 14, 15, and/or 20. Approval for access must be obtained from the Deputy Administrator for Defense Programs.

d. Cleared DOE contractor employees who are foreign nationals may visit other facilities only under the access restrictions which apply to their clearances.

8. CLASSIFIED VISITS TO DOE FACILITIES BY NON-U.S.CITIZENS.

a. For all classified visits by non-U.S. citizens to DOE and DOE contractor facilities, the following must be established and verified:

(1) the identity of the visitor;

(2) assurance that the sharing of specific classified information with the foreign national is covered by an existing treaty or agreement;

(3) receipt of security assurances from the appropriate foreign embassy;

(4) verification that the appropriate DOE Federal official has approved the sharing of the specific information to be disclosed during the classified visit.

b. DOE contractor employees may be designated to serve as hosts for classified visits by non-U.S. citizens. A host must be a U.S. citizen with an access authorization equal to or higher than the overall classification level of the visit. The host must ensure that:

(1) foreign nationals are not granted access to classified information before approval is received from the appropriate designated authority with programmatic responsibility;

(2) foreign nationals are precluded from any access to classified information outside the scope of the international agreement or treaty governing the visit and/or any limitations set by the approval authority with programmatic responsibility, and sharing of classified information is in accordance with the protocols specifically outlined in the agreement or treaty governing the visit (e.g., level, category, and type of classified information, protection procedures for incoming classified foreign government information, security clearance verification, transmission protocols for classified information during and after the visit, post-visit documentation, etc);

(3) appropriate procedural limitations (e.g., use of escorts in limited/restricted areas) are in place to ensure that the foreign visitor has access only to information permitted by the applicable international agreement or treaty for which the individual has a verified need, and that access to all other classified information or matter is precluded.

c. Requests for visits and access by foreign nationals to specific types of facilities and information must be referred to and approved by the appropriate Headquarters office:

(1) for visits to uranium enrichment plants or facilities and access to classified information on uranium enrichment technology development, including advanced isotope separation technology, the Office of Nuclear Energy;

(2) for visits and access to classified information in connection with the military application of atomic energy under 42 U.S.C. Section 2164 and 42 U.S.C. Section 2121, the Deputy Administrator for Defense Programs;

(3) for visits and access to classified information in connection with nonproliferation, international security, or International Atomic Energy Agency requirements, the Deputy Administrator for Defense Nuclear Nonproliferation;

(4) for visits and access to classified information in connection with naval nuclear propulsion, the Deputy Administrator for Naval Reactors;

(5) for visits and access to classified information in connection with Sensitive Compartmented Information, the Office of Intelligence and Counterintelligence.

9. DOCUMENTATION. Reports of classified visits must be maintained in accordance with *DOE Administrative Records Schedule 18*, paragraph 17.1.

SECTION 5. SAFEGUARDS AND SECURITY TRAINING PROGRAM

1. OBJECTIVE. To establish programs that ensure personnel are trained to a level of proficiency and competence that ensures they are qualified to perform assigned safeguards and security (S&S) tasks and/or responsibilities.

2. PURPOSE. The DOE Quality Assurance Program mandates that all DOE facilities and sites train and qualify their personnel to be capable of performing assigned work, and that continuing training be provided to maintain job proficiency. This section describes the requirements for establishing training for personnel working in S&S programs.

3. DEFINITION. As used in this section, training means the process of providing for and making available to an employee a planned, prepared, and coordinated program, system, or routine of instruction in S&S topical areas applicable to the employee's position that will improve individual and organizational performance and assist in achieving the Department's mission and performance goals.

4. REFERENCES.

   a. DOE O 226.1B, *Implementation of Department of Energy Oversight Policy*, dated 4-25-11, contractor requirements document.

   b. DOE O 350.1 chg 3, *Contractor Human Resource Management Programs*, dated 9-30-96, contractor requirements document.

   c. DOE O 413.3B, *Program and Project Management for the Acquisition of Capital Assets*, dated 11-29-10, contractor requirements document.

   d. DOE O 414.1D, *Quality Assurance*, dated 4-25-11, contractor requirements document.

   e. DOE-STD-1171-2009, *Safeguards and Security Functional Area Qualification Standard*.

   f. DOE-STD-1123-2009, *Safeguards and Security General Technical Base Qualification Standard*.

5. REQUIREMENTS. Contractors are responsible for ensuring that security training activities are accomplished at facilities and sites under their cognizance. Procedures applicable to S&S training must be documented in facility or site security plans.

   a. The S&S training program for each facility must encompass all program elements which are performed by employees working at that location. The content of training (initial, refresher, and on-the-job) must be consistent with the knowledge

and skills required to perform assigned S&S tasks and/or responsibilities as determined by valid and complete job analyses.

b. Individual training needs must be evaluated against a job or functional analysis of the position to ensure that appropriate job-related training is identified. Training requirements must be determined by analyzing needs, the job or function, and/or desired performance. Analyses must be conducted to ensure that training courses identify and address the requirements of the job competencies.

c. Training courses must be produced using a systematic approach that includes at least analysis, design, development, implementation, and evaluation phases.

d. Training that meets analysis requirements can be provided by external resources such as commercial vendors or other government training agencies. Training products procured from these resources must be evaluated at the site level for consistency with DOE policy and needs.

e. Evaluation of training must be performed to ensure that instructional objectives are met and to determine overall effectiveness. Knowledge and/or performance-based testing must be used to measure the knowledge and/or skills acquired from training programs.

f. Accurate and complete employee training records that contain dates of course attendance, course title, and scores/grades achieved (where applicable) must be maintained in accordance with DOE Administrative Records Schedule 1, Personnel Records.

g. Training plans that project training derived from a valid needs analysis for the forthcoming year must be developed annually.

h. In accordance with the NISPOM, facility/site security officers must complete training appropriate to their position and the security operations conducted at their assigned facilities. This training should be completed within 1 year of appointment to the position of FSO.

SECTION 6. RESTRICTIONS ON THE TRANSFER OF SECURITY-FUNDED TECHNOLOGIES

1. OBJECTIVE. Protect and control classified and unclassified controlled Office of Health, Safety and Security (HSS) funded technology, other Technology Development Program (TDP)-related information, and protection practices and expertise that may be provided to recipients who are not Department of Energy (DOE) Federal or contractor employees.

2. PURPOSE. This section establishes DOE policy for ensuring that safeguards and security (S&S) funded technology, TDP information, and protection practices and expertise are disseminated outside the DOE only when such dissemination is in compliance with national laws and regulations.

3. REFERENCES.

   a. E.O. 12829, *National Industrial Security Program*, dated 01-26-93.

   b. DoD 5220.22-M, *National Industrial Security Program Operating Manual (NISPOM)*.

   c. 10 CFR Part 110, *Export and Import of Nuclear Equipment and Material*.

   d. 10 CFR Part 810, *Assistance to Foreign Atomic Energy Activities*.

   e. 10 CFR Parts 730 to 780, *Export Administration Regulations*.

   f. 22 CFR Parts 120 to 130, *International Traffic in Arms Regulations*.

   g. 31 CFR Parts 500 to 598, *Office of Foreign Assets Control (OFAC), Department of the Treasury*.

