MANUAL

DOE M 470.4-1

Approved: 8-26-05
Review: 8-26-07
Chg 1: 3-7-06

SAFEGUARDS AND SECURITY PROGRAM PLANNING AND MANAGEMENT

U.S. DEPARTMENT OF ENERGY

Office of Security and Safety Performance Assurance

Vertical line denotes change.

AVAILABLE ONLINE AT:
http://www.directives.doe.gov

INITIATED BY:
Office of Security and Safety Performance Assurance

SAFEGUARDS AND SECURITY PROGRAM PLANNING AND MANAGEMENT

1. PURPOSE. To establish program planning and management requirements for the Department's Safeguards and Security (S&S) Program.

2. OBJECTIVES.

   a. Effect the policy in DOE P 470.1, *Integrated Safeguards and Security Management (ISSM) Policy*, by integrating program planning and management into Department of Energy (DOE) operations as determined by line management, and according to sound risk management practices. [DOE P 470.1, *Integrated Safeguards and Security Management (ISSM) Policy*, is the Department's philosophical approach to the management of the S&S Program. A principal objective of the ISSM Program is to integrate S&S into management and work practices at all levels, based on program line management's risk management-based decisions, so that missions may be accomplished without security events, such as interruption, disruption or compromise. This approach includes individual responsibility and implementation of the security requirements found in this Manual.]

   b. Establish individual responsibilities to fulfill the requirements in this Manual.

   c. Establish requirements for S&S planning and evaluations.

   d. Establish requirements for S&S management.

   e. Promulgate the requirements of the National Industrial Security Program.

3. PROGRAM INTEGRATION. S&S program planning and management must be integrated with other programs such as physical protection, protective force (PF), information security, personnel security, and nuclear material control & accountability (MC&A). Mechanisms must also exist to assure that S&S program planning is fully integrated with overall site strategic and near-term operational planning. Additionally, the activities and requirements in the weapons surety, foreign visits and assignments, safety, emergency management, cyber security, and intelligence and counterintelligence programs should also be considered in the implementation of this Manual.

4. CANCELLATIONS. The directives listed below are canceled. Cancellation of a directive does not by itself modify or otherwise affect any contractual obligation to comply with the directive. Canceled directives that are incorporated by reference in a contract remain in effect until the contract is modified to delete the reference to the requirements in the canceled directives. The publication of this Manual incorporates or cancels all previous memoranda or letters that were issued by the Office of Security or its predecessor organizations that established policy.

a. DOE N 473.9, *Security Conditions*, dated 7-8-04.

b. DOE M 470.1-1, *Safeguards and Security Awareness Program*, dated 10-02-02.

5. APPLICABILITY.

a. Departmental Elements. Except for the exclusion in paragraph 5c, this Manual applies to all Departmental elements, listed on Attachment 1. This Manual automatically applies to Departmental elements created after it is issued.

The Administrator of the National Nuclear Security Administration (NNSA) will assure that NNSA employees and contractors comply with their respective responsibilities under this Manual.

b. Contractors.

(1) The Contractor Requirements Document (CRD), Attachment 2, sets forth requirements of this Manual that will apply to site/facility management contracts that include the CRD.

(2) The CRD must be included in the site/facility management contracts that involve classified information or matter, or nuclear materials and contain DOE Acquisition Regulation (DEAR) clause 952.204-2, titled *Security Requirements*.

(a) Departmental elements must notify contracting officers of affected site/facility management contracts to incorporate this directive into those contracts.

(b) Once notified, contracting officers are responsible for incorporating this directive into the affected contracts via the *Laws, Regulations, and DOE Directives* clause of the contracts.

(3) 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. 228b.). 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*, (10 CFR Part 824).

(4) As stated in DEAR clause 970.5204-2, titled *Laws, Regulations, and DOE Directives*, 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 management

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. In doing so, contractors must not unnecessarily or imprudently flow down requirements to subcontracts. That is, contractors must both ensure that they and their subcontractors comply with the requirements of this CRD and incur only costs that would be incurred by a prudent person in the conduct of competitive business.

(5) This Manual does not automatically apply to other than site/facility management contracts. Application of any of the requirements in this Manual to other than site/facility management contracts will be communicated as follows.

(a) Heads of Field Elements and Headquarters Departmental Elements. Review procurement requests for new non-site-/non-facility-management contracts that involve classified information or matter, or nuclear materials and contain DEAR clause 952.204-2, titled *Security Requirements*. If appropriate, ensure that the requirements of the CRD of this Manual are included in the contract.

(b) Contracting Officers. Assist originators of procurement requests who want to incorporate the requirements of the CRD of this Manual in new non-site-/non-facility-management contracts, as appropriate.

c. Exclusion. In accordance with the responsibilities and authorities assigned by Executive Order 12344 and to ensure consistency throughout the joint Navy and DOE organization of the Naval Nuclear Propulsion Program, the Deputy Administrator for Naval Reactors will implement and oversee all requirements and practices pertaining to this Manual for activities under the Deputy Administrator's cognizance.

d. Exemption.

(1) Requirements in this Manual 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 Office of Civilian Radioactive Waste Management (RW) facilities.

(2) This exemption does not apply to requirements for which the NRC defers to DOE or does not exercise regulatory jurisdiction.

6. DEVIATIONS. Deviations from requirements must be processed in accordance with Section M.

7. DEFINITIONS. Terms commonly used in the program are defined in the S&S Glossary located in DOE M 470.4-7, *Safeguards and Security Program References*. In addition to those in the Glossary, the following definitions are provided for use in this Manual.

a. DOE line management refers to DOE and NNSA Federal employees who have been granted the authority to commit resources or direct the allocation of personnel or approve implementation plans and procedures in the accomplishment of specific work activities.

b. Line management refers to DOE and NNSA Federal and contractor employees who have been granted the authority to commit resources or direct the allocation of personnel or approve implementation plans and procedures in the accomplishment of specific work activities.

c. DOE cognizant security authority refers to DOE and NNSA Federal employees who have been granted the authority to commit security resources or direct the allocation of security personnel or approve security implementation plans and procedures in the accomplishment of specific work activities.

d. Cognizant security authority refers to DOE and NNSA Federal and contractor employees who have been granted the authority to commit security resources or direct the allocation of security personnel or approve security implementation plans and procedures in the accomplishment of specific work activities.

e. Category I/II refers to facilities or sites possessing Category I quantities of special nuclear material (SNM) or credible rollup quantities of SNM to a Category I quantity.

f. For the purposes of this Manual, the Office of Security refers to the DOE Office of Security, Office of Security and Safety Performance Assurance.

8. IMPLEMENTATION. Requirements that cannot be implemented within 6 months of the effective date of this Manual or within existing resources must be documented by the cognizant security authority and submitted to the relevant program officers: the Under Secretary for Energy, Science and Environment or the Under Secretary for Nuclear Security/Administrator, NNSA; and the Office of Security. The documentation must include timelines and resources needed to fully implement this Manual. The documentation must also include a description of the vulnerabilities and impacts created by the delayed implementation of the requirements.

Vertical line denotes change.

9. CONTACT. Questions concerning this Manual should be directed to the Office of Security at 202-586-3345.

BY ORDER OF THE SECRETARY OF ENERGY:

CLAY SELL
Deputy Secretary

CONTENTS

PART 1. PLANNING AND EVALUATIONS

Vertical line denotes change.

CONTENTS (continued)

CONTENTS (continued)

SECTION D—SITE SAFEGUARDS AND SECURITY PLAN/RESOURCE PLAN

CONTENTS (continued)

Vertical line denotes change.

CONTENTS (continued)

CONTENTS (continued)

Vertical line denotes change.

CONTENT (continued)

CONTENTS (continued)

Vertical line denotes change.

CONTENTS (continued)

Vertical line denotes change.

CONTENTS (continued)

Vertical line denotes change.

ATTACHMENTS

PART 1—PLANNING AND EVALUATIONS

SECTION A—SAFEGUARDS AND SECURITY PROGRAM PLANNING

1. OBJECTIVE. To establish a standardized approach for protection program planning that will provide an information baseline for use in integrating Departmental safeguards and security (S&S) considerations, facilitating management evaluation of program elements, determining resources for needed improvements, and establishing cost-benefit bases for analyses and comparisons.

2. REQUIREMENTS. The following are essential elements for planning for S&S programs.

   a. S&S Philosophy. S&S interests and activities must be protected from 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. DOE protective forces (PFs) that protect Category I quantities of special nuclear material (SNM); credible rollup of SNM to a Category I quantity; or those facilities that meet or exceed the Threat Level 2 criteria specified in DOE O 470.3A, *Design Basis Threat Policy*, dated 11-29-05, for chemical, radiological, or biological thresholds, must employ the DOE Tactical Doctrine contained in Appendix 2 of Section A.

   b. S&S Management Plan. This Plan must provide a description of the implementation of S&S policy and provide detailed information on the assignment of roles, responsibilities, and authorities, as well as the development of budgets and allocation of resources. The S&S Management Plan must be updated annually (at least every 12 months) and must document:

      (1) roles, responsibilities, delegations, and authorities for the S&S program;

      (2) organizational structure and accountability; and

      (3) planning and budget (including personnel resources).

      See Appendix 1, S&S Management Plan, for content requirements and suggested format. However, if a *Functions, Responsibilities, and Authorities Manual* for S&S has been approved and issued, and it meets the requirements stated above, it can be used in place of a S&S Management Plan.

   c. S&S Program Operations. Actions must be taken to ensure an acceptable S&S program, including curtailment or suspension of operations when such operations would result in an immediate and unacceptable impact to national security, the environment, or the health and safety of the public or employees.

Vertical line denotes change.

(1) Site-Specific Characterization. Protection programs must be tailored to address specific site characteristics and requirements, current technology, ongoing programs, and operational needs to achieve acceptable protection levels that reduce risks in a cost-effective manner.

(2) Threat Policy/Guidance. DOE O 470.3, *Design Basis Threat (DBT) Policy* must be used with local threat guidance during the conduct of vulnerability assessments (VAs) for protection and control program planning. The DBT must be the baseline threat definition but local threat guidance may be used to increase the level of threat to be analyzed.

(3) Targeted Protection Strategies.

(a) Strategies for the physical protection of special nuclear materials (SNM) and vital equipment must incorporate the applicable requirements established in DOE M 470.4-2, *Physical Protection*.

(b) Protection strategies must be implemented as specified in the DBT. PF resources must focus on decisively defeating the terrorist threat, which is facilitated by positioning posts so there is little or no delay in responding to critical targets, eliminating posts which detract from constant readiness, and maximizing use of physical protection systems to enhance PF effectiveness. PF resources must be positioned to interdict and neutralize the adversary threat as far as possible outside the boundaries of the target location.

(c) Protection program elements must be designed to prevent and/or mitigate the consequences of acts of radiological, chemical, or biological sabotage that would cause unacceptable impact to national security, the environment, or the health and safety of the public or employees. Protection elements, such as active denial systems, must be designed and deployed to minimize the need for PF recapture/recovery operations.

(d) Strategies for the protection and control of classified information or matter must incorporate the applicable requirements established in DOE M 470.4-4, *Information Security*.

(e) Security systems must be used that prevent, detect, or deter unauthorized access, modification, or loss of classified and unclassified controlled matter and its unauthorized removal from a site or facility.

(f) Strategies for the protection of government property not covered above must reflect a graded approach. DOE offices, facilities, and

Vertical line denotes change.

property protection areas (PPAs) must meet or exceed General Services Administration (GSA) minimum security standards.

(g) Security countermeasures for explosive threats must address a range of activities including hand-carried, mailed, and vehicle-transported devices.

d. Graded Protection. The Department recognizes that risks must be accepted (i.e., that actions cannot be taken to reduce the potential for or consequences of all malevolent events to zero); however, an acceptable level of risk must be determined based on evaluation of a variety of facility-specific goals and considerations. By a graded approach, the Department intends that the highest level of protection be given to security interests and activities whose loss, theft, compromise, and/or unauthorized use would seriously affect the national security, the environment, Departmental programs, and/or the health and safety of the public or employees. Protection of other interests and activities must be graded accordingly.

e. Risk Management. S&S programs must be based on the results of vulnerability and risk assessments, the results of which are used to design and provide graded protection in accordance with an asset's importance or the impact of its loss, destruction, or misuse. The results of the assessments, to include the determination of system effectiveness, are one of the key considerations the manager must evaluate when establishing the level of risk. For example, if it is determined that there is high risk that is not being mitigated by compensatory measures, reporting must be made to the Secretary of Energy or the Deputy Secretary who can accept high risk. Cognizant Under Secretaries can accept moderate risk.

(1) Vulnerability and risk assessments must be conducted and documented to support the identification of risks to be accepted by the Department.

(2) To determine the appropriate level of protection against risk, line management must consider the threat, the vulnerability of the potential target, and the potential consequences of an adversarial act.

f. Site-Specific Programs.

(1) S&S programs must address site-specific characteristics.

(2) Performance assurance programs must be developed, managed, and implemented to ensure that S&S programs and protection program elements protect security interests and activities. These programs must ensure intensive, frequent performance testing of PF individual and unit tactics with oversight by line management and independent oversight organizations.

Vertical line denotes change.

(3) A management and planning process to achieve integrated, site-specific protection from unauthorized actions must be implemented. This process must be based on a graded approach that implements the integrated concepts of deterrence, prevention, detection, and response.

(4) The DBT must be used as the basis for planning protection programs.

3. PLANNING.

a. S&S Plans. S&S plans must be developed for facilities with any of the following S&S interests:

(1) Category I quantities of SNM or credible roll-up quantities of SNM to a Category I quantity;

(2) Category II, Category III, or Category IV SNM;

(3) radiological, chemical, or biological sabotage threats;

(4) critical mission disruption threats;

(5) intra-/inter-site transportation of SNM;

(6) classified information or matter;

(7) facilities engaged in the protection of government property;

(8) facilities that the Secretary, Deputy Secretary, or Under Secretaries deem appropriate.

b. Site Safeguards and Security Plan (SSSP). The SSSP is a 5-year master planning document that must be prepared for sites with facilities described in paragraphs 3a(1), (3), (4), or (8) above. The SSSP must depict the existing condition of site protection programs and, when the DBT performance standard cannot be met, establish improvement priorities and resource requirements for the necessary improvements. Plan composition is reflected in Part 1, Section C, 5.

c. Site Security Plan (SSP). At locations where an SSSP is not required because of the limited scope of interests (i.e., criteria contained in 3a(2), (5), (6), or (7) above, apply), an SSP must be developed to describe the protection program. SSPs must be approved by the local DOE cognizant security authority. In addition, specialized plans must be developed to address protection programs for other protection operations. Requirements for specialized plans that may or may not be components of the SSP are set forth in the applicable DOE directives.

d. Planning Inputs. The documents listed below must be used to support program forecasts and information input used in the protection program planning process.

(1) Applicable Departmental directives, guidance, and intelligence assessment information developed and disseminated by line management or the Office of Security.

(2) Programmatic guidance and forecasts of significant changes planned in site operations as communicated through line management.

(3) Current and projected operational constraints and resources.

(4) Analysis of cost and effectiveness of security technologies versus traditional protection methodologies.

e. Plan Review and Approval.

(1) The SSSP requires approval by DOE line management and concurrence by the cognizant Head of the Departmental Element (see Attachment 1). Such approval authority must be formally delegated to line management.

(a) Copies of approved SSSPs must be provided to the Office of Security for review and comment.

(b) Other security plans may be approved as stipulated in the applicable directive. If approving authority is not otherwise stipulated, these security plans may be approved by DOE line management.

(2) The SSSP must be submitted to DOE line management within 150 days of the termination date of data collection and approved within 120 days of the submittal date. Directive changes, facility reconfiguration, a new VA, or other activities that occur after the stated effective date will not be considered for purposes of reviewing/approving the plan.

(3) The SSSP must be reviewed annually (at least every 12 months). Updates to the SSSP that may significantly alter the agreed-upon protection philosophy or performance standards of protection systems must be subjected to the formal VA process, and if changes are shown to significantly alter system effectiveness performance, the update(s) will be subject to the same concurrence and approval as stated in paragraph 3e(1), above.

(4) An information copy of approved modifications must be provided to the Office of Security.

SECTION A

APPENDIX 1—SAFEGUARDS & SECURITY MANAGEMENT PLAN

The Safeguards and Security (S&S) Management Plan provides a description of the implementation of S&S policy and provides detailed information on the assignment of roles, responsibilities, and authorities, as well as the development of budgets and allocation of resources. The following outline delineates the content requirements and provides a suggested format.

1. EXECUTIVE SUMMARY.

   a. Program Mission Statement. Briefly describe the program mission and how the mission relates to national security. Describe the major elements or activities performed in terms of program mission and its relationship to the DOE national security mission.

   b. S&S Program Structure. Briefly describe the strategy and organizational elements used to implement the S&S program under their cognizance.

   c. Management and Planning Assumptions. Briefly describe those assumptions that affect the management and planning of the implementation of the S&S program. These assumptions should include items such as:

      (1) future of the program (mission, staffing levels, site status, etc.);

      (2) current and planned S&S projects; and

      (3) status of the organization's S&S budget.