4. REQUIREMENTS. Contractors are responsible for ensuring that activities related to the transfer of security-funded technologies are accomplished at facilities and sites under their cognizance. Procedures applicable to the transfer of security-funded technologies must be documented in facility or site security plans.

   a. General. The dissemination in any form of HSS-funded classified and/or unclassified controlled technology, other TDP S&S-related information, or protection practices/expertise to individuals or organizations outside the Department and its operational facilities is prohibited until the following has taken place:

      (1) verification of the recipient's capability to protect and control the information consistent with Department S&S and classification and control policies;

(2) a determination that the intended recipient has a strict need-to-know; a security clearance or access authorization at the appropriate level for any classified information; and that the Department's ability to protect its facilities and assets will not be weakened or degraded by the transfer in question; and

(3) approval of the transfer is obtained in accordance with the requirements for a risk assessment and the review and approval process set forth below, and with applicable Export Control laws and regulations.

b. Risk Assessment. An assessment of the risks for unauthorized use/transfer of classified technology, information, or practices must be conducted before release of the technology/information. The risk assessment must be used as the basis for approving or denying proposed transfers. Proposed release must be handled on a case-by-case basis because eligibility criteria are determined by both the type of information or technology and the intended recipient. The following factors must be addressed:

(1) a determination as to whether the applicant is eligible to receive a specific type of information and/or technology. No person is entitled solely by virtue of rank, position, or access authorization or security clearance to have access to classified or unclassified controlled HSS-funded technology, information or protection practices/expertise;

(2) relevance of and impact on the subject information or technology to the protection of Departmental facilities and assets;

(3) ability of the intended recipient to protect the information and/or technology in a manner equivalent to minimum security standards required by the Department.

c. Review and Approval Process. Reviews to determine if Export Control laws and processes apply must be conducted and the general and/or specific authorization (including any required license) from the appropriate authority must be obtained. Coordination and approval must include the Departmental element and the Chief Health, Safety, and Security Officer. Reports must be made in accordance with Export Control laws as applicable.

ATTACHMENT 4. DEPARTMENT OF ENERGY TACTICAL DOCTRINE

This Attachment provides information and/or requirements associated with DOE O 470.4B as well as information and/or requirements applicable to contracts in which the associated CRD (Attachment 1 to DOE O 470.4B) is inserted.

1. INTRODUCTION.

   a. Overview. The establishment of Departmental doctrine governing the defense of sensitive national security assets is necessary to ensure the uniform application of effective security measures throughout the complex. This attachment is the condensed expression of the Department's fundamental approach to protecting nuclear weapons and components, special nuclear material (SNM), or targets subject to radiological or toxicological sabotage and must be employed in the development of defensive planning for the protection of such assets at fixed sites. Application of the elements of this doctrine at other facilities or sites is optional. In keeping with the development of higher standards for individual training and fitness, aggressive small unit tactics must be employed within the bounds of a well-defined and constructed area defense that contains fixed strong points, obstacles/barriers, advanced detection and assessment capabilities, and employs coordinated fire planning, updated weapon systems, and armored vehicles. The tactical team, consisting of two or more security police officers (SPOs) is the foundation of the Tactical Doctrine's protective force element, enabling more effective command, control, and communications.

   b. Purpose of an Armed Protective Force (PF). Within DOE, armed PFs exist to deter and to defeat terrorist or other adversarial actions that could have major national security consequences; primarily, unauthorized access to nuclear weapons and components, special nuclear material, or targets subject to chemical, biological, or radiological sabotage or that contain a unique capability that must be protected. Given the limited availability of armed PFs, they shall not be used to:

      (1) perform routine, repetitive tasks that are not related directly to target protection;

      (2) perform access control functions that can be better accomplished through automation;

      (3) act as administrative escorts for construction projects or service personnel (unless required for protection of assets); or

      (4) staff posts that offer convenience to management and/or employees.

2. REFERENCES.

a. *The Evolution of US Army Tactical Doctrine, 1946-76,* Maj. Robert A Doughty, Combat Studies Institute, 1979.

b. *Warfighting,* Marine Corps Doctrinal Publication 1, U.S. Marine Corps, 6-20-97.

c. *Military Operations on Urbanized Terrain (MOUT),* Basic Officer Course, B0386, U.S. Marine Corps.

d. *Defensive Fundamentals I,* Basic Officer Course, B0337, U.S. Marine Corps, The Basic School, Marine Corps Combat Development Command, Quantico, Virginia.

e. *Defensive Fundamentals II,* Basic Officer Course, B0339, U.S. Marine Corps, The Basic School, Marine Corps Combat Development Command, Quantico, Virginia.

f. *Defensive Fundamentals III,* Basic Officer Course, B0349, U.S. Marine Corps, The Basic School, Marine Corps Combat Development Command, Quantico, Virginia.

g. *Defensive Sandtable Exercise Packet,* Officer Course, B0349.8 and BO345.8, U.S. Marine Corps.

h. Department of the Army FM-3, *Operations: Military Operations,* 14 June 2001.

i. Department of the Army FM 3-90, *Operations: Tactics,* 4 April 2001.

j. Department of the Army FM 21-75, *Operations: Combat Skills of the Soldier,* 3 August 1984.

k. *The Principles of War,* Carl von Clausewitz, "On War," 1832.

l. *The Secret of Future Victories,* Paul F. Gorman, Gen. (Retired), U.S. Army, 1992.

3. TACTICAL DOCTRINE.

a. Concept. In general, at Category I SNM or radiological/toxicological sabotage target facilities within the DOE, defensive plans will involve an area defense with fixed strong points, or fighting positions, that encompass a target and lie within a concentric arrangement of intrusion detection systems and barriers designed to detect, delay, and engage the adversary as far from the target as possible. An armed protective force (PF) consisting of highly trained, motivated, and skilled tactical units/teams will be positioned on, or in proximity to, each target. Early detection will permit interdiction by fixed and/or mobile response teams using fire and maneuver techniques to deny further access to adversaries and/or to channel them into attrition areas covered by interlocking bands of fire from hardened fighting positions.

b. Defensive Planning Principles.

(1) Prepare the Defensive Area.

(a) Prepare a barrier plan to:

1 Minimize the number of access points and/or avenues of approach.

2 Channel the adversary into attrition areas by use of barriers and preplanned, interlocking bands of fire.

3 Control the high ground, either by physical presence or by weapons fire.

(b) Prepare a defensive fire plan to ensure that:

1 clear fields of fire and observation across the battlefield are maintained;

2 defensive positions are mutually supporting;

3 high volumes of fire can be brought onto key terrain features, obstacles, and along expected routes of approach; and

4 the volume of fire brought upon an adversary increases as a target area is approached.

(2) Integrate All Aspects of the Defensive Plan.

(a) Employ multiple layers of detection.

(b) Employ multiple layers of delay (e.g., barriers/obstacles).

(c) Integrate technology, such as remotely operated weapon systems ROWS), active denial systems, and advanced detection and observation systems, with response force tactics.

(d) Ensure that barriers are covered by weapons fire.

(e) Ensure that the entire defensive perimeter is covered by interlocking fields of fire from mutually supporting positions.

(f) Where feasible, control the configuration of the battlefield by eliminating anything that could provide potential adversary cover and/or concealment.

(g) Ensure that likely avenues of approach are defended with sufficient force to compel decisive engagements with the adversary.

(h) Protect defenders by employing hardened fighting positions situated for mutual support.

(i) Establish supplementary defensive positions.

(j) Prepare to maneuver forces to attack and to defeat an adversary whose progress is delayed by engagement with defensive fire.

(3) Make the Adversary Fight to the Target.

(a) Adversary detection and engagement must occur as far from the target as possible.

(b) Plan for the assessment of remote alarms to identify the number of adversaries, thereby helping to differentiate between diversionary attacks and the main force. If protective forces are used for assessment:

1 plan for staged withdrawal of forces dispatched to assess remote alarms to prepared supplementary defensive positions.

2 plan for overwatch of assessment forces with long range weapons from within the defensive perimeter.

(c) Coordinate barrier and fire control planning to ensure that the adversary will be subjected to high volumes of fire in exposed positions prior to entry into the defensive perimeter.

(d) Ensure adequate standoff for vehicle-borne improvised explosive devices (VBIEDs).

(e) Limit the ability of airborne improvised explosive devices to impact key defensive positions and primary target buildings.

(4) Make the Target Location Deadly.

(a) Use technology to distract, interrupt, disable, or neutralize anyone who has obtained unauthorized access to target locations.

(b) Include considerations for re-entry and recapture of target locations in all barrier and response plans.

(5) Manage the Site Population.

(a) Limit the number of personnel, vehicles, and equipment in the target areas at all times.

(b) Develop formal site-specific procedures for the disposition of workers in the event of an attack.

1 If the tactical conditions permit, workers may be evacuated to safe areas from prospective target locations and likely avenues of approach.

2 Sheltering in place may be the best option. Workers should be provided with specific instructions, such as to remain off the phone unless they possess information about the event, to lie on the floor, and, if PF enter their location, to keep their hands and security badges visible.

c. Tactical Application. The PF is deployed in a strategic posture composed of both fixed and mobile posts to interrupt, interdict, deny, and neutralize an adversary force attack. The PF is armed and equipped with state of the art weaponry, tactical equipment, vehicles, and communication systems. The PF is adept at implementing approved Security Incident Response Plans under adverse emergency conditions. The PF consists primarily of defensive personnel (SPO-Is) in well-prepared positions with a relatively small number of offensively qualified personnel (SPO-IIs) who could maneuver against the adversary if required. A dedicated reentry/recapture capability in the form of more highly trained and qualified personnel (SPO-IIIs) supported by SPO-IIs is available in the event that denial of access was ineffective. If desired, a defensive plan may be executable by a PF consisting only of SPO-Is and SPO-IIIs, comprising defensive and offensive capabilities respectively. In that case, the SPO-IIIs' element missions include those described below in paragraph (2)(b).

(1) Response Force Characteristics.

(a) Survivability

(b) Mobility

(c) Lethality

(d) Flexibility

(e) Speed

(f) Unpredictability

(g) Mutual Support

(h) Reliable communications

(2) Response Force Element Missions. A site PF response force is composed of small units/teams of no fewer than two SPOs, deployed in configurations that provide tactical advantages for both defensive and offensive operations. In the event that facility PF deployment consists of single-person patrol units or posts, plans must require consolidation into small unit tactical teams with a designated leader during the response.

(a) Special Response Team (SRT).

1 Mission. The SRT executes recapture operations and conducts or supports pursuit and recovery operations as well as interruption, interdiction, neutralization, containment, and denial strategies.

2 Capabilities. SPO III qualified personnel are deployed as one or more dedicated teams with specialized weapons and equipment, operating from mobile tactical vehicles, as ground assault forces, or a combination of both.

(b) Security Police Officer-II.

1 Mission. Executes interruption, interdiction, neutralization, containment, and denial strategies and supports recapture, fresh pursuit, and recovery operations.

2 Capabilities. SPO II personnel operate in small units with specialized weapons and equipment from mobile patrols/tactical vehicles and fixed posts.

(c) Security Police Officer-I.

1 Mission. Supports and/or executes interruption, interdiction, neutralization, containment, and denial strategies.

2 Capabilities. SPO I personnel operate from mobile patrols and fixed posts to perform routine S&S related functions. They are also capable of performing specialized active defense functions such as staffing defensive fighting positions. They may also deploy in armored vehicles, employing the capabilities of the vehicle with the planned expectation of remaining with it, operating Remotely Operated Weapon Systems (ROWS), and performing Central Alarm Station (CAS) duties.

(d) Security Officer.

1 Mission. Ensures routine security-related functions are maintained (e.g., access/egress control, escort duties, CAS operations).

2 Capabilities. Unarmed SOs perform observation and reporting activities, logistical re-supply to other PF elements, message courier duties, and provide transportation support.

(3) Deployment Considerations.

(a) A layered, or zone, defensive strategy is implemented that maximizes the PF's ability to detect, engage, and neutralize adversary forces as they move toward a target location.

(b) Fixed, reinforced fighting positions, or bunkers, are utilized to enhance survivability, deny access to targets, provide overlapping fields of fire for mutual support, and to control avenues of approach.

(c) Protection strategies are designed to reduce predictability of the response.

(d) Small units/teams of no fewer than two SPO II and/or SPO III personnel are deployed in configurations that provide tactical advantages for both defensive and offensive operations. If members of a team are deployed as one-person units, all plans must allow for a reconsolidation during the response.

(e) Personnel who will occupy fixed fighting positions, those who will perform as the flexible maneuver elements, and those who will, if required, conduct recapture/recovery operations are identified.

(f) Each PF member is issued at least one primary weapon along with a secondary firearm, such as a handgun, used principally for close quarters engagement or to transition to in the event of a stoppage of the primary weapon.

(g) PF weapons systems capabilities support tactical operations in both day and night conditions.

(h) The PF employs direct-fire weapons to engage and to neutralize adversary forces out to the maximum effective range of the weapon.

(i) As prescribed by the facility or site security plan, the PF employs indirect-fire or explosive projectile weapons to deny access to target locations and to suppress and to neutralize adversary forces occupying positions of cover and/or concealment.

(j) PF members are knowledgeable of adversary attack methods identified in the Graded Security Protection (GSP) policy and critical pathways documented in site-specific vulnerability assessment reports.

(k) A secure tactical command post is identified to ensure that command, control, and communications links are maintained and that backup systems are available.

(l) Command and control is structured down to the lowest unit/team level. Operational control of forces includes organizing and employing of forces, designating combat objectives, assigning individual and unit tasks, and issuing orders and directions necessary for mission accomplishment.

(m) Accurate adversary and battle information is relayed to command/control centers as it occurs.

(n) A system for Identification, Friend or Foe (IFF) is employed to minimize incidents of casualties from "friendly fire."

(4) Denial Strategy Implementation.

(a) Early warning system technologies are emplaced to detect and to assess adversary movement as far as possible from target locations.