2. PART 1—ORGANIZATIONAL STRUCTURE AND ACCOUNTABILITY

   a. Line Management Organization. Describe the structure and relationship of line management. Identify the roles, responsibilities, and authorities of these line management elements to include organizational charts.

   b. Cognizant Security Authority Organization. Describe the structure of line management that is specifically responsible for implementing the Departmental element's S&S program. Identify the individuals and positions responsible for committing resources and directing the activities of personnel associated with the S&S program.

      (1) Headquarters Organizational Structure. For the Headquarters elements, provide an organizational chart to show the S&S organization and management structure and the lines of authority and points of interface with other programs which affect S&S (e.g., safety, facility operations,

and the cognizant security authority's material control and accountability (MC&A) organization, if independent of the security organization). Describe the functions and responsibilities of S&S personnel and indicate how S&S activities are integrated with those of other facility organizations; include organizational responsibilities for line management overseeing the program as well as the interface points with the respective Departmental element.

(2) Field Organizational Structure. For the Field elements, provide an organizational chart to show the S&S organization and management structure and the lines of authority and points of interface with other programs which affect S&S (e.g., safety, facility operations, and the cognizant security authorities' MC&A organization, if independent of the security organization). Describe the functions and responsibilities of S&S personnel and indicate how S&S activities are integrated with those of other facility organizations; include organizational responsibilities for line management overseeing the program as well as the interface points with the respective Departmental element.

c. Contractor Sites. Provide the contract name, number, and other information that describes the authority under which the contractor executes management functions for facilities under the cognizance of a Departmental element. Identify the site contractor elements responsible for S&S programs and describe their S&S activities. Provide Federal and contractor organization charts and identify key positions and the relationships between the organizations responsible for S&S activities. Describe Federal and contractor involvement in the development of S&S resource requirements.

3. PART 2—ROLES, RESPONSIBILITIES, DELEGATIONS, AND AUTHORITIES. Delegations must be documented in writing and delineate all assigned S&S roles, responsibilities, and authorities for the S&S program. This section:

a. documents offices/positions affected by the S&S Management Plan;

b. establishes the approval chain for S&S plans, procedures and implementation policy;

c. establishes the approval chain for S&S policy deviations;

d. assigns reporting requirements for incidents of security concern; and

e. provides a list of roles and responsibilities for key positions and the delegated authorities for each.

4. PART 3—S&S PROGRAM IMPLEMENTATION. This section of the S&S Management Plan documents the processes and methods used to implement the Department's security policies. This section identifies:

   a. the methods used for ensuring all applicable programmatic requirements are implemented throughout the organizational element;

   b. the methods used for ensuring effective integration of S&S programmatic elements; and

   c. SSSPs and SSPs used to implement S&S policy requirements.

5. PART 4—PLANNING AND BUDGET (INCLUDING PERSONNEL RESOURCES). This section of the S&S Management Plan documents the key processes of planning and budgeting, including strategic planning, budget formulation, budget execution, and program evaluation.

   a. Describe the strategic planning assumptions used to ensure the S&S program will meet mission objectives.

   b. Provide a 5-year plan that describes the budget formulation priorities for future S&S resources and programs.

   c. Provide the current year plan for executing the S&S budget. This plan details the allocation of resources that support S&S functions and missions.

   d. Provide a program evaluation plan that details how the cognizant security authority will assess the implementation of the S&S program and the organization's progress toward meeting established missions/goals. The program evaluation plan must cover both the Federal and contractor elements of the Departmental element. This plan can be used to support award fee decisions by the Departmental element.

   e. Briefly describe any changes to operational requirements which affect S&S program operations or would require increments or decrements to operational accounts (e.g., program direction, operational support, etc.).

SECTION A

APPENDIX 2—DEPARTMENT OF ENERGY TACTICAL DOCTRINE

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 appendix is the condensed expression of the Department‘s fundamental approach to protecting nuclear weapons and components, special nuclear material, or targets subject to radiological or toxicological sabotage. 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 is supported by fixed strong points, obstacles/barriers, advanced detection and assessment capabilities, coordinated fire planning, updated weapon systems, and armored vehicles.

   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. When availability of armed PFs is limited, 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. TACTICAL DOCTRINE.

   a. Concept. In general, at Category I/II 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. A Tactical Response Force (TRF) 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 mobile

Vertical line denotes change.

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 fixed, 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.

Vertical line denotes change.

(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 a decisive engagement with the adversary.

(h) Protect defenders by employing hardened fighting positions situated for mutual support.

(i) Establish supplementary defensive positions.

(j) Prepare to maneuver offensive 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) Assign sufficient resources to be able to assess remote alarms to identify the number of adversaries, thereby helping to differentiate between diversionary attacks and the main force.

(c) Plan for staged withdrawal of forces dispatched to assess remote alarms to prepared supplementary defensive positions.

(d) Plan for overwatch of assessment forces with long range weapons from within the defensive perimeter.

(e) 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.

(f) Ensure adequate standoff for vehicle-borne improvised explosive devices (VBIEDs).

(g) 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.

Vertical line denotes change.

(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 area 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 TRF is deployed in a strategic posture to interrupt, interdict, deny, and neutralize an adversary force attack. The TRF is armed and equipped with state of the art weaponry, tactical equipment, vehicles, and communication systems. The TRF is adept at implementing approved Security Incident Response Plans under adverse emergency conditions. The primary mission of the TRF is the protection of nuclear weapons, weapons components, and SNM from theft, sabotage, and unauthorized control. Ancillary duties include the safeguarding of classified information and other classified assets.

(1) Tactical Response Force Characteristics.

(a) Survivability

(b) Mobility

(c) Lethality

(d) Flexibility

(e) Speed

(f) Unpredictability

(g) Mutual Support

(h) Reliable communications

Vertical line denotes change.

(2) Tactical Response Force Element Missions. A site TRF is composed of small units/teams of no fewer than two SPO II and/or SPO III personnel, deployed in configurations that provide tactical advantages for both defensive and offensive operations.

(a) Special Response Team (SRT).

Mission: The SRT executes recapture/recovery and pursuit operations and supports interruption, interdiction, neutralization, containment, and denial strategies.

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.

Mission: Executes interruption, interdiction, neutralization, containment, and denial strategies and supports recapture/recovery and fresh pursuit operations.

Capabilities: SPO II personnel operate in small units with specialized weapons and equipment from mobile patrols/tactical vehicles and fixed posts.

(3) Tactical Response Force Support. All site Security Police Officers and Security Officers have a key role in supporting the overall site security posture and the TRF.

(a) Security Police Officer-I.

Mission: Supports interruption, interdiction, neutralization, containment, and denial strategies.

Capabilities: SPO I personnel operate from mobile patrols and fixed posts. SPO I personnel perform routine S&S related functions and are capable of performing specialized active defense functions such as staffing defensive fighting positions, operating Remotely Operated Weapon Systems (ROWS), and performing Central Alarm Station (CAS) duties.

(b) Security Officer.

Mission: Ensures routine security-related functions are maintained (e.g., access/egress control, escort duties, CAS operations).

Vertical line denotes change.

Capabilities: Unarmed SOs perform observation and reporting activities, logistical re-supply to other PF elements, message courier duties, and provide transportation support.

(4) Deployment Considerations.

(a) A layered, or zone, defensive strategy is implemented that maximizes the TRF'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.

(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 TRF member is issued at least one primary weapon along with a secondary firearm, such as a handgun, used principally for close quarters engagement or for transition in the event of a stoppage of the primary weapon.

(g) TRF weapons are capable of tactical operations in both day and night conditions.

(h) The TRF employs direct-fire weapons (i.e., machine guns, precision rifles, battle rifles, etc.) to engage and to neutralize adversary forces out to the maximum effective range of the weapon.

(i) As prescribed by the SSSP, the TRF employs indirect-fire or explosive projectile weapons (e.g., M3 MAAWS, MK19/GMG, M203, etc.) to deny access to target locations and to suppress and to neutralize adversary forces occupying positions of cover and/or concealment.

(j) TRF members are knowledgeable of adversary attack methods identified in the Design Basis Threat (DBT) 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."

(5) 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 (for a two-person crew, usually the gunner).

(d) Potential target access points are covered by suppressive fire weapons.

(e) TRF members utilize positions of cover and maximize the element of surprise to the extent possible.

(f) The TRF initiates a decisive engagement with adversary forces as far as possible outside the target location.

(g) Once an adversary has been identified and engaged, TRF elements never lose contact.

Vertical line denotes change.

(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) TRF teams, using suppressive fire weapons, maneuver in force against adversaries occupying covered positions.

(j) The TRF has plans in place to transition quickly from defensive to offensive operations.

(6) Recapture/Recovery Operations.

(a) The site PF is staffed and deployed in sufficient strength to ensure the protection of sensitive assets. The dedicated recapture/recovery element of the SRT is established with additional resources sufficient to ensure that recapture/recovery 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/recovery operations within identified target locations.

(c) SRTs possess the 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 SNM is at risk, regaining control of the SNM is the primary consideration.

(e) SRTs are supported by other TRF elements to the maximum extent possible as they move toward the target objective.

(f) TRF members provide overwatch for the assault team(s) movement, cover avenues of approach, and provide support by fire to the SRT as they breach/enter the target location.

(g) All TRF personnel are capable of providing direct support to the recapture/recovery mission by supplementing the main assault force, controlling the target area, and suppressing enemy defensive positions.

(7) Pursuit Operations.

(a) TRF members are trained and equipped to conduct Fresh Pursuit operations, on and off DOE property in accordance with DOE

Vertical line denotes change.

M 470.4-3, Section A, Appendix A-1, "Guidelines for Fresh Pursuit."

(b) Fresh Pursuit operations are coordinated with responding Federal, State, and local law enforcement agencies according to approved agreements.

(c) TRF members use vehicle immobilization techniques and/or other means of applying deadly force to terminate the pursuit.

(d) TRF members maintain control of sensitive assets until relieved by cognizant Federal authorities.

(8) Weapons of Mass Destruction.

(a) All TRF and SPO-I 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) TRF 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.

3. 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. A requirement for increased FOFs for training purposes does not always have to involve the very large scale exercises that are conducted during inspections and annual SSSP validations. 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.

Vertical line denotes change.

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 small and as few 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 DOE M 470.4-3, *Protective Force*, Section A, Chapter II, paragraph 9.

Vertical line denotes change.

SECTION B—SECURITY CONDITIONS

1. OBJECTIVE. To ensure that the Department uniformly meets the requirements of the Homeland Security Advisory System outlined in Homeland Security Presidential Directive-3, (HSPD-3), dated 3-11-02, and provides the responses specified in Presidential Decision Directive 39, *U.S. Policy on Counterterrorism* (U), dated 6-21-95.

2. THREAT INDICATORS. While the Design Basis Threat (DBT) provides specific description of threats that all components of the safeguards and security (S&S) system must be capable of defeating, analysis of terrorism should be an ongoing process. Although each analysis relies on information included in previous assessments, judgments with respect to threats to Federal and Department of Energy (DOE)-affiliated personnel, facilities, and assets begin anew with each analysis.

   a. Homeland Security Threat Conditions [known in DOE as Security Conditions (SECONs)] 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. A threat indicator is a condition that, when present, increases the possibility of a terrorist incident. Seldom does one single indicator suggest that the threat is imminent, but, when a number of indicators are present, the level of concern should increase correspondingly. A decision on assigning SECONs must integrate a variety of considerations. This integration will rely on qualitative assessment, not quantitative calculation. Higher SECONs indicate greater risk of a terrorist act, with risk including both probability and gravity. Despite best efforts, there can be no guarantee that, at any given SECON, a terrorist attack will not occur. An initial and important factor is the quality of the threat information itself. The evaluation of this threat information includes, but is not limited to, the following factors.

      (1) To what degree is the threat information credible?

      (2) To what degree is the threat information corroborated?

      (3) To what degree is the threat specific and/or imminent?

      (4) How grave are the potential consequences of the threat?

   b. Local and site-specific threat analysis is a dynamic process because the threat and the countermeasures used to combat the threat are constantly changing. To keep up with possible changes in the threat, security professionals should develop a predetermined list of general and specific threat indicators. Threat indicators should be revised according to site/facility situations and needs. They should be reviewed at least every 6 months or when a significant incident or change in conditions indicates that the threat level is increasing or decreasing. Examples of

threat indicators that can be used to develop a site-/facility-specific assessment are listed below.

(1) International incidents or indicators against U.S. interests, personnel, or facilities.

(2) Domestic incidents or indicators against Federal or State interests countrywide.

(3) Local incidents or indicators directed against Federal or DOE interests.

(4) Specific targeting of DOE personnel, facilities, or materials.

3. SECURITY CONDITIONS. The DOE SECON system has been aligned with the Homeland Security Advisory System.

a. The DOE SECON system describes a progressive level of common sense protective measures that may be implemented in response to a malevolent or terrorist threat to any or all DOE facilities, assets, and personnel. The purpose of the SECON system is to establish standardized protective measures for a wide range of threats and to help disseminate appropriate, timely, and standardized information for the coordination and support of DOE crisis or contingency activities. Once a SECON level is declared, the associated protective measures should be implemented as soon as possible to the extent they apply to the individual site or facility. Cognizant security authorities must coordinate SECON status through their DOE points of contact, as appropriate, and notify the DOE Headquarters (HQ) Operations Center (OC) and Departmental element of the site/facility SECON status. Measures associated with each SECON are not prioritized but should be initiated concurrently when practical.

b. National Nuclear Security Administration (NNSA) facilities must be prepared to respond to SECON directives provided by the Under Secretary for Nuclear Security/Administrator, NNSA. Non-NNSA facilities must be prepared to respond to SECON directives provided by the Under Secretary for Energy, Science and Environment for their individual facilities. Headquarters facilities must be prepared to respond to SECON directives provided by the Director, Office of Security. At their discretion, DOE line management may increase protection measures for facilities under their cognizance if they determine that the local threat situation warrants additional security. In this event, the DOE HQ OC and Departmental element must be notified of the SECON level. If DOE line management or Departmental elements believe that their facilities' SECON levels should be less than those issued by the Under Secretary for Energy, Science and Environment or the Under Secretary for Nuclear Security/Administrator, NNSA, a request for exception must be submitted for consideration (see paragraph 3c below).

c. Any departure from the requirements of this section must be considered an exception which must be approved in accordance with the requirements set forth in Section M. No exception is permitted to the protective measures when under SECON 1, Severe Condition (Red).

d. To the extent possible throughout each increase or decrease in SECON, the cognizant security authority must:

(1) keep employees informed;

(2) coordinate when appropriate with State and local officials' actions taken regarding security and emergency planning; and

(3) at each level of SECON, review security plans, vulnerability assessments (VAs), emergency response procedures, public affairs guidance and plans, legal authorities, and Continuity of Operations Plans.

e. A record of specific actions taken for each measure must be maintained. A description of each SECON, including the necessary circumstances for implementing, the impact on operations, and the purpose of each protective posture, is outlined below.

(1) **SECON 5, LOW CONDITION (GREEN).** This condition is declared when there is a low risk of terrorist attacks. SECON 5, Low Condition (Green) exists when a general threat of possible malevolent or terrorist activity exists, but warrants only a routine security posture.

(2) **SECON 4, GUARDED CONDITION (BLUE).** This condition is declared when there is a general risk of terrorist attacks. SECON 4, Guarded Condition (Blue) applies when there is an increased general threat of possible malevolent or terrorist activity against personnel and facilities, the nature and extent of which are unpredictable, and circumstances do not justify full implementation of SECON 3, Elevated Condition (Yellow) measures. It may be necessary, however, to implement certain selected measures from higher SECONs to address intelligence received or to act as a deterrent. All measures selected for use under SECON 4, Guarded Condition (Blue) must be capable of being maintained indefinitely.

(a) Measure 1. At regular intervals, warn all personnel to report the following to security:

1 suspicious personnel, particularly those carrying suitcases or other containers, or those observing, photographing, or asking questions about site operations or security measures;

2 unidentified vehicles parked or operated in a suspicious manner on or in the vicinity of the site or near site facilities;

3 abandoned parcels or suitcases; and

4 any other activity considered suspicious.

(b) Measure 2.

1 Ensure that security personnel have immediate access to building floor plans and emergency/evacuation plans for all site facilities.

2 Ensure that security personnel are able to seal off an area immediately.

3 Ensure that key personnel required to implement security plans are on-call and readily available.

4 Maintain the site Emergency Management Team (EMT) on 2-hour recall.

5 Expand Operations Security measures.

6 Exercise bomb threat procedures.

(c) Measure 3. Secure and seal buildings, rooms, and storage areas not in regular use. Maintain a list of secured facilities.