(b) Highly mobile tactical vehicles (armored and/or unarmored) mounted with light and/or heavy weapon systems are deployed to support combat operations, conduct reconnaissance operations, control avenues of approach, maneuver to suppress and destroy hostile threats, and to provide mutual support for other tactical vehicles.

(c) A commander is designated for each tactical armored vehicle.

(d) Potential target access points are covered by suppressive fire weapons.

(e) PF members utilize positions of cover and maximize the element of surprise to the extent possible.

(f) The PF initiates a decisive engagement with adversary forces as far as possible outside the target location.

(g) Once an adversary has been identified and engaged, PF elements never lose contact.

(h) Adversaries are engaged while they negotiate obstacles (i.e., fences, barriers, etc.), deploy from vehicles (both airborne and ground based), and cross open ground.

(i) PF teams, using suppressive fire weapons, maneuver in force against adversaries occupying covered positions.

(j) The PF has plans in place to transition quickly from defensive to offensive operations.

(5) Recapture Operations.

(a) The site PF is staffed and deployed in sufficient strength to ensure the protection of sensitive assets. The dedicated SRT is established with additional resources sufficient to ensure that recapture capabilities continue to exist in the event that the denial strategy fails.

(b) SRT training is focused on site-specific targets and ensures that SRTs are adequately prepared to conduct recapture operations within identified target locations.

(c) SRTs possess the site-specific tactics, tools, and techniques necessary to gain entry, neutralize the adversary threat, control the situation, and secure national security assets.

(d) If hostages are involved and a Category I SNM or radiological/toxicological sabotage target asset is at risk, regaining control of the asset is the primary consideration.

(e) SRTs are supported by other PF elements to the maximum extent possible as they move toward the target objective.

(f) PF members provide overwatch for the assault team(s) movement, cover avenues of approach, and provide support by fire to the recapture team as they breach/enter the target location.

(g) All PF personnel are capable of providing direct support to the recapture mission by supplementing the main assault force, controlling the target area, and suppressing enemy defensive positions.

(6) Pursuit and Recovery Operations.

(a) PF members are trained and equipped to conduct fresh pursuit and recovery operations, on and off DOE property.

(b) Fresh pursuit and recovery operations are coordinated with responding Federal, State, and local law enforcement agencies according to approved agreements.

(c) PF members use vehicle immobilization techniques and/or other means of applying deadly force to terminate the pursuit.

(d) PF members maintain control of sensitive assets until relieved by cognizant Federal authorities.

(7) Weapons of Mass Destruction.

(a) All PF personnel are trained and equipped to operate within an environment where Weapons of Mass Destruction (WMD) have been employed; i.e., chemical, biological, or radiological weaponry. PF training programs include tactical deployment in WMD personal protective equipment.

(b) PF members are able to transition to WMD fighting procedures rapidly enough so as to not weaken the overall combat posture.

(c) Individual tactical equipment is compatible with WMD personal protective equipment.

4. MANAGEMENT CONSIDERATIONS.

a. Training. Training is the key to a quality force, and the best form of tactical training is person-on-person, or force-on-force (FOF) engagements, on a repetitive basis. FOFs do not always have to involve very large scale exercises, nor do they always need to occur in or around the actual facilities. Encouraging and assisting PF members to refine their individual and small unit tactical skills and to condition them to the reflex of shooting at adversaries can be facilitated with smaller scale training exercises using surrogate facilities. This will enable the Department to afford a much higher frequency of such activities because the costs in terms of facility shut down, coordination with operations, shadow force deployment, etc., will be substantially avoided. But, in order to achieve the desired results, these exercises must employ engagement simulation systems such as Multiple Integrated Laser Engagement Systems (MILES), dye marking cartridge (DMC) weapons, or hybrid DMC/MILES weapons that combine DMC for close-range and MILES for longer range.

b. Planning and Implementation. There are issues that may be considered ancillary to the planning and implementation of the DOE facility defense model but which nevertheless are important to the viability of tactical planning and execution. Some factor directly into the planning process while others relate indirectly. Examples are:

(1) Targets must be as consolidated and in as few locations as possible.

(2) All tactical training should simulate as closely as practicable the environment and manner in which PF personnel are expected to fight.

(3) Persons assigned as full-time staff PF instructors must be qualified in accordance with the provisions of the current protection program operations directive.

ATTACHMENT 5. INCIDENTS OF SECURITY CONCERN

This Attachment provides information and/or requirements associated with DOE O 470.4B as well as information and/or requirements applicable to contracts in which the associated CRD (Attachment 1 to DOE O 470.4B) is inserted.

1. OBJECTIVE. To ensure the occurrence of a security incident prompts the appropriate graded response, to include an assessment of the potential impacts, appropriate notification, extent of condition, and corrective actions. The long-term management of incidents serves as an effective Program Planning and Management (PPM) tool for enhancing site-specific implementation of security policies.

2. PURPOSE. To set forth requirements for the U.S. Department of Energy (DOE) Incidents of Security Concern (IOSCs) process, including timely identification, notification, inquiry, reporting, and closure of IOSCs. The IOSC program serves multiple purposes to include:

   a. Ensuring that security incidents are communicated to DOE/National Nuclear Security Administration (NNSA) line management, U.S. Congress, other agencies or foreign governments, as appropriate;

   b. Meeting regulatory reporting requirements;

   c. Enhancing the ability to track and trend the health of the security program at the site and overall Department;

   d. Ensuring that incidents are assessed relative to the impact to national security and the collateral impact with other programs and security interests;

   e. Enabling mechanisms to support performance assurance, self-assessment, oversight, and other key security functions;

   f. Enhancing the ability to influence policy development and site security implementation; and

   g. Ensuring that the S&S programmatic successes are identified and communicated internally and externally.

3. DEFINITIONS. Terms commonly used in the DOE S&S Program are defined in the DOE Policy Information Resource (PIR) tool located at http://www.pir.pnl.gov. In addition to these definitions, the following are provided:

   a. Category A Security Incidents. Incidents that meet a designated level of significance relative to the potential impact on the Department and/or national security (defined in the subsequent sections), thereby requiring the notification

and pertinent involvement of the DOE/NNSA cognizant security office (CSO) and the contractor CSO.

b. Category B Security Incidents. Incidents of lesser significance (i.e., incidents that do not meet the Category A criteria) that are managed and resolved by the contractor CSO. However, oversight responsibilities remain with the DOE/NNSA CSO.

c. Significant Nuclear Defense Intelligence Losses. Defined by 50 U.S.C. Section 2656 as "any national security or counterintelligence failure or compromise of classified information at a facility of the Department of Energy or operated by a contractor of the Department that the Secretary considers likely to cause significant harm or damage to the national security interests of the United States."

d. Compromise. Evidence is provided that information was disclosed to an unauthorized person(s) (e.g., published by media, classified information was briefed to uncleared individuals, etc.).[2]

e. Suspected Compromise. Evidence is provided that there is a high probability that information was compromised. Although there is no clear indication of compromise (i.e., no direct recipient), the circumstances associated with the incident indicate that there is an obvious possibility that unauthorized disclosure did occur (e.g., classified information is transmitted by email outside of the organization's firewall, classified information is communicated on an unsecure phone line, etc.).

f. Likelihood of Compromise Is Remote. Although protection and control measures are violated, the circumstances associated with the incident indicate that there is a low possibility that information was disclosed to unauthorized personnel (e.g., classified information is left unsecured and unattended for a limited amount of time in an area accessed only by personnel with the appropriate clearance level, classified information is transmitted by email inside the organization's firewall and is discovered and isolated within a specified period of time.

g. Compromise Did Not Occur. Evidence is provided that there is no possibility that information was compromised.

h. Authorized Person. A person who has a favorable determination of eligibility for access to classified information, has signed an approved nondisclosure agreement,

[2] The compromise or suspected compromise can occur through unauthorized disclosure (i.e., identifiable recipient) and/or several types of medium such as but not limited to computer, verbal, facsimile, phone, etc. The latter is described in DoD 5220.22-M, N*ational Industrial Security Program Operating Manual (NISPOM)*, as "Improper Transmission". Also, the latter type of incidents may not be associated with a specific unauthorized recipient, but rather result in a compromise or suspected compromise determination due to the inherent vulnerabilities of the transmission.

and has a need-to-know for the specific classified information in the performance of official duties.

4. REFERENCES.

a. 18 U.S.C. Section 923 (g)(6),*Licensing*. Each licensee shall report the theft or loss of a firearm from the licensee's inventory or collection, within 48 hours after the theft or loss is discovered, to the Attorney General and to the appropriate local authorities.

b. 42 U.S.C. Sections 2271 to 2181, *Enforcement of Chapter*. Gives the U.S. Federal Bureau of Investigation (FBI) the authority to investigate alleged or suspected criminal violations of the Atomic Energy Act, makes violations of the Act criminal, and provides for injunction and contempt proceedings.

c. 42 U.S.C. Section 2282b (Section 234B, as amended). Establishes civil penalties for violations of directives regarding protection of classified information by contractors or their employees.

d. 50 U.S.C. Section 402a, *Coordination of Counterintelligence Activities*. States that the FBI is advised immediately of any information, regardless of its origin, that indicates that classified information is being, or may have been, disclosed in an unauthorized manner to a foreign power or an agent of a foreign power.

e. 50 U.S.C. Section 2656, *Notice to congressional committees of certain security and counterintelligence failures within nuclear energy defense programs*. Requires the Secretary of Energy to notify the Committees for Armed Services of the U.S. Senate and House of Representatives of each "significant nuclear defense intelligence loss."

f. 42 U.S.C. Section 5801, 5877 and 307, *Energy Reorganization Act of 1974*. Requires investigating suspected, attempted, or actual thefts of special nuclear materials in the licensed sector and developing contingency plans for dealing with such incidents.

g. E.O. 13526, *Classified National Security Information*, dated 12-29-09. If the Director of the Information Security Oversight Office finds that a violation of this policy or its implementing directives has occurred, the Director shall make a report to the head of the agency or to the senior agency official so that corrective steps, if appropriate, may be taken.

h. National Security Decision Directive 84, *Safeguarding National Security Information*. Requires unauthorized disclosures of classified information to be evaluated to determine information disclosed and extent of dissemination, and discusses coordination with the U.S. Department of Justice.

i. 7 CFR Part 331, *Possession, Use, and Transfer of Select Agents and Toxins*. Implements the provisions of the *Agricultural Bioterrorism Protection Act of 2002* setting forth the requirements for possession, use, and transfer of select agents and toxins. The biological agents and toxins listed in this part have the potential to pose a severe threat to plant health or plant products.

j. 9 CFR Part 122, *Organisms and Vectors*. Establishes the permits required, the application for permits and the suspension or revocation of the permits.

k. 6 CFR Part 27, *Chemical Facility Anti-Terrorism Standards*. Establishes the standards for possessing or planning to possess, at any relevant point in time, a quantity of a chemical substance determined by the Secretary to be potentially dangerous or that meets other risk-related criteria identified by the Department.

l. 10 CFR Part 824, *Procedural Rules for the Assessment of Civil Penalties for Classified Information Security Violations*. Establishes rules to assess a penalty for violation of a directive relating to the protection of classified information pursuant to 42 U.S.C. Section 2282b (Section 234B, as amended, of the Atomic Energy Act) or for violation of a compliance directive that directs action for the protection of classified information.

m. 10 CFR Part 1016, *Safeguarding of Restricted Data*. Requires the permittee to report any infractions, losses, compromises, or possible compromise of Restricted Data.

n. 10 CFR Part 1045, *Nuclear Classification and Declassification*. Addresses the sanctions for knowing, willful, or negligent actions contrary to the requirements of the CFR that results in the misclassification of information.

o. 32 CFR Part 2001.48, *Reporting Loss of Classified Information*. Mandates reporting, inquiry, etc. for the loss, possible compromise, or unauthorized disclosure of classified information. If the incident entails a criminal violation, coordination is required with legal counsel and Department of Justice.

p. 48 CFR Chapter 9, *Department of Energy Acquisition Regulation*. Supplements 48 CFR Chapter I, *Federal Acquisition Regulations*, and includes the security clauses to be used in DOE solicitations and contractors or agreements involving access to classified information and/or a significant quantity of special nuclear material (SNM).

q. DoD 5220.22-M, *National Industrial Security Program Operating Manual (NISPOM)*, 1-303. Requires any reports of loss, compromise, or suspected compromise of classified information, foreign or domestic, to be reported to the cognizant security agency (CSA). Classified material that cannot be located within a reasonable period of time shall be presumed to be lost until an investigation determines otherwise.

r. DOE O 151.1C, *Comprehensive Emergency Management System,* dated 11-2-05 . Establishes policy and assigns roles and responsibilities for the DOE Emergency Management System.

s. DOE O 206.1, *Department of Energy Privacy Program*, dated 1-16-09. Establishes Departmental implementation of agency statutory and regulatory requirements for privacy, specifically those provided in the *Privacy Act of 1974*, as amended, and Office of Management and Budget directives.

t. DOE O 221.1A, *Reporting Fraud, Waste and Abuse to the Office of Inspector General,* dated 4-19-08. Establishes requirements and responsibilities for reporting fraud, waste, abuse, misuse, corruption, criminal acts, or mismanagement to the DOE, Inspector General.

u. DOE O 231.1 A chg 1, *Environment, Safety, and Health Reporting*, dated 6-3-04. Requires a timely collection, reporting, analysis, and dissemination of information on environment, safety, and health issues as required by law or regulations or as needed to ensure that DOE and NNSA are kept fully informed on a timely basis about events that could adversely affect the health and safety of the public or the workers, the environment, the intended purpose of DOE facilities, or the credibility of the Department.

v. DOE M 231.1-1A chg 2, *Environment, Safety, and Health Reporting Manual, dated 3-19-04*. Establishes requirements categorizing occurrences related to environment, safety, and health or operations ("Reportable Occurrences"); notifying DOE of these occurrences; and developing and submitting documented follow-up reports. This occurrence reporting directive further requires that the notifications be timely in accordance with the significance of the occurrence.

w. Deputy Secretary memorandum, *Security Incident (Including Cyber) Notification Protocol,* dated 6-24-11 addressing all heads of Departmental Elements, requires notifying Congress of various losses, and in particular, classified material that may compromise national security.