(d) Measure 4. Increase unannounced security spot checks (inspection of personal identification; vehicle registration; and the contents of vehicles, suitcases, briefcases, and other containers) at access points for the site and facilities.

(e) Measure 5. Reduce the number of access points for vehicles and personnel to minimum levels consistent with the requirement to maintain a reasonable flow of traffic.

(f) Measure 6. As a deterrent, randomly apply measures 14, 15, 16, 17, or 18 from SECON 3, Elevated Condition (Yellow) either individually or in combination.

(g) Measure 7. Review all operations plans, personnel details, and logistics requirements that pertain to implementing higher SECONs.

(h) Measure 8. Review security measures for critical/sensitive personnel (e.g., directors, managers, members of special access/ security programs, etc.) and implement additional measures warranted by the threat and existing vulnerabilities (e.g., identified personnel should alter established patterns of behavior when traveling in public areas).

(i) Measure 9. Increase liaison with local law enforcement, intelligence community, security agencies, and the Federal Bureau of Investigation, (FBI) to monitor the threat to site personnel and facilities. Notify local law enforcement agencies and the FBI concerning SECON 3, Elevated Condition (Yellow) measures that, if implemented, could affect their operations in the local community.

(j) Measure 10. Reserve for site/facility use.

(3) **SECON 3, ELEVATED CONDITION (YELLOW).** A SECON 3, Elevated Condition (Yellow) is declared when there is a significant risk of terrorist attack. Elevated Condition (Yellow) applies when an increased and more predictable threat of malevolent or terrorist activity exists. The measures in this SECON must be capable of being maintained for lengthy periods without causing undue hardship, affecting operational capability, or aggravating relations with the local community. For measures requiring an increase in the frequency of a specific action, the new frequency is to be more often than in the lower-level security condition. In addition to the measures required by SECON 4, Guarded Condition (Blue), the following measures should be implemented.

(a) Measure 11. Increase the frequency of warnings required by Measure 1, and inform personnel of additional unclassified threat information, if available. Encourage increased community security awareness of suspicious persons, vehicles, and activities.

(b) Measure 12. Maintain EMT personnel on 2-hour recall; periodically exercise recall to ensure readiness. Keep all other personnel involved in implementing special response/contingency plans on call. Identify, contact, and brief specialists that may be required for unique contingencies; coordinate lines of communication.

(c) Measure 13. Review provisions of all operations plans and orders and special operating procedures associated with implementing SECON 2, High Condition (Orange).

(d) Measure 14. Move automobiles and objects such as trash containers, newspaper boxes, crates, etc., at least 30 yards from all facilities, particularly buildings of a sensitive or prestigious nature. Identify any areas where an improvised explosive device could be hidden (i.e., pallet stacks, trash piles, stacked construction supplies, etc.). If the configuration of the facility or area precludes implementation of this measure, take appropriate compensatory measures per local plans [frequent inspection by Explosive Ordnance Disposal (EOD) teams, if available; controlled access to parking areas; etc.]. Consider centralized parking.

(e) Measure 15. Secure, seal, and regularly inspect all buildings, rooms, and storage areas that can be isolated with minimum site impact.

(f) Measure 16. At the beginning and end of each work day and at frequent intervals, inspect the interior and exterior of buildings in regular use for suspicious activity or unattended packages and for signs of tampering or indications of unauthorized entry.

(g) Measure 17. Implement screening procedures for all incoming official mail to identify possible explosive or incendiary devices or other dangerous material. If available, have EOD-trained teams inspect suspicious items and screen mail periodically. Provide guidance concerning suspicious packages. Encourage employees to inspect their individual mail, report suspicious items to security, and refrain from handling such items until cleared by the appropriate authority.

(h) Measure 18. Inspect other deliveries and locally designated common-use facilities to identify explosives and incendiary, biological, or chemical devices. Use EOD-trained teams for some screening inspections when available. Instruct site personnel to report suspicious packages to security and refrain from handling them until cleared by the appropriate authority.

(i) Measure 19. Increase both overt and covert security force surveillance of locally designated soft targets to improve deterrence and build confidence among site personnel. (Covert surveillance must comply with DOE directives and appropriate regulatory restrictions.)

(j) Measure 20. Inform employees of the general threat situation. Limit visitors and escorted uncleared personnel. Periodically update all personnel as the situation changes to stop rumors and prevent unnecessary alarm.

(k) Measure 21. Brief representatives of all activities on the site concerning the threat and security measures implemented in response to the threat. Explain reasons for actions. Implement procedures to provide periodic updates for these activity representatives.

(l) Measure 22. Verify the identity of all personnel entering property protection areas (PPAs) and other sensitive activities specified in local plans (i.e., inspect identification badges and grant access based on visual recognition). Use of automated access control systems at interior security areas is acceptable and encouraged, where practical.

On a random basis, visually inspect the interior of all vehicles and the exterior of all suitcases, briefcases, packages, and other containers. Increase the frequency of detailed vehicle inspections (trunk, undercarriage, glove boxes, etc.) and the frequency of detailed inspections of suitcases, briefcases, and other containers.

(m) Measure 23. Increase the frequency of random identity checks (inspection of security badges and vehicle registration documents) conducted by security force patrols on the site.

(n) Measure 24. Remind all personnel to lock parked vehicles and inspect vehicles for suspicious items before entering and driving them.

(o) Measure 25. Implement additional security measures for critical/sensitive personnel in accordance with existing plans.

(p) Measure 26. Brief all security force personnel concerning the threat and policies governing rules of engagement, use of deadly force, and fresh pursuit. Ensure there is no misunderstanding of these instructions. Repeat this briefing on a periodic basis.

(q) Measure 27. Increase liaison with local police, intelligence, security agencies, and the FBI to monitor the threat to site personnel and facilities. Notify local police agencies concerning SECON 2, High Condition (Orange) or SECON 1, Severe Condition (Red) measures that, if implemented, could affect their operations in the local community.

(r) Measure 28. Survey the surrounding area to determine whether operational activities near the area might create emergencies or contingencies that could affect the site/facility (e.g., airports,

military/other government facilities, industrial facilities, railroads or pipelines, etc.).

(s) Measure 29. Reserve for site/facility use.

(4) **SECON 2, HIGH CONDITION (ORANGE).** A SECON 2, High Condition (Orange) is declared when there is a high risk of terrorist attacks. This condition applies when an incident occurs or intelligence is received indicating that some form of malevolent or terrorist action against personnel and facilities is imminent. Implementation of measures in this security condition for more than a short period probably will create hardship and affect the routine activities of the site and its personnel. For measures requiring an increase in the frequency of a specific action, the new frequency is to be more often than in the lower level SECON. The following measures should be implemented.

(a) Measure 30. Continue all SECON 4, Guarded Condition (Blue) and SECON 3, Elevated Condition (Yellow) measures or introduce those that have not already been implemented.

(b) Measure 31. Recall staff representatives and initiate 24-hour operation of the EMT. Place the Special Response Team (SRT) on standby alert. Keep all personnel responsible for implementing special/response contingency plans at their places of duty. Review site evacuation plans.

(c) Measure 32. Reduce site access points to the absolute minimum necessary for continued operation.

(d) Measure 33. Verify the identity of all personnel entering the site/facilities, including appropriate offsite facilities under DOE control. Inspect all security badges for tampering. On a random basis, visually inspect the interior of all vehicles and the exterior of all suitcases, briefcases, and other containers. Increase the frequency of detailed vehicle inspections (trunk, undercarriage, glove compartments, etc.) and the frequency of inspections of suitcases, briefcases, and other containers.

(e) Measure 34. Implement centralized parking and shuttle bus service, where required.

(f) Measure 35. Ensure that security personnel have been briefed concerning policies governing the rules of engagement, use of force, and fresh pursuit, particularly criteria for use of deadly force. Ensure that non-security supervisory personnel are familiar with above policies and procedures, if applicable. Ensure that

special equipment and ammunition are available for immediate issue.

(g) Measure 36. Increase security patrol activity to the maximum level sustainable. The concept of continuing random security patrol activity is encouraged.

(h) Measure 37. Position security force personnel in the vicinity of critical facilities.

(i) Measure 38. Erect barriers required to control direction of traffic flow and to protect facilities vulnerable to bomb attack by parked or moving vehicles.

(j) Measure 39. Consult local authorities about closing public roads and facilities that might make sites more vulnerable to terrorist attacks.

(k) Measure 40. Consider canceling public events.

(l) Measure 41. Consider initiating Continuity of Operations plans

(m) Measure 42. Reserve for site/facility use.

(5) **SECON 1, SEVERE CONDITION (RED).** A SECON 1, Severe Condition (Red) reflects a severe risk of terrorist attacks. This condition applies in the immediate area where a malevolent or terrorist attack has occurred that may affect the site or when an attack is initiated on the site. Implementing SECON 1, Severe Condition (Red) will create hardship and affect the activities of the site and its personnel. Normally, this SECON is declared as a localized response. For measures requiring an increase in the frequency of a specific action, the new frequency is to be more often than in the lower-level SECON. The following measures should be implemented.

(a) Measure 43. Continue all previous SECON measures and introduce those that have not already been implemented.

(b) Measure 44. Augment security forces to ensure absolute control over access to the site, facilities, and other potential target areas. Establish surveillance points; use night-vision devices.

(c) Measure 45. Working closely with facility management, identify the owners of all vehicles already on the site. In those cases where the presence of a vehicle cannot be explained (owner is not present and the vehicle has no obvious site affiliation), inspect the vehicle for explosives; incendiary, chemical, or biological devices; or

other dangerous items and remove the vehicle from the vicinity of facilities, soft targets, and other sensitive areas as soon as possible.

(d) Measure 46. Inspect all vehicles entering the site. Inspections should include cargo storage areas, undercarriage, glove boxes, and other areas where explosives, incendiary, chemical, or biological devices or other dangerous items could be concealed.

(e) Measure 47. Limit access to the site, facilities, and other areas to those personnel with a legitimate and verifiable need to enter. Implement positive identification of all personnel. No exceptions.

(f) Measure 48. Inspect all baggage such as suitcases, packages, and briefcases brought on the site for explosives, incendiary, chemical, or biological devices, or other dangerous items.

(g) Measure 49. Implement frequent inspections of the exterior of buildings (including roof areas) and parking areas. Conduct inspections at facilities and in the vicinity of soft targets.

(h) Measure 50. Coordinate with the Operations Division/Center to establish communications, responsibilities, and authorities before, during, and after attack.

(i) Measure 51. Request that local authorities close those public roads and facilities in the vicinity of the site/facilities that might facilitate execution of a malevolent or terrorist attack.

(j) Measure 52. Cancel public events.

(k) Measure 53. Execute Continuity of Operations plans.

(l) Measure 54. Reserve for site/facility use.

SECTION C—SITE SAFEGUARDS AND SECURITY PLANS

1. OBJECTIVE. The Site Safeguards and Security Plan (SSSP) is a risk management document that provides summary information used to describe safeguards and security (S&S) programs and vulnerability and risk assessments at applicable sites. The objective of this section is to delineate SSSP content and establish a standard approach to presenting site protection information and vulnerability assessment (VA) results. The results and conclusions contained in the plan are intended to guide long-term planning for site S&S operations. This is accomplished during plan development by identifying: key site protection elements; annually (at least every 12 months) evaluating site protection in terms of its adequacy to meet continued mission and threat parameters; and, identifying resource requirements.

2. APPLICATION. The SSSP is used to evaluate site and facility program elements and resources as they relate to identified threats and risks. The protection measures identified in approved SSSPs become the basis for executing and reviewing site protection programs.

3. SCOPE. The approved SSSP provides assurance that S&S measures address identified threats and risks. To provide this assurance, the plan must reiterate the assumptions identified to, and agreed upon, by line management. These assumptions must include reference to the contract under which the site is operated and those contractual issues that may impact S&S, applicable Department of Energy (DOE) directives, the threat upon which VAs are based, the methodology used to conduct VAs, deviations and proposed deviations, and any unique S&S impacting issues and assumptions that were addressed, and agreed to, by the responsible parties.

4. PURPOSE. The SSSP describes the graded protection of DOE assets required to be implemented by line management. The SSSP identifies site risks, cost-benefit analyses, and comparison of proposed upgrades. The resource plan (RP) must identify near- and long-term resource requirements needed to ensure the integrity of existing and planned S&S upgrades. The annual (at least every 12 months) review serves as the basis for tracking the implementation of protection measures and strategies necessary to maintain system effectiveness and identifies unfunded requirements.

5. PLAN COMPOSITION. The SSSP includes:

   a. references to implementing documents and evidence files;

   b. descriptions of site protection strategies, key site S&S programs, approved and pending deviations, plans and procedures designed to implement, manage and maintain S&S programs;

   c. system effectiveness determinations for the protection of special nuclear material (SNM), prevention or mitigation of sabotage events, and prevention and/or timely

detection of the loss of classified information or matter based on the status of performance indicators, such as results of VAs, performance tests, surveys, inspections, and evaluations of personnel qualifications and training;

d. proposed S&S program upgrades;

e. VAs results that support conclusions reported in the SSSP;

f. assumptions used as part of the VA process;

g. threat parameters used for VAs that are described in the current Design Basis Threat (DBT), regional threat assessments, and impacts made by local area threat assessments, if applicable;

h. the details of the changes in the protection through the spectrum of Security Conditions (SECON) (1-5), to include effects on the calculated baseline system effectiveness;

i. a description of the evidence files containing material that supports the VAs; and

j. an RP that describes S&S upgrades programmed for completion, upgrades being introduced as a result of planned and unplanned site changes impacting the protection program or deficiencies identified as a result of the annual (at least every 12 months) review of the SSSP, a description of the funding source to implement the upgrades, and unfunded requirements.

6. EVIDENCE FILES. Supporting documentation that validates data/information used in the VA process and in other protection program planning presented in the plan and that may require corroboration must be available in evidence files. Evidence files must be maintained to provide VA process and other protection program planning documentation in a logical and readily retrievable form to validate assumptions, modeling input data, test results, and other data that may be used to support protection system design or conclusions regarding protection effectiveness.

7. DATA COLLECTION. The effective date (snapshot in time) of the data contained in the SSSP must be specified.

8. FORMAT. Information provided in the SSSP should be brief, accurate, and concise. Implementing plans and procedures should be referenced in the plan where appropriate. A brief overview of a plan or procedure is adequate.

Duplication of information should be avoided. Information already included in other sections of the plan may be referenced or summarized for clarity.

A cover letter must be attached to the plan indicating that the plan has been reviewed, risks acknowledged and accepted (if appropriate), and signed by line management. For example, the SSSP should be approved by the Head of Field Element and submitted for

concurrence to the Departmental element. If high or marginal risk acceptance is needed, the correspondence must be routed for signature to the Secretary or Deputy Secretary or Under Secretaries, respectively.

The use of charts, plats, graphs, drawings, videos, photographs, and matrixes is encouraged wherever appropriate to clarify or satisfy the intent of plan objectives. References to sources of information and the location of supporting documentation should be provided to assist in verifying information contained in the plan.

The SSSP is divided into 12 chapters. Each chapter provides specific information relevant to site security. Use of this layout will ensure a uniform SSSP for review and comment or during an emergency.

a. Chapter 1, Site Description and Mission.

(1) Site Mission Statement. Describe the site mission and how the mission relates to national security and the health and safety of the public, employees, and the environment. Describe the major programs or activities performed at the site in terms of mission and their relationship to the DOE national security mission.

(2) Site Description and Area Layout. Describe the physical and geographical area in which the site and the S&S program are located. Provide a map, photograph, or drawing of the site that identifies locations of Category I facilities, facilities with a credible roll-up of SNM to a Category I quantity, the central alarm station (CAS) and secondary alarm stations (SAS), security-related communications facilities, and other facilities of security interest. Show the location of barriers defining the site Protected Area (PA). A small-scale map or drawing should be used to show the relationship of the site to the surrounding area and be of sufficient detail to orient the user.

(3) Management Organization, Planning Assumptions and Evidence File.

(a) Site Management Organizations. Identify the contract name, number, and other information that describes the authority under which the contractor executes management functions. Identify site contractors responsible for S&S programs and describe their S&S activities. Provide Federal and contractor organization charts and identify key positions and the relationships between the organizations for S&S activities. Provide a list of roles and responsibilities for key positions. Describe Federal and contractor involvement in the development of S&S resource requirements.

(b) Management and Planning Assumptions. Describe those assumptions that were addressed and agreed to during the SSSP scoping, preparation, or other SSSP management-related meetings.

Describe all relevant S&S-related planning assumptions that were formerly agreed to and included in a Memorandum of Agreement (MOA) by the responsible organization representatives who are party to the development and review of the SSSP. These assumptions should address the following issues:

1 site SECON;

2 VA methodology used for insider, neutralization, outsider, and collusion analyses;

3 identified credible targets;

4 protection strategies;

5 approved compensatory measures; and

6 performance testing conducted or to be conducted.

(c) Evidence Files. Describe and identify the contents, location, and control mechanisms for the SSSP evidence files. Reference approved standard operating procedures (SOPs) as applicable. Supporting documentation that validates data/information used in the VA process should not be included in the SSSP. However, this data/documentation should be available in a logical and readily retrievable arrangement in evidence files, for use in review and validation of the SSSP.

b. Chapter 2, Site Threat Description and Target Identification.

(1) Threat Description. Establish a graded approach to protection for Category I SNM and SNM facilities with credible roll-up of SNM to a Category I quantity, and facilities having radiological, biological, or chemical, sabotage event potential and facilities having disruption of critical mission sabotage event potential. Use the DBT as the baseline for threat determination, along with higher levels of threat dictated by local and regional threats (when available), and describe the site-specific threats used as the basis for conducting VAs and for which the protection program is designed.

(2) Target Identification. Identify, describe, and prioritize targets of security interest that meet the following criteria.

(a) Category I quantities of SNM and the facilities with credible roll-up of SNM to a Category I quantity.

(b) A radiological, biological or chemical sabotage inventory that, if released, would cause an unacceptable impact on national security or the health and safety of employees, the public, or the environment.

(c) Critical national security facilities, and assets (as defined in the DBT), designated by the Department (e.g., or each disruption of critical mission target) that would impact DOE programs supporting national defense and security.

(d) Those facilities possessing automated information systems that process or contain Sensitive Compartmented Information (SCI), Special Access Program (SAP), weapon data classified Secret Restricted Data (S/RD) Sigma 1, 2, 14 and 15 or higher.

(e) Temporary recurring targets. When predictable programmatic operations can reasonably be expected to present temporary SNM, sabotage, or information targets such as those permanent locations previously described, these targets must be described and analyzed at the same level of detail and in the same manner as permanent locations.

Provide a brief introductory description of the targets and a chart or list, such as shown below, that indicates the type of target, its location, attractiveness level, size, and configuration. Include SNM theft/diversion targets; radiological, biological, and chemical targets; and disruption of critical mission targets and those facilities possessing automated information systems that process SCI, SAP, weapon data classified S/RD Sigma 1, 2, 14, and 15 or higher.

(3) Theft or Diversion of SNM. Describe how Category I SNM targets and SNM facilities that roll-up to a credible Category I quantity have been identified and evaluated as potential abrupt theft targets. Also, describe how these SNM targets have been identified and assessed for protracted theft (diversion), if applicable.

For each identified SNM target, provide a description of the following, using a table similar to Table C-1, SNM Theft/Diversion Targets: physical location of identified SNM; the type of material, as described under the several material listings in DOE M 470.4-6, *Nuclear Material Control and Accountability*, such as pure products, high-grade material, weapons, including pits, ingots, oxide fuel elements, etc.; and the

Category (I through II) and attractiveness level (A through C) of the target material.

Table C-1. SNM Theft/Diversion Targets

Location	SNM Type	Category/ Attractiveness Level	Goal Quantity/ Portability
Bldg. 1, Vault	Pu-239 ingots	Cat. I/B	2 ingots/ man portable
Bldg. 1, Assay Room	Pu-239 ingots	Cat. I/B	2 ingots/ man portable
Bldg. 1, Fabrication Room	Pu-238 oxide powder	Cat. II/D	2 canisters/ man portable
Bldg. 2	U-235 fuel elements	Cat. II, roll-up to Cat. I/C	20 fuel element/ not man portable
Bldg. 3	U-235 fuel elements	Cat. II, roll-up to Cat. I/C	20 fuel element/ not man portable

(4) Radiological Sabotage. Indicate the process or methodology used to identify and evaluate radiological sabotage targets.

For each identified radiological sabotage target, provide a description using a table similar to Table C-2, Radiological Sabotage Targets, of the following: the physical location of all identified targets; the type of material; the maximum inventory level; and the material size and configuration.

Table C-2. Radiological Sabotage Targets

Location	Material Type	Maximum Inventory	Material Size and Configuration
Bldg. 1, Fabrication Room	Pu-238 oxide powder	10 kg	Paint Cans, at 50 g each
Bldg. 4	H_3 gas	10 kg	Cylinders, at 500 g each

(5) Biological or Chemical Sabotage. Describe the methodology used to evaluate biological or chemical targets. Using the criteria referenced in the DBT, determine the sabotage threat level (STL) for each location. Reference the plans and procedures that govern the biological or chemical sabotage assessment program.

For each identified target type not addressed by the commercial equivalency protection program, provide a description of the following using a table similar to Table C-3, Biological/Chemical Sabotage Targets: the physical location of additional identified biological or chemical sabotage material targets; the type of material; the maximum inventory level; the material size and configuration; and, the exposure level at the near-site boundary (NSB) for maximum inventory release.

Table C-3. Biological/Chemical Sabotage Targets

Location	Material Type	Maximum Inventory	Material Size and Configuration	Exposure Level at NSB
Bldg. 5	Chlorine	10,000 lb	55-gal drums, at 350 lb each	>ERPG III Levels

(6) Disruption of Critical Mission Sabotage. Describe how potential disruption of critical mission sabotage production and process components (machinery, equipment, flow process, power sources, ventilation, waste handling, etc.) have been identified and evaluated for inclusion as disruption of critical mission targets. Ensure that the evaluation includes how the sabotage event would affect production (at the facility, on intersite processes, and on overall national level inventory needs) and, if so, what areas, processes, and/or components within the facility affect those necessary production level capabilities and inventory needs.

For each disruption of critical mission target, provide a description, using a chart similar to Table C-4, Disruption of Critical Mission Targets, of the following: the physical location of essential production components; the type of equipment, process, power sources, or vital components; and the dollar value or production capability loss.

Table C-4. Disruption of Critical Mission Targets

Location	Equipment Type	Loss of DOE Mission Capability and Mission Impact
Bldg. 1, Fabrication Room	Fuel Fabrication Presses	100 percent loss of capability for 360 days with moderate mission impact
Lab. A	Laser Tunnel	100 percent loss of capability for 360 days with low mission impact

(7) Intra-Site Transportation of SNM. Describe, in a brief narrative, the Category I SNM targets and credible Category II SNM targets that roll up

to Category I quantity that are moved from one location to another on the site on a recurring basis.

Using a chart, identify the type of SNM, attractiveness level, and size and configuration of the material.

c. Chapter 3, Site Protection Strategies. Identify the protection strategies employed that address the overall protection program and enhance the concept of graded protection. Describe the protection program strategies employed. The basic strategies pertaining to protection are denial of access, denial of task, and containment that upon failure could evolve into recapture/recovery or pursuit strategies. Protection programs and tactical deployments designed to prevent unauthorized control of material and devices and to prevent acts of radiological, biological, chemical, and disruption of critical mission must be integrated with protection strategies. These activities could include protection layers of intrusion detection systems (IDS) and concentric security areas, access control measures, compartmentalization, insider protection programs, and procedural measures. The plan should clearly convey the strategy to be employed, and plan reviewers will anticipate that procedures are available to ensure implementation of these strategies. Display in a chart similar to Table C-5, Site-Wide Protection Strategies, the protection strategy used, the facility and target involved, and the title and responsible office for each plan or procedure. Ensure the information provided is consistent with that found in Chapter 2, Site Threat Description and Target Identification.

Table C-5. Site-Wide Protection Strategies

Protection Strategy	Facility or Activity	Target Type	Implementing Plan or Procedure	Responsible Office
Denial of Access	Facility ABC	Cat. I: Pu metal oxide Cat. II: nitrate UF_6	Plan ABC 1.3	Protective Force Manager
Containment	Vault storage Areas 301, 302, and 303	Weapon parts and Pu metallic buttons	Plan ADC.1	Protective Force Manager
Denial of Task	SNM in transit	Weapon parts	Plan CFE 1.5	Protective Force Manager

d. Chapter 4, Physical Protection Systems.

(1) Summary of Physical Protection Systems Used for Category I and Credible Roll-up Quantities of SNM to a Category I Quantity, Sabotage, Classified Information or Matter, and Classified Automated Information Protection. Describe the physical protection systems for each facility that has Category I quantities of SNM; credible roll-up quantities of SNM to a Category I quantity; radiological, biological, chemical and sabotage targets (including disruption of critical mission), and those facilities possessing automated information systems that process or contain SCI, SAP, weapon data classified S/RD Sigma 1, 2, 14 and 15, or higher. Provide a narrative description of the physical protection systems and how these systems are integrated at the site and facility level. Describe how physical protection systems (access control, intrusion detection, assessment, etc.) are implemented to allow the protective force (PF) to focus resources on its primary mission of defeating an armed terrorist threat. Describe how the barriers are protected by an IDS, security lighting, protective force (PF), and assessment systems and how structures located in or on the barrier are protected so as not to degrade protective systems. Describe the design of barrier systems used to deny vehicle approach routes to critical targets.

Following the narrative, complete a chart similar to Table C-6, Facility Protection Systems, that includes the following facility protection systems: security areas and their barriers, access controls (automated card access for both interior and exterior locations and contraband screening by the PF at protected and material access areas); assessment [closed circuit television (CCTV) and/or PFs both interior and exterior]; security computer system integrator/ processor; CAS and SAS; CCTV cameras monitoring and switching systems; security lighting; electrical and back-up power sources (emergency batteries and/or generators); and communications. In the chart, list the major physical protection systems, the location of the systems, and a brief description of the type of equipment installed.

(2) Physical Protection Measures for Category I and Credible Roll-Up Quantities of SNM to a Category I Quantity in Transit (Onsite). Describes the types, frequency, and protection measures used for the intra-site shipment of Category I SNM and credible roll-up quantities to a Category I quantity. Provide a narrative that describes the typical physical protection measures taken to ensure the integrity of those shipments from their point of loading, through transit, and at the off-load destination. If other materials are transported on site that would represent an STL 1 concern, provide a narrative that describes the typical physical protection measures from their point of loading, through transit, and at the off-load destination.

Vertical line denotes change.

Table C-6. Facility Protection Systems

Protection System	Equipment Description	Location	Responsible Office
Exterior Intrusion Detection	"H" Field	Protected Area Perimeter Associated Areas	Office of the Plant Engineer
Exterior Assessment/ CCTV	Microwave Taut Wire CCTV System	Protected Area Perimeter Associated Areas	Office of the Plant Engineer
Interior Intrusion Detection	Volumetric Infrared Motion Detectors	All Material Access Areas	Office of the Plant Engineer

e. Chapter 5, Site Protective Force.

(1) PF Mission, Organization, and Capabilities. Describe the PF organization and equipment deployed to perform 24-hour-per-day protection. Confirm that the basis for PF organization and planning is based on the identified site threat. Provide a narrative summary of the PF mission(s), capabilities, and deployment concepts used for site protection. Describe the methods used to review and prioritize post assignment priorities and eliminate posts that detract from combat readiness at high priority sites. Indicate the availability of plans and procedures that address normal and emergency deployment. Describe the PF equipment used including firearms, communications, vehicles, and any special items. Provide an organization chart of the PF, including response forces, showing the management and organization structure and key organizational interface positions with the cognizant security authorities and site operations and safety organizations. Using a schematic, display the PF communications network and include available secure networks and linkages to offsite law enforcement organizations with whom support agreements exist. In a chart, show the weapons and special equipment assigned to PF personnel, including members of the response force.

(2) Qualifications and Training. Indicate that the qualifications for hire and training of the PF conform to current policy requirements. In a chart similar to Table C-7, Qualifications and Training, list the titles and offices responsible for implementing and maintaining the plans or procedures that describe the following pertaining to the PF: qualifications for employment and the hiring process; initial, specialized and advanced training; tactical performance testing program; and other relevant written documentation, such as post and general orders that enhance the efficiency and effectiveness of the PF.

Vertical line denotes change.

Table C-7. Qualifications and Training

Plan/Procedures Title	Responsible Office
Specialized Training Plan	Training Department
Tactical Response Plans	Department

(3) Special Response Teams (SRTs) and Plans. Ensure the availability of SRTs and current response plans and procedures for implementing site-specific S&S program strategies and tactics for denial of access, denial of task, containment, recapture/recovery, pursuit, and contingency operations, as described in current DOE policy. Indicate that requalification training and exercises are used to verify the effectiveness of SRTs. Identify and document agreements and MOUs with local, State, and Federal law enforcement agencies regarding requests for on-site support during a contingency event. Ensure that a VA was used to assist management in determining the equipment and deployment of SRTs. In a brief narrative, confirm the availability of personnel and response plans and procedures that provide assurance of adequate protection. Indicate that contingency plans and procedures are available to respond to the activities listed below.

(a) Containment/denial of access/denial of task (includes a range of tactical options designed to either preclude adversary force access to nuclear weapons/materials or to deny unauthorized removal).

(b) Recapture/recovery or pursuit operations (used when containment/ denial fail and could involve SRTs and other force options including the use of off-site law enforcement agencies).

Describe the organization, equipment, and training provided to SRTs and how training and performance testing are used to verify the effectiveness of SRT planning in the strategies described above. Describe the role of VA in determining SRT deployment, equipment, and training.

In a chart similar to Table C-7, list tactical response plans and procedures and the office responsible for implementing and maintaining them.

Use a similar chart to list memoranda or letters of understanding and other agreements with local, State, or Federal law enforcement agencies regarding requests for onsite support during a contingency event.

f. Chapter 6, MC&A Program.

Describe the MC&A management program and summarize the results of the MC&A VA and other MC&A program planning activities. Describe the mission

of the site MC&A organization. Summarize current and planned nuclear materials processing and storage activities. Using an organization chart, show the MC&A organization and management structure and the lines of authority and points of interface with other S&S programs, facility operations, and the cognizant security authorities' MC&A organization. Describe the functions and responsibilities of safeguards personnel and indicate how MC&A activities are integrated with those of site protection programs and other facility organizations; include organizational responsibilities for those program elements that support multiple S&S programs (e.g., portal monitors and access controls). Confirm that MC&A personnel complete required training.

List, in a chart similar to Table C-8, MC&A Plans and Procedures, the facilities required to develop and maintain MC&A plans and procedures, the titles of those plans and procedures, and the office(s) responsible for approving and maintaining them.

Table C-8. MC&A Plans and Procedures

Facility Name	Plan/Procedure Title	Responsible Office(s)
ABC Facility	ABC Facility MC&A Plan, 1/1/99	S&S Director
XYZ Facility	XYZ Facility MC&A Plan, 6/9/99	S&S Director

Give the name(s) and date(s) of reports of MC&A VAs and other planning exercises. Summarize the results of these assessment(s). Identify those components of the MC&A system that provide the greatest effectiveness against theft and diversion. Describe actions taken to remediate identified program deficiencies or to prepare for planned changes in facility nuclear materials processing and storage activities.

g. Chapter 7, Site Personnel Security and Human Reliability Programs. Describes the site-wide program for personnel security that, in conjunction with information and physical security programs, ensures only authorized access to classified information or matter, or SNM and confirms that the personnel security program is in conformance with and implements the requirements prescribed in current DOE policy. Describe the key elements of the site-wide personnel security program for access authorizations and, if applicable, the key elements of the site's Human Reliability Program (HRP). Describe the method(s) used at the site to ensure the appropriate level of access authorizations are issued for the category of material processed or stored at the site and for approving justification, processing, and reevaluating the need for such access authorizations. Indicate how the effectiveness of the program is assessed. Indicate the site procedures that require

contractors to perform pre-hire checks to ensure proper qualifications and suitability of the applicant before submitting requests for access authorizations. Briefly describe the programs used to mitigate the effectiveness of potential "insider" activities and the application of these programs in addressing insider concerns. Provide an organization chart showing the location of the personnel security organization in relationship to the cognizant security authority and other contractor S&S organizations. Provide an organization chart identifying the designated HRP management official in relationship to the cognizant security authority and the designated HRP certifying official. Verify that the site has a current HRP implementation plan. List, in a chart similar to Table C-9, Personnel Security/Human Reliability Program Implementation, the titles of site-wide personnel security-related plans and procedures, the HRP implementation plan, if applicable, and the office(s) responsible for implementing and maintaining them.

Table C-9. Personnel Security/Human Reliability Program Implementation

Plan/Procedure Title	Responsible Office
XYZ Implementation Plan	Security Department

h. Chapter 8, Automated Information Security Program. Briefly describe the automated information systems for those facilities possessing automated information systems that process SCI, SAP, weapon data classified S/RD Sigma 1, 2, 14, and 15 or higher. Provide an organization chart showing the responsible automated information systems security program and its relationship to the cognizant security authority and contractor organizations.

In a chart similar to Table C-10, list the title of the automated information systems security program plans and procedures with the associated office responsible for implementing and maintaining the plan and procedures, the plans and procedures governing the automated information system VAs with the associated office responsible for implementing and maintaining the plan and procedures, and the reports containing the results of the VAs.