5. ROLES AND RESPONSIBILITIES.

a. DOE/NNSA CSO. The DOE/NNSA CSO must define the designee(s) (i.e., program office and/or site office) responsible for executing the subsequent roles and responsibilities. Note: The terms DOE/NNSA CSO and Federal designee(s) are used interchangeably throughout this policy.

(1) As the element with programmatic responsibility for the information, coordinate formal reviews of incidents involving the loss, theft, compromise, or suspected compromise of Top Secret, Sensitive Compartmented Information (SCI), Special Access Program (SAP), and Restricted Data (RD) Nuclear Weapon Data to render a "significant

nuclear defense intelligence loss." If the incident meets the "significant nuclear defense intelligence loss" criteria, the appropriate Federal entity(s), after consultation with the Director, National Intelligence, and the Director, FBI, must provide notification to Congress. The notification of Congress must occur within 30 days of categorizing the event as a 50 U.S.C. Section 2656 reportable incident.

(2) Must determine if the incident warrants a damage assessment and conduct if necessary.

(3) Must review all Category A Security Incidents.

(4) Serves as the liaison to Congress, the Secretary, other government agencies, the FBI, and the Inspector General for incidents under their purview.

(5) Must track and trend incidents for the purpose of assessing program strengths and weaknesses across programmatic sites.

(6) Responsible for approving the site's IOSC program plan.

(7) Must ensure that the site's IOSC program plan thoroughly addresses all elements of the program and that sufficient resources are provided to conduct inquiries and to implement corrective actions.

(8) Performs IOSC program implementation oversight to include, but not limited to, reviewing inquiries, conducting determinations of compromise, tracking and trending, and integrating of the data into the larger PPM function.

(9) Ensures that the contractor CSO completes the actions necessary to resolve IOSCs, including actions necessary to prevent recurrence.

(10) Utilizes the IOSC program as a feedback mechanism to assist management in evaluating programmatic performance across all security disciplines.

(11) Coordinates with the Deputy Director, Counterintelligence Directorate, concerning incidents that indicate a deliberate compromise of classified information or that involve foreign persons, governments, or activities.

b. Office of Health, Safety and Security (HSS).

(1) Establishes the IOSC program based on national policies and best business practices.

(2) Oversees, maintains, and provides training on the Safeguards and Security Information Management System (SSIMS).

(3) Assesses incident data for the purpose of reviewing and enhancing security policies.

(4) Provides technical incident and causal analysis expertise to site and program offices as requested.

(5) Enforces provisions under 10 CFR Part 824, which implements subsections a, c, and d of section 234B of the *Atomic Energy Act of 1954*, 42 U.S.C. Section 2282b.

c. Contractor CSO.

(1) Develops the site IOSC program plan, which addresses each component of the subject policy. Integrates the site IOSC program plan with the larger PPM function for the purpose of influencing other functions and enhancing site-specific implementation of security policies. The site IOSC program plan must include implementation guidance from the DOE/NNSA CSO describing expected actions or responses for the individual elements of the policy. These implementing instructions include, but are not limited to, the identification of specific incident types requiring Federal notification, specific Federal offices and entities requiring notification, and the mechanism for notifying entities within line management.

(2) Assesses and categorizes all incidents, to determine the appropriate level of notification, which will influence the consideration for external notification, corrective actions, damage assessments, etc.

(3) Ensures that any documents generated concerning incidents are reviewed for classification as required by DOE O 475.2A, *Identifying Classified Information,* dated 2-1-11 as applicable.

(4) Performs tracking and trending analyses on the collective set of incidents for the purpose of monitoring security program performance and modifying site security procedures accordingly.

(5) Assesses the impacts of incidents relative to other site programs and security interests and coordinates, as necessary, with the programmatic element responsible for the information that is compromised or suspected of compromise.

(6) Advises the DOE/NNSA CSO of adverse trends or other indicators that security plans and/or procedures are not achieving the desired results.

SECTION 1. INCIDENT IDENTIFICATION AND REPORTING REQUIREMENTS

1. GENERAL.

   a. Each IOSC with the exception of incidents of Management Interest (MI) (see section 2 c. (2)) requires categorization, an initial report, an inquiry, and a closure report. The level of effort associated with the latter three steps is graded based on the incident category and the factors (severity, asset, etc.) surrounding the incident.

   b. Initial and final reporting is imperative as the DOE/NNSA CSO has specific responsibilities for notifying and/or coordinating with other agencies, governments, Departmental leadership, and Congress for select incidents.

   c. All information generated as part of this process must be protected according to its sensitivity and/or classification determination.

   d. Security incidents include a range of possible actions, inactions, or events that:

      (1) Pose threats to national security interests and/or Departmental assets;

      (2) Create potentially serious or dangerous security situations;

      (3)

      (4) Have a significant effect on the S&S Program's capability to protect DOE S&S interests;

      (5) Indicate the failure to adhere to security procedures; or

      (6) Illustrate the system is not functioning as designed by identifying and/or mitigating potential threats (e.g., detecting suspicious activity, hostile acts, etc.).

2. INCIDENT IDENTIFICATION AND CATEGORIZATION. DOE uses a graded approach for the identification and categorization of IOSCs. This approach provides a framework for the requirements of reporting timelines and the level of detail for inquiries into, and root cause analysis of, specific security incidents. By establishing a graded approach, line management can effectively allocate the resources necessary to implement this policy.

   a. All IOSCs must be categorized by significance level and type. As Table 1 illustrates, there are two levels of significance and three types of incidents.

Table 1. Significance Levels and Incident Types

SIGNIFICANCE LEVEL CATEGORY	
A	B
INCIDENT TYPE	
Security Interest (SI)	Security Interest (SI)
Management Interest (MI)	Management Interest (MI)
Procedural Interest (PI)	Procedural Interest (PI)

b. Incident Significance Level Categories.

(1) Category A incidents, which meet a designated level of significance relative to the potential impact on the Department and/or national security, require the notification of the DOE/NNSA CSO and the contractor CSO. The involvement of the DOE/NNSA CSO for Category A incidents is imperative for assessing impacts, coordinating with external agencies, and/or notifying senior management.

(2) Category B incidents, which do not meet the Category A criteria, are managed and resolved by the contractor CSO; however, this does not preclude the DOE/NNSA CSO from exercising its oversight responsibilities. The monitoring of Category B incidents by the contractor CSO is essential as it allows management to proactively address reoccurring incidents, thereby minimizing the occurrence of potentially more significant incidents.

c. Incident Types.

(1) Security Interest (SI). This type of incident involves the loss, theft, compromise, or suspected compromise of Departmental assets.

(2) Management Interest (MI). This type of incident does not necessarily involve Departmental assets but is a unique type of incident that may have potential undesirable impacts. MI incidents therefore warrant management notification. MI incidents differ from SI and Procedural Interest (PI) incidents in that the emphasis is on notification; therefore, MI incidents do not require formal inquiry, closure, etc.