Table C-10. Automated Information Systems Security Programs

Plan/Procedure/Report Title	Responsible Office	Date (if pertinent)

i. Chapter 9, S&S Equipment Maintenance and Testing Programs. Describe maintenance and testing programs and life cycle planning, designed to enhance the continuous operability of S&S-related equipment used in the protection of Category I SNM (including areas with credible roll up of SNM to a Category I quantity), and classified automated information systems. Summarize in a narrative the maintenance and testing programs in use that ensure the availability and operability of S&S-related equipment and systems. Indicate the availability of compensatory measures/procedures that are used when equipment is taken out of service or otherwise not available. Describe how S&S maintenance and testing programs are incorporated into the Performance Assurance Program Plans. Indicate how the performance testing and other S&S site and facility maintenance programs comply with DOE policy.

Describe the life cycle planning conducted for major S&S equipment and component replacement. Relate how this planning is used to support and validate S&S equipment budget requirements.

In a chart similar to Table C-11, list the maintenance, testing, and records management programs; the relevant plans and procedures that implement the programs; and the responsible office, as these programs apply to equipment used by the PF, security related systems, and equipment and instrumentation used for MC&A. Many of these may be addressed in a single maintenance and testing program.

Describe the records management program used for scheduling, recording, and tracking identified S&S maintenance requirements, deficiencies, and testing schedules.

j. Chapter 10, Site Protection Evaluation Program. Chapter 10 is designed to ensure the availability and use of testing and evaluation programs for site S&S programs and systems.

In a narrative, describe the programs available and used to evaluate the effectiveness of S&S protection programs and the interaction of these evaluation tools (i.e., surveys may focus on shortfalls found in security inspections). Include in this narrative an outline of the PF tactical performance testing program describing the evaluation mechanisms used by line management. At a minimum, the programs described in Chapters 4, 5, 6, and 8 of the SSSP should be addressed and the evaluation plan or procedure identified. In a chart similar to Table C-12, Site Protection Program Evaluation Program, list the names of the evaluation plans/procedures used by the cognizant security authority to assist in determining the effectiveness of site and facility protection programs and systems. List the office responsible for the evaluation plan/procedure and its purpose.

Vertical line denotes change.

Indicate, in a brief description, that performance testing is used to verify the effectiveness of S&S systems/programs and to validate VA activities. Additionally, briefly describe barriers and other systems that cannot be adequately performance tested to demonstrate protection capabilities and their integration into protection strategies due to physical, operational, or policy parameters.

k. Chapter 11, Deviations from DOE Directives. List all deviations that have been approved. In a table similar to Table C-13, Deviations from DOE Directives, list the deviation, the officially assigned deviation number, the directive reference (DOE directive and section within the directive), and the dates the deviation was approved and expires.

Provide similar information for those deviations pending approval. This information should be displayed in a chart similar to Table C-14, Pending Deviations from DOE Directives.

l. Chapter 12, Summary of VA and Risk Assessment Results.

(1) Executive Summary. Summarize the VA and risk assessments results for Category I SNM, Category II SNM (including credible roll up of SNM to a Category I quantity), theft targets, radiological, biological, and chemical sabotage targets, and disruption of critical missions.

Confirm in the narrative that performance testing was used to validate VA input data and the results of the VA. Following the narrative, complete a matrix similar to Table C-15, Summary of Identified Risks, which identifies the risk associated with the results of the VA. In part 10 of the matrix, summarize the proposed corrective actions or upgrades. For line item construction project (LICP) work or other major capital expenditures, cite the source of the required funding. Use the RP information as the basis for this summary.

(2) Scope. Describe the targets to be covered, the items/issues to be excluded, and the limits on the conduct of the VAs in this SSSP.

(3) Methodology.

(a) Theft or Diversion of SNM. Identify the SNM targets subject to theft and/or diversion. Describe the rationale and mechanism used to identify these targets.

Using a table similar to Table C-16, SNM Theft/Diversion Targets, provide a description for each identified SNM target consisting of the following: the physical location of identified SNM; the type of material (such as pure products, high grade material, weapons,

etc.) which could include pits, ingots, oxide fuel elements, etc.; the Category (I through II) and attractiveness level (A through E) of the target material; and the size and portability of the theft target.

Table C-11. S&S-Related Maintenance, Testing, and Records Management Programs

Program Area	Plan/Procedure Title	Test Plan or Management Plan	Responsible Office/Organization
PF - Equipment - Training Courses - Firearms Qualification - Other			
Vehicles/Aircraft			
Communications			
MC&A			
Security Systems - Personnel Access and Inspection Equipment - Security Lighting - Intrusion Detection and Assessment Systems - Electrical Power Supplies			
Sensitive Area Access Control			
Survey/Inspection Deficiencies			

Table C-12. Site Protection Program Evaluation Program

Plan/Procedure Name Or Title	Responsible Office	Plan or Procedure Goal/Purpose
Performance Assurance Program	Contractor Manager	Establish/confirm system effectiveness
DOE/Contractor Self-Assessment Program	Program Manager	Identify program strengths/weaknesses
Facility Approval, Security Surveys	Cognizant Security Authority	Confirm availability and adequacy of required S&S programs
Force on Force Exercises	Contractor Manager	Confirm system effectiveness
Limited Scope Performance Tests	Contractor Manager	Confirm system effectiveness
Joint Tactical Simulation Model	Contractor Manager	Confirm system effectiveness

Table C-13. Deviations from DOE Directives

Deviation Description	Deviation Number	Directive Reference	Approval and Expiration Dates

Table C-14. Pending Deviations from DOE Directives

Deviation Description	Deviation Number	Directive Reference	Approval And Expiration Dates

(b) Radiological Sabotage. Identify the radiological targets subject to sabotage. Describe the rationale and mechanism used to identify these targets. A key source of information to assist in the identification and/or elimination of radiological targets is the facility safety analysis report.

Using a table similar to Table C-17, Credible Radiological Sabotage Targets, provide a description for each identified radiological sabotage target consisting of the following: the physical location of all identified targets, the type of material, the maximum inventory level, and the material size and configuration.

(c) Biological Sabotage. Identify the biological targets subject to sabotage. Describe the rationale and mechanism used to identify these targets. Reference any policy and analyses external to the SSSP that address biological targets.

Using a table similar to Table C-18, Credible Biological Sabotage Targets, provide a description for each identified biological sabotage target consisting of the following: the physical location of all identified targets, the type of material, the maximum inventory level, and the material size and configuration.

(d) Chemical Sabotage. Identify the chemical targets subject to sabotage. Describe the rationale and mechanism used to identify these targets. Indicate whether security protection provided for chemical sabotage targets is comparable to that provided by the

commercial sector for similar materials. A key source of information to assist in the identification and/or elimination of chemical targets is the facility safety analysis report. Reference any policy and analyses external to the SSSP that address chemical targets.

Using a table similar to Table C-19, Credible Chemical Sabotage Targets, provide a description for each identified chemical sabotage target consisting of the following: the physical location of all identified chemical sabotage targets, the type of material, the maximum inventory level, how the security provided is not comparable to that of the commercial sector, the material size and configuration, and the exposure level at the NSB for maximum inventory release.

(e) Disruption of Critical Mission. Identify the disruption of critical mission targets. Describe the rationale and mechanism used to identify these targets. Ensure that the evaluation includes how the disruption would cause an unacceptable impact on national security.

Using a table similar to Table C-20, Disruption of Critical Mission Targets, provide a description for each identified target consisting of the following: the physical location of the target, a description of the function of the target, the impact to national security, and the estimated time for recovery.

(f) VA Parameters and Planning Assumptions. Describe/list the baseline parameters and planning assumptions used in conducting the VAs. Provide a summary list of parameters and planning assumptions used in completing VAs. These should include assumptions discussed and concurred in by appropriate DOE offices or planning assumptions identified as a result of data collection/discovery during the VA process.

Table C-15. Summary of Identified Risks

Target Number	Target Location and Description	Threat Type and Number		Risk Rating (High, Moderate, Low)						Remarks	Analyses Validated by Perf. Testing
				Base Case	Current Modif. Rating (date)	Protected Action and Adjusted Rating: Near-Term (<2 yr) (date)		Protected Action and Adjusted Rating: Long-Term (>2 yr) (date)			
(1)	(2)	(3)		(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)
SNM Theft Targets											
1	Glovebox 112-A Bldg. 222	Terrorist, X outsiders with help of insider	High	High	Relocate SI to access door	Mod	Harden access portal	Low		Install hardware to allow SL relocation (FY-89 GPP)	Yes
2	Test samples in NDA room, Bldg. 222	Criminal Insiders	High	High	Enhance HRP for NDA technicians and supervisors	High	Install CCTV recording for post-review of activities in NDA room	Mod		SNM protection unchanged, but probability of attempt reduced thru HRP and delayed assessment capability	Yes
Radiological Sabotage Targets											
3	Test reactor #5 North Area, Bldg. 408	Insider	Mod	Mod	Reinforce SI number when in use	Low	None	Low		Use overtime when reactor in use-3 times per year	No
Chemical Sabotage Targets											
4	Laboratory Bldg. 4	Insider	Mod	Mod	None	Low	None	Low		None	No
Biological Sabotage Targets											
5	Fabrication Room, Bldg. 1	Insider	Mod	Mod	None	Low	None	Low		None	No
Disruption of Critical Mission Targets											
6	Access port 4 D-line process line, Bldg. 460	Disgruntled employee	High	Mod	Implement 2-man rule	Low	Harden and remote control of portal	Low		Install hardware to reduce high manpower costs (use FY-92 GPP)	Yes
7	Extrusion equipment in fuel manufacturing area, Bldg. 97	Psychotic employee	High	High	Establish spares inventory for long lead time parts	Mod	Identify alternate extrusion capability off-site	Low		Additional physical protection not cost-effective. Improved spares also provide repair capability for non-sabotage outages	Yes

Table C-16. SNM Theft/Diversion Targets

Location	SNM Type	Category/ Attractiveness Level	Quantity/ Portability
Bldg. 1, Vault	Pu-239 ingots	Cat. I,/B	2 ingots/man portable
Bldg. 1, Assay Room	Pu-239 ingots	Cat. I,/B	2 ingots/man portable
Bldg. 1, Fabrication Room	Pu-238 oxide powder	Cat. II/D	2 canisters/man portable
Bldg. 2	U-235 fuel elements	Cat. II, roll-up to Cat. I/ C	20 fuel elements/not man portable
Bldg. 3	U-235 fuel elements	Cat. II, roll-up to Cat. I/ C	20 fuel elements/not man portable

Table C-17. Credible Radiological Sabotage Targets

Location	Material Type	Maximum Inventory	Material Size and Configuration
Bldg. 1, Fabrication Room	Pu-238 oxide powder	10 kg	Paint Cans, at 50 g each
Bldg. 4	H_3 gas	10 kg	Cylinders, at 500 g each

Table C-18. Credible Biological Sabotage Targets

Location	Material Type	Maximum Inventory	Material Size and Configuration
Bldg. 1, Fabrication Room	Anthrax solution	10 g	20 petri dish at 0.5 g each
Bldg. 4	Botulism aerosol	20 g	10 2-liter cylinders, at 5 kg each

Table C-19. Credible Chemical Sabotage Targets

Location	Material Type	Maximum Inventory	Commercial Sector Security Difference	Material Size & Configuration	Exposure Level at NSB
Bldg. 5	Chlorine	10,000 lb	Lack of access control	55-gallon drums, at 350 lb each	>ERPG III levels

Table C-20. Disruption of Critical Mission Targets

Location	Target Function	Impact to National Security	Estimated time for Recovery
Site A, Bldg. 4	Fuel cell production	Increased reliance on fossil fuels	180 days

(g) Critical Path Protection Elements. Describe the process used to identify critical path protection elements and the types of tests to which site protection elements are subjected (procedural, simulation, barrier, equipment, PF, etc.). Using a table similar to Table C-21, Performance Testing Results of Site Specific Essential Protection Element Values, provide a list of: physical security system components for each protection layer [Limited Area (LA), PA, material access area (MAA), and Target Area], the critical protection element tested, if any, as determined from performance testing. Also, indicate the number of tests conducted to obtain results and the testing frequency used to monitor the protection element specific value.

(h) Single Point Failure Analysis. Describe the analyses used to determine any single-point failures identified during the VA. Describe/list the single-point failure(s) to include the nature of the vulnerability, measures to mitigate the vulnerability and the potential exploitability by an adversary.

(i) Critical Path Scenarios. Describe and provide the critical path scenarios, including the bounding scenarios, developed during the VA for each target. Identify the protection system effectiveness (P_E) value for each of these targets. Describe and identify the critical detection points along each adversary path.

Should multiple targets exist within the same security area, such as several SNM targets within the same MAA and same building, bounding critical path scenarios may be described. Provide justification that supports bounding cases.

For each critical path scenario provide floor plans, diagrams, sketches, or an adversary path description (as shown in Table C-22) or, if appropriate, refer to the descriptions that may have been used previously to illustrate the critical path and protection elements described in the scenarios.

Identify and describe the point along the adversary path at which detection is required to allow for sufficient response time for adversary neutralization to be effected for each of the critical path scenarios (i.e., critical detection point).

Table C-21. Performance Testing Results of Site-Specific Essential Protection Element Values

Protection Layer and Physical Security System Components Tested	Critical Elements Tested	No. of Tests Used as Basis for VA values	Test Frequency	Value used in VA
PA - Identification and Intrusion Element	Attempt to smuggle firearms through Portal 1.	36	Quarterly	0.6
	Attempt to defeat door contacts Bldg. 1, door 3.	34	Quarterly	0.7
MAA - Search Component	Attempt to smuggle firearms through MAA portal	24	Once every 2 months	0.8
Target Area - Identification Component	Attempt to gain unauthorized vault access	48	Monthly	0.9

(j) Protection System Effectiveness. Verify that the P_E values identified for each critical path scenario were used to calculate conditional risk for each identified target. Using tables similar to those on the following pages (Table C-23, Protection Effectiveness P_E for Theft or Diversion of SNM; Table C-24, Protection Effectiveness (P_E) for Radiological Sabotage; Table C-25, Protection Effectiveness (P_E) for Biological Sabotage; Table C-26, Protection Effectiveness (P_E) for Chemical Sabotage; Table C-27, Protection Effectiveness (P_E) for Disruption of Critical Missions; Table C-28, Protection Effectiveness (P_E) for Theft or Espionage of Classified Information or Matter; and Table C-29, Protection Effectiveness (P_E) for Other Losses), show the targets and P_E values for each target.

(k) Neutralization Analyses. Identify and describe the mechanism(s) used to determine/calculate the neutralization value(s) used in the risk evaluation. Identify and describe the basis for the neutralization values, parameters that impact the neutralization calculations and any site-specific issues that modify neutralization calculations.

(l) Insider Analysis. Describe the analysis for determining the insider threat for each target class included in the SSSP. This analysis must include the programs supporting the elimination/mitigation of select insider groups from the threat spectrum, identification of the potential insider population, and insider protection programs that

were not included in other protection system elements. Describe the programs that are factored into the VA process and provide justification for their use. Identify by position and title the participants in the HRP.

(m) Conclusions. Provide a summary of system effectiveness for the identified targets. Document VA analyst's observations and recommendations developed as a result of the VA process. Summarize the system effectiveness using a table similar to C-30, System Effectiveness Summary.

Table C-22. Critical Path Scenarios

Scenario Title:	Base Case 1	Results	
Facility:	Building XYZ	P_I	.
Target Location:	Room,123 State, Open	P_N	
Adversary Threat/Adversary:	Terrorist w/insider: X# outsider, Y# insiders		
Goal Type/Quantity:	Oxide, Xx kg	P_E	
VA Path Analysis Tool:	ASSESS	C	
Computer File ID:	.PPS, .OUT; .NEU	Syst. Eff.:	
Neutralization Tool:	JTS	Syst. Eff.:	

Time (Sec)			SCENARIO ACTIONS
Total	ADV	PF	
			Adversary pre-positions escape vehicles
			Adversary mails weapons and explosives into PA (No x-ray or explosives detection capability)
			Adversary proceeds to access control portal
0	20		Adversary attempt to deceit through portal (P_D = 0.xx – badge check with xxxx at access portal). If detected, adversary begins overt actions. CRITICAL DETECTION POINT
		25	CAS receives alert and begins to annunciate alert
20	25		Adversary proceeds to target building XYZ, door 7 on the NE corner
25			Protective Force units begin response
		70	Unit A responds to NE corner of building XYZ
		55	Unit B responds to SE corner of building XYZ
		80	Unit C responds to SE corner of building XYZ
		60	Unit D responds to SE corner of building XYZ
45	5		Adversary reaches door 7 to building XYZ, insider opens door 7 into building XYZ (P_D = 0.xx – BMS)
50	5		Adversaries enter building XYZ and transverse to vault room 123. CAS receives BMS door alarm and annunciates the alarm
55	50		Adversaries collect target material
80			Unit B reaches response position
85			Unit D reaches response position
95			Unit A reaches response position
105	5		Adversaries proceed to door 7 to exit building XYZ. Unit C reaches response position.
110			Adversary exits building XYZ via door 7. (P_D = xxx - ,)
112			Unit A engages adversary
			Etc.

Table C-23. Protection Effectiveness (P_E) for Theft or Diversion of SNM

Location	Material Type	Facility Condition	Adversary Type	Adversary Scenario Summary	Protective Force Response Summary	P_E Value
Bldg. 1, Vault	Pu-239 ingots	Open	Terrorist	Vault open. Outsiders deceit into PA. Insider crashes out of Bldg. 1 MAA with material. Hands off to outsiders. Adversaries leave PA/site by vehicle.	Armed response to BMS door alarm. Containment at MAA boundary. Positioning of blocking forces at PA boundary if MAA containment defeated. Pursuit in PPA if escape from facility.	.7
Bldg. 1, Assay Room	Pu-239 ingots	Open	Terrorist	Scenario same as vault open scenario.	Scenario same as vault open scenario.	.7
Bldg. 1, Fabrication Room	Pu-238 oxide powder	Open	Terrorist	Scenario same as vault open scenario.	Scenario same as vault open scenario.	.7

Table C-24. Protection Effectiveness (P_E) for Radiological Sabotage

Location	Material Type	Facility Condition	Adversary Type	Adversary Scenario Summary	Protective Force Response Summary	P_E Value
Bldg. 1, Fabrication Room	Pu-238 oxide powder	Open	Terrorist	Building open. Outsiders deceit into PA. Outsiders force MAA boundary by foot. Insider allows access into Bldg. 1 Outsiders enter fabrication room, obtain Pu-238 oxide, defeat HEPA filters, and vent material to environment through building ventilation.	Armed response to MAA boundary alarm.	.4
Bldg. 4	H_3 gas	Open	Terrorist	Building open. Outsiders deceit into PA. Outsiders force MAA boundary by foot. Insider allows access into Bldg. 4. Outsiders disperse H_3 to the environment with explosives.	Armed response to MAA boundary alarm.	.4

Table C-25. Protection Effectiveness (P_E) for Biological Sabotage

Location	Material Type	Facility Condition	Adversary Type	Adversary Scenario Summary	Protective Force Response Summary	P_E Value
Bldg. 5	Anthrax	Open	Terrorist	Building open. Outsiders deceit into PA. Insider allows access into Bldg. 5. Outsiders disperse anthrax to the environment with explosives.	Building Containment	.2
		Closed	Terrorist	Outsiders deceit into PA. Outsiders breach door into Bldg. 5. Outsiders disperse anthrax to the environment with explosives.	Building Containment	.2

Table C-26. Protection Effectiveness (P_E) for Chemical Sabotage

Location	Material Type	Facility Condition	Adversary Type	Adversary Scenario Summary	Protective Force Response Summary	P_E Value
Bldg. 5	Chlorine	Open	Terrorist	Building open. Outsiders deceit into PA. Insider allows access into Bldg. 5. Outsiders disperse chlorine to the environment with explosives.	Building Containment	.2
		Closed	Terrorist	Outsiders deceit into PA. Outsiders breach door into Bldg. 5. Outsiders disperse chlorine to the environment with explosives.	Building Containment	.2

Table C-27. Protection Effectiveness (P_E) for Disruption of Critical Missions

Location	Equipment Type	Facility Condition	Adversary Type	Adversary Scenario Summary	Protective Force Response Summary	P_E Value
Bldg. 1, Fabrication Room	Fuel Fabrication	Open	Nonviolent Insider	Insider enters Fab. Room. Starts fire to destroy equipment located in room.	Building Containment	.2

Table C-28. Protection Effectiveness (P_E) for Theft or Espionage of Classified Information or Matter

Location	Classified Information or Matter	Facility Condition	Adversary Type	Worst-case Scenario Summary	Protective Force Response Summary	P_E Value
Bldg. 5, Office Area	TSRD Documents	Open	Nonviolent Insider	Insider obtains TSRD, makes copies, encloses copies in envelope, and hand-carries out of Bldg. 5. Insider mails classified documents out of PA to off-site location.	None	.2

Table C-29. Protection Effectiveness (P_E) for Other Losses

Location	Item	Facility Condition	Adversary Type	Worst-case Scenario Summary	Protective Force Response Summary	P_E Value
Bldg. 5, Lab Area	R&D Laboratory	Open	Nonviolent Insider	Insider starts fire in laboratory.	Building Containment	.2

Table C-30. System Effectiveness Summary

Goal	Target	Location	Operations	P_E
Theft of SNM	Bldg. 1	Vault	Day Shift	.8
Theft of SNM	Bldg. 1	Assay Room	Day Shift	.8
Theft of SNM	Bldg. 1	Fab. Room	Day Shift	.75
Rad. Sabotage	Bldg. 1	Fab. Room	Day Shift	.85
Rad. Sabotage	Bldg. 4	Bldg. 4	Day Shift	.9
Chem. Sabotage	Bldg. 5	Laboratory	Day Shift	.8
Bio. Sabotage	Bldg. 5	Laboratory	Day Shift	.8
Indust. Sabotage	Bldg. 1	Fab. Room	Day Shift	.8
Espionage of Classified	Bldg. 5	Office Area	Day Shift	.8
Other Losses	Bldg. 5	Laboratory	Day Shift	.8

SECTION D—SITE SAFEGUARDS AND SECURITY PLAN RESOURCE PLAN

1. OBJECTIVE. The Resource Plan (RP) identifies safeguards and security (S&S) resources necessary to ensure protection of Department assets and identifies changes in resource requirements (i.e., operational requirements, capital equipment, general plant projects (GPPs) and line item construction projects (LICPs) that directly impact risk, indirectly impact risk, or derive from changing S&S policy, directives, guidance, or other Department or other Departmental direction.

   a. Operational Requirements. Briefly describe operational requirements relating to S&S operations that would require increments or decrements to operational accounts (e.g., program direction, operational support, etc.). Operational requirements must include, but are not limited to, material consolidation, facility mission changes, changes in the Design Basis Threat (DBT) impacting site operations, protective force (PF) redeployments, maintenance and testing changes, PF manning levels, procuring technical expertise and support personnel, and additional training requirements. Summarize the pertinent information in a table such as outlined in Table D-1, Operational Requirements. The table and supporting narrative must include the following:

      (1) the title of each operational requirement;

      (2) the basis of the requirement (drivers behind the requirement);

      (3) the funding profile and the impacts if not funded (if possible, state the impact in terms of probability of system effectiveness (P_E) and indicate if this is a new resource requirement); and

      (4) provide a status of operational requirements that were previously authorized but have not yet been completed.

      Provide a separate section for each operational requirement.

Table D-1. Operational Requirements

Requirement (section)	Basis	Funding Request/Profile						Currently in Budget (Y or N)	Type of Expense
		FY xxxx (current year)	FY + 1	FY + 2	FY + 3	FY + 4	FY + 5		

b. Capital Equipment. Briefly describe identified/proposed capital equipment procurements and funding requirements that are not part of a LICP or GPP, and support S&S programs and operations. These procurements could include, but are not limited to, alarm and assessment system components, material control and accountability (MC&A) systems, access control system components, and equipment necessary to complete the S&S mission (e.g., breaching tools, vehicles, PF armaments, additional capabilities necessary to address changes in the DBT). Summarize the pertinent information in a table as outlined in Table D-2, Capital Equipment. The table and supporting narrative must include the following:

(1) a title for each capital equipment procurement;

(2) the basis of the requirement (drivers behind the requirement);

(3) the funding profile and the impacts if not funded (if possible, state the impact in terms P_E, and indicate if this is a new resource requirement); and

(4) a status of capital equipment upgrades that were previously authorized but have not yet been completed.

Provide a separate section for each capital equipment procurement.

Table D-2. Capital Equipment

Capital Equipment (section)	Basis	Funding Request/Profiles						Currently in Budget (Y or N)
		FY xxxx (current year)	FY + 1	FY + 2	FY + 3	FY + 4	FY + 5	

c. GPP. Describe significant identified/proposed GPPs that are not part of an LICP or capital equipment expense but that are necessary to support S&S programs and operations. These GPPs could include, but are not limited to, alarm and assessment systems/components, MC&A systems, access control systems/components, or infrastructure improvements. Summarize the pertinent information in a table as outlined in Table D-3, General Plan Projects. The table and supporting narrative must include:

(1) a title for each GPP;

(2) the basis of the requirement (drivers behind the requirement);

(3) the funding profile and the impacts if not funded (if possible, state the impact in terms P_E, and indicate if this is a new resource requirement);

(4) a status of general plan project upgrades that were previously authorized but have not yet been completed.

Provide a separate section for each GPP.

Table D-3. General Plant Projects

General Plant Projects (section)	Basis	Funding Request/Profiles						Currently in Budget (Y or N)
		FY xxxx (current year)	FY + 1	FY + 2	FY + 3	FY + 4	FY + 5	

d. LICPs. Describe current and proposed LICPs that are not part of a GPP or capital equipment procurement but are necessary to support S&S programs and operations. Summarize the pertinent information in a table as outlined in Table D-4, Line Item Construction Projects. The table and supporting narrative must include:

(1) a title for each LICP;

(2) the basis of the requirement (drivers behind the requirement);

(3) the funding profile and the impacts if not funded (if possible, state the impact in terms P_E, and indicate if this is a new resource requirement); and

(4) the status of S&S upgrades that were authorized but have not yet been completed. Discuss any changes to cost estimates [i.e., total estimated cost (TEC) versus total project cost (TPC)] identified in the previous RP.

Provide a separate section for each LICP.

Table D-4. Line Item Construction Projects

LICP Title (section)	Basis	Funding Request/Profiles						Total Costs		Schedule		Currently in Budget (Y or N)
		FY xxxx (current year)	FY + 1	FY + 2	FY + 3	FY + 4	FY + 5	TEC	TPC	Start Date	Finish Date	

Table D-5. Unfunded/Unsupported Requirements

Requirement (section)	Basis	Resource Type	Base FY	Original Funding Request/Profiles						Impact
				FY xxxx	FY + 1	FY + 2	FY + 3	FY + 4	FY + 5	

2. UNFUNDED/UNSUPPORTED REQUIREMENTS. Briefly describe proposed S&S operational requirements, capital equipment procurements, GPPs, or LICPs that had been previously identified and have not been funded supported. Summarize the pertinent information in a table such as Table D-5, Unfunded/Unsupported Requirements. The table and supporting narrative must include:

   a. a title for each unfunded requirement;

   b. the basis for the requirement (drivers behind the requirement);

   c. the type of resource requested (operating expense, capital equipment, GPP, or LICP);

   d. the fiscal year the requirement was originally identified;

   e. the proposed funding profile and impacts due to lack of funding (if possible, state the impact in terms of P_E).

   Provide a separate section for each unfunded requirement.

3. REFERENCES FOR THE RESOUCE PLAN.

   a. Facility SSSP. Provide a reference to the most recent/current SSSP.

   b. Programmatic Documentation. Provide a reference (include title, date, and responsible organization) for any programmatic policy, directive, or guidance necessitating the allocation of additional resources.

4. HEADINGS AND TERMS FOR TABLES D-1 THROUGH D-5. Following are the types of data to be included in the RP.

   a. Basis.

      (1) Compliance.

      (2) Risk reduction.

      (3) SSSP derived.

      (4) Cost-efficiency.

      (5) Operational efficiency.

      (6) Enhanced operations.

      (7) DBT change.

b. Type of expense.

(1) Operational = annual recurring cost that will need to be added to the budget baseline.

(2) Single = one time only expense paid from operating dollars.

c. Total Costs.[1]

(1) TEC = Total estimated cost.

(2) TPC = Total project cost.

d. Resource Type.

(1) OE = operational expense.

(2) CE = capital expense.

(3) GPP = general plant project.

(4) LICP = line item construction project.

(5) BASE FY = fiscal year in which the resources were identified and requested.

e. Impact.

(1) Continued risk.

(2) Cost escalation.

(3) Unable to comply with xxxx (list applicable directive).

(4) Programmatic impact.

(5) Operational impact.

(6) Other (list).

[1]As defined in DOE O 413.3, Chg 1, *Project Management for the Acquisition of Capital Assets.*

SECTION E—VULNERABILITY ASSESSMENT PROGRAM

1. OBJECTIVE. The Vulnerability Assessment (VA) Program must consider other programs such as protective force (PF), material control and accountability (MC&A), emergency operations, safety, maintenance, facility operations, personnel security, physical protection, and information security.

2. CONDUCTING VULNERABILITY ASSESSMENTS. The process of conducting a VA includes gathering data that describe the physical and operational characteristics of a safeguards and security (S&S) system, assigning values such as delay and detection, and analyzing the results to determine the relative effectiveness in conjunction with the adversary's capabilities as identified in the Design Basis Threat (DBT) and the Adversary Capabilities List (ACL). Below is a description of the VA process.

   a. Assumptions. Assumptions and scoping agreements must be defined. All assumptions must be documented in the VA report.

   b. Threat. The person responsible for the conduct of VAs, hereinafter referred to as the analyst (see paragraph 9 of this section), must understand how the DBT relates to VAs. The analyst performing the VA must apply DOE Headquarters (HQ), regional and local threat guidance.

      (1) DOE HQ Threat.

         (a) The DBT must be used to define threat against which VA analysts evaluate the protection system

         (b) The site's protective systems must be analyzed against the ACL.

      (2) Regional and local threats must be considered during the conduct of VAs.

   c. Targets. All security interests whose loss, theft, compromise, and/or unauthorized use will affect the national security and/or the health and safety of DOE and contractor employees, the public, the environment, or DOE programs are potential targets. The analyst must consider target configurations and conditions, as well as operational conditions and acquisition times.

   d. Modeling. Modeling is used to analyze S&S programs, interests, assets, and the effectiveness of program implementation. Modeling can include computer-based tools and simulations, table-top analyses, and subject matter expert analyses. Section E, Appendix 3, VA Modeling Tools, lists those modeling tools approved by DOE. Methods to ensure that the models accurately reflect the facility posture must be part of the final VA results. The modeling process must establish critical pathways. The following must be considered:

      (1) facility characterization;

Vertical line denotes change.

(2) System effectiveness models and equations must be used. Section E, Appendix 4, System Performance Effectiveness Equation, delineates the system effectiveness equation;

(3) response force times;

(4) the probability of neutralization (P_N) must be calculated using data available regarding the PF response and their ability to interrupt and neutralize an adversary. The methods used must be documented and retained as part of the evidence file. The calculated number for P_N must be derived from more than one source, one of which must be joint tactical simulation (JTS), joint conflict and tactical simulation (JCATS), or force-on-force (FoF) exercises;

(5) blast effect modeling must consider blast effects on barrier breaching, a force multiplier, and target buildings;

(6) table-top methods used to determine system effectiveness must be documented and a means provided to allow for validation or verification;

(7) radiological sabotage must be fully analyzed against the DBT and ACL. Existing information from safety analyses can be used but must be analyzed to consider deliberate rather than accidental release;

(8) chemical and biological sabotage must be analyzed against the DBT and ACL;

(9) the analysis must use the thresholds stated in DOE O 470.3, *Design Basis Threat (DBT) Policy*; and

(10) the use of chemical and biological agents must be analyzed as a force multiplier. Methods of release and mitigation measures must be a part of the analysis.

e. Performance Testing. If conducted, the results of the following tests (including validation) must be considered in determining system effectiveness:

(1) FoF exercises;

(2) limited scope performance tests (LSPTs);

(3) alarm response and assessment performance tests (ARAPTs);

(4) breaching test data; and

(5) critical system element tests.

Vertical line denotes change.

f. Results. The results of VAs indicate P_E. The VA results must be used for determining:

(1) protection system effectiveness reporting;

(2) S&S upgrades;

(3) manning/armament levels for the PF; and

(4) justifications for waivers of and exceptions to S&S policy.

g. VA Practitioner Training. VA practitioners must successfully complete VA Program training within 2 years of appointment. This requirement can be met through the National Training Center (NTC).

3. QUALITY ASSURANCE. The analyst must verify the data used for the analyses. These data include:

a. modeling data to include detection, assessment, delay, interruption, neutralization, PF response times, etc.;

b. all facility modeling characterization direct settings, rationales, and documentation;

c. performance test results and documentation; and

d. sensitivity analyses such as single point failure and critical system element analyses.

4. VULNERABILITY ASSESSMENT. All information used to support or document VAs must be maintained and made available upon request. Examples include:

a. modeling inputs;

b. PF response;

c. adversary capabilities;

d. blast effects;

e. sabotage data;

f. timeline data; and

g. neutralization data.