(3) Procedural Interest (PI). This type of incident is associated with the failure to adhere to security procedures, and all evidence surrounding the

incident suggests the asset was not compromised or the likelihood of compromise is remote.

d. Incident Criteria. Based on the three types of incidents, the following provides a general framework for distinguishing between Category A and B incidents.

(1) SI.

(a) Category A SI incidents involve the following assets:

1 SNM and nuclear material (note that "Loss" does not include quantities that are within established shipping, processing, and inventory limits);

2 All classified matter;

3 As one involving quantities of radiological, chemical, and/or biological materials that if misused could endanger the public;

4 Security key or keycard based on the significance of the asset being protected and the degree of access provided by the key or keycard (e.g., direct access versus access impeded by other layers/measures);

5 Protective force firearms, ammunition, explosives, and equipment per the reporting requirements in DOE M 470.4-3A, *Contractor Protective Force*, dated 11-05-06, and other equipment documented in the site IOSC program plan;

6 DOE security badge determined to be the target of the theft;

7 Matter of a foreign government that requires reporting based on established agreements and required protocols; or

8 Other assets determined by the DOE/NNSA CSO and/or contractor CSO.

(b) Category B SI incidents involve the following assets:

1 Official Use Only (Ex 2); Official Use Only/Export Controlled Information (Ex 2 or 3); Unclassified Controlled Nuclear Information; Naval Nuclear Propulsion Information; and

2 Other assets as determined by the DOE/NNSA CSO and/or contractor CSO.

(2) MI.

(a) Category A MI incidents are significant enough to warrant notification to the DOE/NNSA CSO. Examples include work stoppages, arrest of an employee enrolled in a human reliability program, etc. Incidents constituting or determined to be a Category A MI must be specified in the IOSC program plan.

(b) Category B MI incidents require notification to the contractor CSO. Incidents constituting or determined to be a Category B MI must be specified in the IOSC program plan.

(3) PI.

(a) Category A PI incidents are associated with the failure to adhere to security procedures and warrant notification to the DOE/NNSA CSO. An example of a Category A PI incident is an unauthorized discharge and other incidents determined by the DOE/NNSA CSO and/or Contractor CSO.

(b) Category B PI incidents do not result in the loss, theft, compromise or suspected compromise of the asset. These incidents are supported by evidence that suggest the likelihood of compromise is remote or that compromise did not occur. An example of a Category B PI incident would be the improper handling, and/or storage of classified matter, where the supporting evidence suggests compromise did not occur or the likelihood was remote.

3. PRELIMINARY INQUIRY, CATEGORIZATION, AND REPORTING REQUIREMENTS.

a. The preliminary inquiry and categorization is based on the subject policy and any additional criteria as documented in the site IOSC program plan. Preliminary reporting and categorization specifications include:

(1) The "clock starts" when a potential incident is brought to the attention of management. At that point, the site has a maximum of 5 calendar days to conduct the preliminary inquiry, to make the initial categorization, and to perform the initial notification(s).

(2) Although a maximum of 5 calendar days are provided, sites are required to report the incident as soon as the incident is categorized. The 5 day period provides flexibility for those incidents requiring additional fact gathering

such as classification review or an inventory check to locate a potentially lost/missing item.

(3) If there is still uncertainty at the 5 calendar day mark, with respect to incident categorization, the incident must be reported as a Category A pending completion of the inquiry process. If the final inquiry reveals additional details and facts, the incident can be re-categorized.

(4) Each security incident must be assigned a unique local site tracking number.

(5) The main emphasis for MI incidents is on notification; therefore, the subsequent section dealing with inquiries and closure reports is not applicable to this specific type of incident (unless additional information is requested by the CSO).

b. Category A Preliminary Reporting Requirements.

(1) The DOE/NNSA CSO must be notified of all Category A incidents.

(2) The site IOSC program plan must contain the notification content and process to include the personnel and organizations identified for notification and any additional and/or specific notification requirements.

(3) If the incident involves classified matter, the Departmental element with programmatic responsibility for the information must be identified. Notification must include whether origination was by another agency or foreign government and a description of the compromised or suspected compromised information. See "Incident Closure" in this section for additional content considerations for the initial report.

(4) If the site determines that an incident involves the loss, theft, compromise, or suspected compromise of Top Secret, SCI, SAP, and RD Nuclear Weapon Data, the designee(s) or element with programmatic responsibility of the information must review the incident and render two additional determinations.

(a) If it is determined that the incident meets the significant nuclear defense intelligence loss criteria, the appropriate Federal entity(s) after consultation with the Director, Central Intelligence, and the Director, FBI must provide notification to Congress. The notification to Congress must occur within 30 days of categorizing the event as a 50 U.S.C. Section 2656 reportable incident.

(b) The element with programmatic responsibility for the information must also determine if the incident warrants a damage assessment. Damage assessments are normally conducted for Top Secret, SCI,

SAP, and RD Nuclear Weapon Data classified information; however, they can also be performed for other incidents involving other levels and categories of classified information. In addition to the specific information compromised or suspected of compromise, other considerations for conducting a damage assessment are, but not limited to, if the incident is associated with a violation of law, if the information was compromised to a wide audience, etc.

c. Category B Preliminary Reporting Requirements. While notification and reporting of Category B incidents does not extend beyond the contractor CSO, the approved site IOSC program plan must document the internal notification process.

d. Reporting to Cognizant Personnel Security Offices. IOSCs, regardless of category, may impact an individual's eligibility for access to classified information. Therefore, upon closure, the outcome of the inquiry for all security incidents regarding individuals applying for or holding a DOE security clearance must be reported to the personnel security office with cognizance over the individual's access eligibility.

e. Reporting Incidents Associated with Sensitive Programs. IOSCs involving activities associated with sensitive programs must follow the same initial reporting process but may omit details because of programmatic controls. These programs include the SCI Program, SAP Program, the Technical Surveillance Countermeasures (TSCM) Program, the Counterintelligence (CI) Program, or other programs identified by the appropriate Federal designee(s). All subsequent reporting must be handled within the programmatic channels until the inquiry report has been closed within the sensitive program.

f. Other Multi-Program Reporting. An event that meets the criteria for reporting as an IOSC does not negate the responsibility to report through other related reporting chains such as (but not limited to):

(1) Per DOE O 231.1A, chg 1, *Environment, Safety, and Health Reporting*, 6-3-04, security incidents that affect both safety and security are reportable through the Occurrence Reporting Processing System (ORPS).

(2) Per DOE O 151.1C, *Comprehensive Emergency Management System*, dated 11-2-05, security incidents that are reportable under the provisions of DOE O 151.1C must continue to be reported in accordance with that Order and this Attachment.

(3) Incidents involving personally identifiable information (PII), both electronic and hardcopy, must be reported to the Office of Chief Information Officer in accordance with DOE O 206.1, *Department of Energy Privacy Program*, dated 1-16-09.

(4) NNSA "Flash Reporting" procedures are not affected by requirements in this section.

(5) Per DOE O 475.1, *Counterintelligence Program*, dated 12-10-04, the geographically closest element of the Office of Counterintelligence/Office of Defense Nuclear Counterintelligence must be notified of security incidents involving any credible information that a non-U.S. citizen or an agent of a foreign power is involved or that there are indications of deliberate compromise from a U.S. Federal or contractor employee. Appropriate notifications (i.e., FBI) will then be made in accordance with 50 U.S.C. Section 402a.