5. ASSIGNING FIGURES OF MERIT. "Figures of merit" is defined as numerical values and/or qualitative ratings assigned to component systems and personnel associated with

the protection system. Collectively the qualitative and/or quantitative measures provide the basis for determining system effectiveness. Approved reference materials must be used to provide initial data and to calculate accurate detection and delay numbers. A list of approved references is provided in DOE M 470.4-7, *Safeguards and Security Program References*. Reference materials are to be used only as a basis for the relative figures of merit. Non-default figures of merit must be documented and based on performance testing or engineering studies.

6. CRITICAL SYSTEM ELEMENTS. Critical system elements are components or subcomponents of an S&S protection system that directly affects the ability of the system to perform a required function. Critical system elements may be equipment, procedures, or personnel. Failure of a critical system element would result in the protection system effectiveness of the target being reduced to levels requiring management action. Critical system elements must be:

   a. identified for every target that requires a VA;

   b. specifically delineated such that specific performance tests can be performed to determine the ability of the protection measures to perform their intended function; and

   c. tested, documented, and the results analyzed to validate element effectiveness.

7. VULNERABILITY ASSESSMENT REPORTS. The vulnerability assessment report (VAR) documents the results of a VA. The VARs must include targets analyzed, methodology used, system effectiveness results, parameters and assumptions under which the VA was conducted, and reference to evidence files. VARs published in support of an SSSP should conform to the suggested format given in Section E, Appendix 5, Suggested VA Report Format. The approval chain for VARs is below.

   a. The analyst responsible for the VA must sign the report.

   b. Line management responsible for the facility/site VA Program must approve the report.

   c. DOE line management responsible for the VA Program must concur with the report.

   d. The DOE cognizant security authority must concur with the report.

8. SYSTEM EFFECTIVENESS. Only the Secretary of Energy or the Deputy Secretary can accept low protection system effectiveness that results in high risk. Cognizant Under Secretaries can accept marginal protection system effectiveness that results in moderate risk. If the results of a VA, survey, self-assessment, audit, or inspection conducted by the cognizant security authority, Departmental element, Office of Security, or Office of Independent Oversight and Performance Assurance indicate a decreased (low or

Vertical line denotes change.

marginal) protection system effectiveness that is not mitigated by compensatory measures based on a risk management determination (see Section A, paragraph 2e), the following actions must be initiated:

a. Low Protection System Effectiveness.

(1) Once a low protection system effectiveness condition that results in high risk is identified, that condition must be reported to the responsible Departmental element within 4 hours.

(2) A corrective action plan must be submitted to the responsible Departmental element within 8 hours, with a copy to the Office of Security.

(3) The Departmental element must make formal notification to the Secretary or Deputy Secretary within 24 hours.

(4) The Departmental element in consultation with the Office of Security must provide comments on the protection system effectiveness and recommendations to the Secretary/Deputy Secretary within 36 hours.

(5) The responsible Departmental element must update the Secretary or Deputy Secretary on low protection system effectiveness conditions every 30 days with an information copy to the Office of Security.

b. Marginal Protection System Effectiveness.

(1) Once a marginal protection system effectiveness condition that results in moderate risk is identified, that condition must be reported to the responsible Departmental element within 2 working days.

(2) The Departmental element must notify the appropriate Under Secretary within 3 working days.

(3) A corrective action plan with recommendations must be submitted to the responsible Departmental element within 5 working days with a copy to the Office of Security.

(4) The Office of Security must provide comments to the Departmental element within 5 working days.

(5) The responsible Departmental element must update the Secretary or Deputy Secretary and appropriate Under Secretary on marginal protection system effectiveness conditions every 90 days with an information copy to the Office of Security.

9. TRAINING AND CERTIFICATION.

a. The analyst responsible for the conduct of Vulnerability Assessments must complete the Department-approved training program (scheduled to be fully implemented by 2008).

b. The analyst must be certified as outlined in the *Vulnerability Assessment Certification* Program Manual which is currently under development.

c. Any person currently conducting VAs may be “grandfathered” until such time as the *Vulnerability Assessment Certification* Program Manual is issued.

SECTION E

APPENDIX 3—VULNERABILITY ASSESSMENT MODELING TOOLS

1. ASSESS—Analytic System and Software for Evaluating Safeguards and Security.
2. ATLAS—Adversary Time Line Analysis System.
3. BATLE—Brief Adversary Threat Loss Estimator.
4. JTS—Joint Tactical Simulation.
5. JCATS—Joint Conflict and Tactical Simulation.
6. AT Planner—Anti-Terrorist Planner.
7. BLAST X—Explosive Effects Analysis Software.
8. BLAST FX—Explosive Effects Analysis Software.
9. ConWEP—Conventional Weapons Effects Program.
10. BEEM—Blast Effects Estimation Model.
11. HOTSPOT—HOTSPOT Health Physics Code provides the capability to calculate the radiation effects associated with the short-term (less than 24 hours) atmospheric release of radioactive materials.
12. RSAC—Radiological Safety Analysis Computer program calculates the consequences of a release of radionuclides to the atmosphere.
13. ACATS—Airborne Chromatograph for Atmospheric Trace Species.
14. ISA—Iterative Site Analysis.
15. VISA—Vulnerability of Integrated Security Analysis.
16. VISA II—Vulnerability of Integrated Security Analysis II.
17. ERAD—Explosive Release Atmospheric Dispersion.
18. ALOHA—Area Locations of Hazardous Atmospheres.
19. ARAC—Atmospheric Release Advisory Capability.
20. ACCS 2—Accident Consequence Code System for the calculation of the health and economic consequences of accidental atmospheric radiological releases.
21. HPAC—Hazard Prediction Analysis Code provides the capability to accurately predict the effects of hazardous material releases into the atmosphere.

Vertical line denotes change.

SECTION E

APPENDIX 4—SYSTEM PERFORMANCE EFFECTIVENESS EQUATION

The methodology requires the determination of the probability of sensing, probability of assessment, and probability of detection at each layer. These are then combined to determine the contribution to overall system effectiveness represented by each layer. Mathematically, this can be expressed as the equation:

$$P_{EL} = P_{IL} \times P_{NL} = P_{DL} * P_{NL} = P_{AL} * P_{SL} * P_{NL}$$

Where:

P_{EL} is the system effectiveness contribution for layer L;

P_{IL} – Probability of Interruption given first detection at layer L, $P_{IL} = P_{DL}$ if detection on layer L is timely, and is equal to 0 ($P_{IL} = 0$) if detection is not timely;

P_{DL} – Probability of Detection at layer L, $P_{DL} = P_{SL} \times P_{AL}$ on layer L. P_{DL} is the probability of first detection at layer L, given that detection has not occurred at an earlier layer, multiplied by the probability of sensing at an earlier layer, multiplied by the probability of sensing at layer L (P_{SL}) and the probability of assessment at layer L (P_{AL});

P_{SL} – Probability of Sensing on layer L;

P_{AL} – Probability of Assessment on layer L; and

P_{NL} – Probability of Neutralization given first detection at layer L.

L is defined as the number of detection layers in the system before the critical detection point (CDP) in the adversary path(s). Detection after the CDP cannot not be counted.

P_E is defined as the system effectiveness of the layer. The system effectiveness of the layer is the product of the probability of interruption of the layer and the probability of neutralization given that detection occurred at that layer ($P_I \times P_N$). The probability of neutralization is determined discretely for each layer given detection at the layer. The neutralization determination is made if detection (regardless of the extent) takes place at the layer in question. Neutralization will occur sometime past the detection point and would be valid for the probability of neutralization of that specific layer.

P_D of the layer is defined as the product of the probability of sensing and the probability of assessment of the layer ($P_S \times P_A$). Note that detection and assessment will be different between the elements of the layer and between layers.

P_{IL} of the layer is defined as $P_{IL} = P_{DL}$ if detection on layer L is timely, and is equal to 0 ($P_{IL} = 0$) if detection is not timely.

Vertical line denotes change.

The Σ symbol is the summation of terms. The summation symbol is defined as:

$$\sum_{i=1}^{n} k_i \equiv k_1 + k_2 + ... + k_n$$

The Π symbol is the product of terms. The product symbol is defined by:

$$\prod_{i=1}^{n} f_i \equiv f_1 \times f_2 \times ... \times f_n$$

For those protection systems based on sensing, assessment, detection, interruption, and active neutralization of an adversary, credit can only be taken up to the "point on the pathway" at which the total of the adversary task time, engagement times, and delay times exceeds the protective force response times. This limiting criteria eliminates credit being taken for protection system capabilities that are not engaged prior to the adversary completing their objective. For denial based protection systems, the point on the pathway is the critical detection point. The critical detection point is defined as the point at which the protective force must have timely detection, assessment, and response to initiate a response to have a high probability of success in the neutralization of the adversary or denial of the adversary's task/objective. Therefore, for a facility employing multiple, complementary layers of protection, the representative total protection system effectiveness is calculated up to the point at which the protection systems can still effectively engage an adversary prior to completion of the objective.

The contributions of each layer along the adversary pathway are then combined to determine the overall system effectiveness, where the overall system effectiveness is provided by the sum of the contributions of each layer (only those encountered along the adversary pathway) to the system effectiveness.

An example of the system effectiveness equations for a three-layer system protecting SNM would be as follows:

In extended notation, the Overall System Effectiveness is:

$$P_E = (P_{A1} \text{ x } P_{S1} \text{ x } P_{N1}) + [(1 - (P_{A1} \text{ x } P_{S1})) \text{ x } (P_{A2} \text{ x } P_{S2} \text{ x } P_{N2})] + \{(1 - ((P_{A1} \text{ x } P_{S1}) + [(1 - (P_{A1} \text{ x } P_{S1})) \text{ x } (P_{A2} \text{ x } P_{S2})])) \text{ x } (P_{A3} \text{ x } P_{S3} \text{ x } P_{N3})\}$$

Which reduces to:

$$P_E = (P_{D1} \text{ x } P_{N1}) + [(1 - P_{D1}) \text{ x } (P_{D2} \text{ x } P_{N2})] + \{(1 - (P_{D1} + [(1 - P_{D1}) \text{ x } P_{D2}])) \text{ x } (P_{D3} \text{ x } P_{N3})\},$$

and since $P_{IL} = P_{DL}$ when detection is timely,

$$P_E = (P_{I1} \text{ x } P_{N1}) + [(1 - P_{I1}) \text{ x } (P_{I2} \text{ x } P_{N2})] + \{(1 - (P_{I1} + [(1 - P_{I1}) \text{ x } P_{I2}])) \text{ x } (P_{I3} \text{ x } P_{N3})\}$$

$$P_E = P_{E1} + [(1 - P_{I1}) \text{ x } P_{E2}] + \{(1 - (P_{I1} + [(1 - P_{I1}) \text{ x } P_{I2}])) \text{ x } P_{E3})\}$$

SECTION E

APPENDIX 5—SUGGESTED VULNERABILITY ASSESSMENT REPORT FORMAT

1.0 Executive Summary

Objective

Purpose and Summary of Protection Effectiveness

2.0 Introduction

Scope

Changes in the VAR

Methodology and Assumptions

3.0 Target Identification and Description

Theft or Diversion

Sabotage (Radiological)

Sabotage (Chemical and/or Biological)

Theft or Espionage of Classified Information or Matter

Other Losses

4.0 Threat Definition

Adversary Type(s)

Adversary Attributes

5.0 S&S Protection Elements

Physical Security Systems

Protective Forces (Response Strategies, Interruption, Neutralization)

Material Control and Accountability

Reliability Program

Vertical line denotes change.

6.0 Performance Testing

Program Description

Site Protection Elements

Critical Protection Elements

7.0 S&S Protection Effectiveness

Scenario

Protection Effectiveness

Validation Testing

8.0 Summary of S&S Protection Effectiveness

Protection Effectiveness

Recommendations

SECTION F—PERFORMANCE ASSURANCE PROGRAM

1. OBJECTIVE. To demonstrate the effectiveness of the protection provided Departmental safeguards and security (S&S) interests by systematically evaluating all protection program essential elements.

2. REQUIREMENTS. Each performance assurance program must be developed to validate the performance of all essential S&S protection elements.

   a. Operability and Effectiveness. Performance assurance programs must provide for operability and effectiveness testing of each protection program essential element or component.

      (1) Operability tests provide measures of integrity and must check the essential elements or total system to confirm operability.

      (2) Performance tests provide comprehensive assurance that protection program elements are performing as designed and provide the required levels of protection.

         (a) Performance tests results are used to validate the effectiveness of all elements of a layered S&S system.

         (b) Performance tests are not substitutes for compliance with requirements.

   b. Continuity. Performance assurance programs must evaluate operational continuity of all S&S essential elements. Limited Scope Performance Tests (LSPTs) and/or force-on-force (FoF) tests may be used as a means of meeting specific performance assurance testing requirements. Performance assurance programs must be evaluated as part of the DOE survey and the facility self-assessment programs as described in Section G of this Manual.

      (1) New protection program essential elements and components must be validated through acceptance testing before operational use.

      (2) Essential elements that have been repaired or undergone maintenance must be validated through testing before use.

      (3) The protective force (PF) must be performance tested both individually and in small tactical units.

      (4) Performance tests must ensure that approved protection strategies of denial, containment, recapture, recovery, and pursuit can be accomplished by the PF.

      (5) Essential elements of the protection program security systems and subsystems are performance tested to ensure that system detection,

Vertical line denotes change.

assessment, and response to alarms and adversarial actions meet stated requirements.

c. Reliability. Each essential element whose failure would reduce protection to an unacceptable level must be tested at frequencies that provide high assurance of operability and reliability.

(1) Testing frequencies must reflect site-specific conditions and operational needs.

(2) Testing frequencies must be documented for each essential element.

d. Performance Tests. At least every 365 days, an integrated performance test encompassing all essential protection elements associated with a comprehensive site or facility threat scenario must be conducted to evaluate the overall facility S&S effectiveness.

(1) Those Category I facilities requiring denial protection strategies must conduct integrated performance testing on a quarterly basis (at least every 3 months).

OR

(2) Those sites with multiple Category I facilities requiring denial protection strategies may rotate quarterly performance testing so that at least one facility is tested on a quarterly basis (at least every 3 months). However, an integrated performance test for all Category I facilities must occur at least once every 365 days.

e. Documentation.

(1) Performance Assurance Program Plan. This plan must be an integral part of the site safeguards and security plan (SSSP)/site security plan (SSP), or material control and accountability (MC&A) plan, as applicable. The performance assurance program plan must describe the program and its administration and implementation by:

(a) identifying protection elements for the protection of Category I and II special nuclear material (SNM) and Top Secret matter;

(b) describing how the performance of these elements is to be ensured, including the manner in which credit is taken for activities performed by external oversight organizations;

(c) addressing how deficiencies identified during performance assurance activities are to be corrected.

(2) Performance Assurance Reports. The results of performance assurance program testing must be documented.

(3) Document Retention. Record keeping systems must provide an audit trail for performance assurance activities and reports.

SECTION G—SURVEY, REVIEW, AND SELF-ASSESSMENT PROGRAMS

1. OBJECTIVES.

   a. Provide assurance to the Secretary of Energy, Departmental elements, and other government agencies (OGAs) that safeguards and security (S&S) interests and activities are protected at the required levels.

   b. Provide a basis for line management to make decisions regarding S&S program implementation activities, including allocation of resources, acceptance of risk, and mitigation of vulnerabilities. The results must provide a compliance- and performance-based documented evaluation of the S&S program.

   c. Identify S&S program strengths and weaknesses, develop and complete a process improvement schedule, and use the results to correct and improve the overall S&S program.

   d. Provide documentation of oversight and assessment activities.

2. REQUIREMENTS.

   a. Types and Frequencies of Surveys and Assessments.

      (1) Initial Surveys. Initial surveys must be conducted at facilities where there will be a facility clearance established for a facility with an importance rating of: A, B, C, or PP (see Section I, Chapter II). Survey activities must be comprehensive and result in a satisfactory composite rating prior to a facility clearance (FCL) being granted.

      (2) Periodic Surveys. Periodic surveys are conducted for all facilities and must cover all applicable topics to ensure survey program objectives are met. The periodic survey may be composed of multiple special survey reports, providing all the requirements of this section are met. Integration of internal and external reports including quality assurance, property appraisals, performance assurance, and other evaluation reports may be used to augment the requirement for a periodic survey. A DOE Federal facility (e.g. site office) conducting a periodic survey fulfills the self-assessment requirement as noted in paragraph 2a(6) below.

         (a) Facilities with importance ratings of A, B, or C must be surveyed once every 12 months [with the exception of Category IV special nuclear material (SNM) only facilities—see paragraph 2a(2)(c) below].

         (b) Facilities with an importance rating of PP must be surveyed once every 24 months.