(6) Per DOE O 221.1A, *Reporting Fraud, Waste and Abuse to the Office of Inspector General*, when an inquiry surrounding an IOSC establishes information indicating that fraud, waste, abuse, misuse, corruption, criminal acts, or mismanagement has occurred, the Office of the Inspector General must be notified.

(7) Per DOE M 205.1-8 Admin Chg 2, *Cyber Security Incident Management Manual*, dated 1-08-09, all cyber security related incidents must be reported to the Computer Incident Response Center (CIRC). Any cyber security incident involving the loss, theft, compromise, or suspected compromise of classified or controlled unclassified information must also be reported through the IOSC program.

(8) Whenever a compromise involves the classified matter of another Federal agency, the Federal designee(s) within line management must coordinate with the other government agencies (OGAs), as appropriate.

(9) Whenever a compromise involves the matter of a foreign government that requires protection (e.g., Confidential Foreign Government Information Modified Handling [C/FGI-Mod], classified Foreign Government Information), the Federal designee(s) within line management must coordinate with the U.S. Department of State and the foreign government as appropriate. The foreign government, however, will not normally be advised of any Departmental security system vulnerabilities that allowed or contributed to the compromise.

(10) If a compromise of SCI has occurred, the Director, Office of Intelligence and Counterintelligence, must consult with the designated representative of the Director, Central Intelligence and other officials responsible for the information involved.

g. Special Reporting Situations. Under certain circumstances, related IOSCs that are anticipated to recur over a long period of time may be consolidated from a reporting and documentation perspective. This situation will be handled on a

case-by-case basis between the contractor CSO and the Federal designee(s) with specific reporting plans documented in the approved site IOSC program plan.

4. CONDUCT OF INQUIRIES. An inquiry must be conducted to establish the pertinent facts and circumstances surrounding the security incident. The specific inquiry process established by the contractor CSO must be documented in the site IOSC program plan. Specific requirements and actions that must be considered when conducting inquiries include:

   a. If a security incident affects more than one site/facility under the purview of a single Program and/or Site Office, that office must assign responsibility to a lead organization. If the sites/facilities fall under the purview of multiple Program Offices, those offices must, by mutual agreement, decide on a lead organization with responsibility for the inquiry.

   b. In all instances where the Federal designee(s) disagrees with the contractor CSO report, the Federal designee(s) must assume supplemental inquiry responsibilities.

   c. When the inquiry into an IOSC necessitates communication with agencies/ organizations external to the Department (e.g., the U.S. Postal Service, the FBI, or other Federal, state, or local agencies), a Federal employee must be responsible for performing all such communication. If necessary, the contractor CSO may perform this function with the written concurrence of the Federal designee.

5. INQUIRY OFFICIALS.

   a. Inquiry officials may be either Federal or contractor employees and must have previous investigative experience or Departmental inquiry official training. Inquiry officials must be knowledgeable of appropriate laws, executive orders, Departmental directives, and/or regulatory requirements.

   b. Inquiry officials are not authorized to detain individuals for interviews or to obtain sworn statements. They may only conduct consensual interview and request signed statements.

   c. Inquiry officials must be appointed in writing by the designated Federal entity(s).

   d. If an inquiry official determines or suspects that a foreign power or an agent of a foreign power is involved, the contractor CSO must stop further inquiry actions and notify the designated Federal designee(s), who will assume further notification and reporting responsibilities to include coordination with the Office of Counterintelligence. In such instances, the inquiry official must document the known circumstances surrounding the IOSC and submit all accumulated data to the Federal designee(s).

e. Inquiry officials are responsible for conducting the inquiry and maintaining all documentation associated with the inquiry. Specific actions must at least include:

(1) Collect all information and physical evidence associated with the security incident. Physical evidence collected must be controlled and a chain-of-custody must be maintained.

(2) Identify persons associated with the incident and conduct interviews to obtain additional information regarding the incident.

(3) Reconstruct the security incident to the greatest extent possible using collected information and evidence. The reconstruction should include a chronological sequence of events that describes the actions preceding and following the incident.

(4) Identify any collateral effect to other programs or security interests.

(5) Analyze and evaluate which systems/functions performed correctly or failed to perform as designed. This action will provide the basis for determining the cause of the incident and subsequent corrective actions.

6. INCIDENT CLOSURE. The final closure report serves as the basis for closing incidents. Similar to inquiries, the level of detail provided in the report will vary on the category of the incident. The report content and closing procedures must be documented in the site IOSC program plan. At a minimum, the final closure report content and closure process must include:

a. The final closure report for Category A incidents must be submitted within 90 calendar days of preliminary incident notification. The time frame for completing inquiries and the process for seeking extensions must be addressed in the site IOSC program plan.

b. Category A incidents must be closed via SSIMS.

c. Category B incidents can be closed using SSIMS or a locally approved system identified in the site IOSC program plan. The incident notification and the inquiry report must contain supporting documentation of factors used to determine that the likelihood of compromise and/or the potential for damage to national security is remote (e.g., failure to secure a document in a security container; however, multiple physical protection layers exist preventing unauthorized disclosure). This documentation provides the basis for making a statement that the circumstances surrounding the security incident are such that the possibility of damage to the national security can be discounted.

d. All supporting documentation must be retained with the final report. For Category A incidents, at a minimum, the documentation must include:

(1) Material and relevant information (i.e., the "who, what, when, and where") that was not included in the initial report;

(2) The name of the individual(s) who was primarily responsible for the incident, including a record of prior incidents for which the individual had been determined responsible;

(3) If applicable, documentation noting if the unauthorized disclosure was willful (i.e., intentional vs. inadvertent disclosure);

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

(5) If applicable, specific reasons for reaching the conclusion that the theft, loss, compromise, suspected compromise, compromise did not occur or that the likelihood of compromise was remote;

(6) Identification of any collateral (i.e., extent of condition) effect to other programs or security interests;

(7) If the incident involves the compromise or suspected compromise of information, the extent of the dissemination (e.g., number of individuals and their citizenship; global disclosure via cyber mediums, open source publication; etc.) must be identified; and

(8) Identification of specific impacts (i.e., degree of damage, reference 32 CFR Part 2001.48) of the incident to the Department and/or national security. Whenever an incident involves classified matter or interests of more than one Government agency, each agency is responsible for conducting the damage assessment resulting from its compromised matter.

7. ADMINISTRATIVE ACTIONS.

a. Whenever possible, the responsibility for an IOSC must be assigned to an individual rather than to a position or office. When individual responsibility cannot be established and the facts show that a responsible official allowed conditions to exist that led to an IOSC, responsibility must be assigned to that official.

b. Security infractions are issued to document the assignment of responsibility for an IOSC. Persons deemed responsible for a security incident may, at management's discretion, be issued a security infraction and/or have disciplinary actions taken in accordance with DOE's or their employer's personnel practices as applicable.

c. Any administrative actions imposed on an uncleared individual must be communicated to the respective personal identity verification office for Homeland Security Presidential Directive-12 (HSPD-12).