(c) For facilities with Category IV SNM and nuclear material, including source material, the nuclear material control and accountability (MC&A) topical area must be surveyed at least every 24 months.

(d) Facilities with importance ratings of D, NP, or E do not require surveys but do require periodic reviews [see paragraph 2(a)(5) below].

(3) Special Surveys. Special surveys may be conducted at facilities for specific limited purposes. Examples include extended survey activities, technical security activities, "for cause" reviews, line management direction, shipment of nuclear and/or classified information or matter, or a change in the contractor operating a government-owned facility.

(4) Termination Surveys. Termination surveys must be conducted to verify the termination of Departmental activities and 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, property, security badge retrieval, debriefings, and verification of the termination or transfer of Department of Energy (DOE) access authorizations.

(a) Onsite termination surveys must be conducted at facilities possessing Top Secret matter, sensitive compartmented information (SCI)/ special access program (SAP) information or matter, or SNM.

(b) Onsite or correspondence termination surveys must be accomplished for all other possessing facilities.

(5) Periodic Reviews. A documented review of entities (D, NP, and E facilities) such as subcontractors, consultants, and common carriers must be performed by the DOE cognizant security authority at least every 5 years.

(6) Self-Assessments. Self-assessments must be conducted between the periodic surveys conducted by the cognizant security authority and include all applicable facility S&S program elements. The self-assessment must ensure the S&S objectives are met (see paragraph 1 above). Federal facilities may use the self-assessment to substitute for the Periodic Survey requirement. NP facilities are not required to conduct self-assessments. However, sponsoring organizations (Federal or contractor) must include in their self-assessments a thorough review of their registration program for NP facilities which may result in a program review of identified subcontractors.

(7) Reviews or Inspections by Other DOE Elements or OGAs. Reviews/inspections conducted by other DOE elements (including site quality assurance programs) or OGAs may be used to meet survey requirements. When using reviews/inspections conducted by other organizations to meet the requirements of the survey, the guidelines below must be followed.

(a) The review/inspection must have been conducted within the survey period.

(b) Applicable portions of the review/inspection must be attached to the survey report.

(c) Portions of topical and subtopical areas not covered by the review/inspection must be surveyed.

(d) If ratings were not assigned during the review/inspection, the surveying office must analyze the impact of any deficiencies and assign ratings.

(8) Extension of Frequency. The results of previous surveys may affect the frequency of future surveys. The interval between periodic surveys may be increased up to 24 months by the DOE cognizant security authority. Documentation of the justification for increases in the interval of periodic surveys must be maintained by the DOE cognizant security authority.

(a) The following conditions must be met for extensions:

1 the facility was rated satisfactory during the most recent survey activity;

2 the facility has no unmitigated deficiencies that impact the security posture of the facility, and all applicable topical area ratings are satisfactory from the previous survey; and

3 all applicable topical area ratings from the most recent self-assessment are satisfactory, and the DOE cognizant security authority concurs with the ratings.

(b) Increasing the interval between surveys for a facility possessing Category I SNM or with credible roll-up to Category I SNM must be approved, in writing, by the Associate Administrator for Defense Nuclear Security or the Under Secretary for Energy, Science, and Environment.

(c) All modifications to survey frequency requirements must be documented in the Safeguards and Security Information Management System (SSIMS).

b. Scope and Methodologies. Surveys and self-assessments must provide an integrated evaluation of all topical and subtopical areas to determine the overall status of the S&S program and ensure the objectives of this section are met (see paragraph 1 above). The integrated evaluation is a comprehensive synergistic approach using multiple S&S program elements that ensures total system effectiveness and, if properly implemented, will meet the objectives identified in paragraph 1 above. The scope of these activities and the methods used must include those listed below.

(1) Compliance. Compliance reflects the status of the S&S program as measured against implementation of applicable Federal statutes, regulations, policies, approved site safeguards and security plans (SSSPs)/site security plans (SSPs), and other approved security plans.

(2) Performance. Performance indicates the degree to which the elements of the S&S program meet protection objectives based on the operational testing of program elements.

(3) Comprehensiveness. Comprehensiveness identifies the breadth of protection afforded all activities and interests within a facility. This is accomplished by an evaluation of the adequacy and effectiveness of programs and a thorough examination of the implementation of policies, practices, and procedures to ensure compliance and performance. All applicable topical areas identified on DOE Form (F) 470.8, "Survey/Inspection Report" Form must be evaluated.

(4) Other. The scope of special and termination surveys is determined by the DOE cognizant security authority in coordination with the surveying office. Determinations of survey scope are predicated on the nature or status of operations at the facility, activity, or element being surveyed. These surveys may not cover all topical areas identified on DOE F 470.8.

3. CONDUCT. Local survey and self-assessment procedures implementing this section must be developed, documented, and approved by the cognizant security authority. Procedures must ensure completion of the objectives contained in paragraph 1 above and must include the requirements listed below.

a. Team Composition. Survey and self-assessment team personnel must possess qualifications, experience, and training sufficient to review and inspect the topical/subtopical areas of the survey/self-assessment. The National Training Center (NTC) provides training courses for survey team leaders and team members.

(1) Survey teams must be led by a Federal employee and may be composed of Departmental Federal and contractor personnel.

(2) Self-assessments must include at least one person from the cognizant security authority.

b. Planning, Scheduling, and Integration. Surveys and self-assessments must be planned, scheduled, and conducted in an integrated manner to achieve the objectives identified in paragraph 1 above. If topical and subtopical area evaluations are performed separately, the surveying office must document and integrate the results of each into a single (periodic) survey report that includes a composite facility rating. The frequency between topical and subtopical areas cannot exceed the frequency for the single (periodic) survey.

c. Validation. Results must be validated by methods including, but not limited to, document reviews, performance testing, and interview analyses and observations.

d. Exit Briefing. An exit briefing must be conducted with the surveyed or assessed organization to include the minimum facts:

(1) program strengths and weaknesses, including all findings;

(2) corrective action reporting requirements for all open findings, regardless of source; and

(3) topical and composite ratings. For less than satisfactory ratings, the communication of the composite rating initiates the actions required in paragraph 8 of this section.

4. FINDINGS.

a. Identification and Documentation. Findings are any validated program deficiency (failure to meet a performance or compliance requirement) regardless of source. Findings may be reflected in documents resulting from internal and external reviews, audits, appraisals, and other sources [e.g., the Office of Independent Oversight and Performance Assurance (OA), the Government Accountability Office (GAO), the Office of the Inspector General (IG), previous surveys, self-assessments, etc.].

All open findings must be reviewed during the survey or self-assessment to validate the status of corrective action and to evaluate the impact on the existing S&S program.

Findings identified during the current survey or self-assessment must be reported immediately to the Departmental element and contractor line management if a vulnerability to national security, classified information or matter, nuclear materials, or Department property results, or may result, in a programmatic impact to the Department. Findings identified during a survey or self-assessment,

even if closed during the survey or self-assessment activity, must be documented in the associated report.

b. Tracking. Findings and deficiencies, regardless of source, and corrective action plans (milestones and estimated completion dates) must be entered into SSIMS in accordance with SSIMS guidelines and tracked until closed. Quarterly status reports must be entered into SSIMS by January 15, April 15, July 15, and October 15, of each year. Self-assessment deficiencies are not required to be entered into SSIMS; however, a local mechanism/system must be used to track these deficiencies and corrective action until closed.

c. Trending. Trending evaluations must be considered in the resolution of findings in the subtopical area of program management to determine if systemic and systematic causal factors exist within the S&S program. Results of this evaluation that indicate negative trends must be analyzed to ensure corrective action plans address root causes and the need to ensure continuous improvement of the S&S program.

5. RATINGS.

a. Types. Ratings must be based on the effectiveness and adequacy of the program at a facility and reflect a balance of performance and compliance results as well as the impact of the deficiency(ies) (e.g., findings, IG recommendations, etc.) and mitigating factors. The ratings listed below must be used for all surveys (except termination), reviews, and self-assessments. Does Not Apply (DNA) and Not Rated (NR) may also be used in applicable situations.

(1) Types of Ratings.

(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.

(d) Inspection Ratings. “Effective Performance,” “Needs Improvement,” and “Significant Weaknesses” are indicators of a management system performance level as outlined in DOE O 470.2B, *Independent Oversight and Assurance Program*, dated 10-31-02.

(2) Rating Determinations.

(a) Existing Conditions. Ratings must be based on existing conditions at the end of the survey and not future or planned corrective actions or conditions.

(b) Impact. Ratings must be based on the impact of all open deficiencies, regardless of source.

(c) Marginal or Unsatisfactory Ratings. Less than satisfactory ratings in any topical area must be based on validated weaknesses in the S&S system or deficiencies in performance.

(d) Topical Area Ratings. A topical area rating must not be marginal for consecutive survey periods and will be assigned an unsatisfactory rating unless one of the following conditions applies.

1 The current survey of the topical area results in a satisfactory rating.

2 The previous survey that resulted in a marginal rating identified different deficiencies and reasons for the rating.

3 The deficiencies and reasons that were the basis for the previous marginal rating were related to the completion of a line item construction project or upgrade program. In that case, acceptable interim measures must have been implemented, physically validated pending completion of the project, and documented in the survey report.

(e) Subtopical Ratings. The decision whether or not to use all subtopical ratings must be documented in local procedures.[2] Regardless of the rating method used, the report must include the evaluation of all required subtopical areas which must be used as part of the appropriate topical area rating justification and rationale.

(f) Justification and Rationale. All ratings must be supported and documented to include the rating justification and rationale.

[2]A minimum of one subtopical area rating must be used to effect the rating for the topical area in Safeguards and Security Information Management System.

6. REPORT CONTENT.

a. Initial/Periodic Survey Reports and Self-Assessment Reports. Reports must contain the following items.

(1) A completed DOE F 470.8 (or equivalent for self-assessments).

(2) An executive summary containing:

(a) the scope, methodology, period of coverage, duration, date of the exit briefing to management;

(b) a brief overview of the facility, function, scope of operations, and contractual information (e.g., contract number, award and expiration dates, contract type, identification of security clauses, identification of the security and overall scores assigned to the most recent contract appraisal);

(c) a brief synopsis of major strengths and weaknesses that impact the effectiveness of the facility's overall S&S program, including identification of any topical areas rated less than satisfactory;

(d) the overall composite facility rating with supporting rationale; and

(e) a reference to a list of findings identified during the survey or self-assessment.

(3) An introduction containing:

(a) the scope, methodology, period of coverage, duration, and date of the exit briefing to management and

(b) a description of the facility, its function and scope of operations, security interests, and contractual information (e.g., contract number, award and expiration dates, contract type, identification of security clauses, identification of the security and overall scores assigned to the most recent contract appraisal).

(4) Narrative for all rated topical and subtopical areas that includes:

(a) a description of the site's implementation of the program element;

(b) the scope of the evaluation;

(c) a description of activities conducted;

(d) the evaluation results and associated issues (including other Department elements or OGA review or inspection results related to this topic/subtopic that were included in the survey);

(e) the identification of all findings, including new and previously identified open findings, regardless of source (e.g., OA, IG, GAO), and their current corrective action status; and

(f) an analysis that provides a justification and rationale of the factors responsible for the rating.

(5) Attachments, including:

(a) a copy of the current DOE F 470.2, "Facility Data and Approval Record" (FDAR);

(b) a listing of all active DOE F 470.1, "Contract Security Classification Specification" (CSCS), or DD F 254, "Contract Security Classification Specification;"

(c) a listing of all new findings resulting from the survey/self-assessment;

(d) a listing of all previous findings that are open, to include the current status of corrective action;

(e) a listing of team members including names, employer, and their assigned area(s) of evaluation; and

(f) a listing of all source documentation used to support the survey/self-assessment conduct and results (e.g., GAO, IG, OA, and similar assessment documents).

b. Special Survey Reports. Special survey reports must follow the format and content for initial and periodic survey/self-assessment reports except that an executive summary is not required. Attachments must be included as appropriate to the scope of the special survey.

c. Reports for Non-Possessing Facilities. Reports for non-possessing facilities must include:

(1) a completed DOE F 470.8;

(2) a copy of the DOE F 470.2 FDAR;

(3) a list of each active DOE F 470.1 CSCS or DD F 254;

(4) an evaluation of the foreign ownership, control, or influence (FOCI) status;

(5) a determination that employees and subcontractors possess appropriate access authorizations;

(6) a review to ensure that individuals no longer employed on the contract have had their access authorizations terminated and security badges have been accounted for; and

(7) other topical/subtopical areas identified on DOE F 470.8 as required by the DOE cognizant security authority.

d. Termination Survey Reports. Termination survey reports must include:

(1) verification of non-possession of classified information or matter, SNM, hazardous material presenting a potential sabotage threat, or Government property;

(2) verification that all DOE access authorizations have been terminated or transferred and that termination statements have been completed and security badges have been accounted for;

(3) validation that all findings have been closed in SSIMS;

(4) verification of termination of all S&S activities;

(5) a copy of the terminating DOE F 470.2 FDAR; and

(6) a completed certificate of non-possession.

e. Memorandum Report Content. Memorandum reports for DOE programmatic entities and OGAs are generated when it is inappropriate to transmit a copy of the survey report due to need-to-know issues. Reports must contain:

(1) a notification of inclusion of their activity in the survey;

(2) the date of the survey;

(3) ratings and rationale for the ratings associated with the activity; and

(4) all findings applicable to that activity.

7. DISTRIBUTION.

a. The surveying office must send a copy of the survey report to the appropriate Departmental elements and support offices, including the Office of Security.

b. The surveying office must send any memorandum report to applicable DOE program offices and OGAs.

c. Survey/memorandum reports must be distributed within 60 working days of the exit briefing.

d. Self-assessment reports must be distributed to the applicable senior managers, personnel responsible for corrective actions, and other personnel, as deemed appropriate.

8. NOTIFICATIONS AND ACTIONS FOR LESS THAN SATISFACTORY SURVEY COMPOSITE RATINGS. When the survey composite ratings are less than satisfactory the following notifications and actions must occur.

a. Marginal Ratings. Within 15 working days of the determination of a marginal composite rating, the DOE cognizant security authority must ensure SSIMS is updated and provide the applicable Departmental elements and OGAs with the following:

(1) a statement identifying the vulnerabilities and the rationale for the rating;

(2) description of the corrective action/compensatory measures taken to date;

(3) a statement acknowledging physical validation of the adequacy of items listed in paragraph 8a(2) above.

(4) If the surveying office is not the same as the DOE cognizant security authority, the surveying office must notify the DOE cognizant security authority of results prior to departure from the site.

b. Unsatisfactory Ratings. Within 24 hours of determination of an overall composite rating of Unsatisfactory, the DOE cognizant security authority must coordinate with the Departmental element to take the following actions.

(1) Suspend the activity and/or the Facility Clearance (FCL) pending remedial action.

OR

(2) Provide the justification for continuing this critical operation to the Office of Security, the Departmental element, and as directed, other applicable Department elements. In addition to providing the rationale, the DOE cognizant security authority must identify and evaluate those immediate interim corrective actions being undertaken to mitigate identified risks or vulnerabilities.

NOTE: If the surveying office is not the same as the DOE cognizant security authority, the surveying office must notify the DOE cognizant security authority of the results immediately. If the surveying office is unable to contact the DOE cognizant security authority, action must be taken to protect activities until the DOE cognizant security authority can be notified. Subsequent action must be taken on the basis of agreement between the two organizations and must be fully documented in the survey report.

9. NOTIFICATIONS AND ACTIONS FOR LESS THAN SATISFACTORY SELF-ASSESSMENT COMPOSITE RATINGS. Actions required in response to less than satisfactory self-assessment composite ratings are listed below:

a. Marginal Ratings. Within 15 working days of the determination of a marginal composite rating, notification must be made to line management that includes:

(1) a statement identifying the vulnerability and rationale for the rating;

(2) a description of the corrective action/compensatory measures taken to date; and

(3) a statement acknowledging physical validation of the adequacy of items listed in paragraph 9a(2) above.

b. Unsatisfactory Ratings. Within 24 hours of determination of an overall composite rating of unsatisfactory, the cognizant security authority must coordinate with the DOE cognizant security authority, which in turn must coordinate with the Departmental element to take the following actions:

(1) suspend the activity and/or recommend suspension of the FCL pending remedial action;

(2) provide justification for continuing operations to the DOE cognizant security authority. In addition to providing the rationale, the cognizant security authority must evaluate those immediate interim corrective actions being undertaken to mitigate identified risks or vulnerabilities; and

(3) if the results of a self-assessment identify an incident of security concern; it must be reported in accordance with Section N.

10. CORRECTIVE ACTIONS. Corrective action plans must be developed for all open survey and self-assessment findings. Corrective action plans for survey and self-assessments must be submitted and reported within 30 working days after the date of the exit briefing. If a finding is corrected during the survey, it will be identified in the survey report with a description of the closure/validation performed by the survey/ self-assessment team. Quarterly reports of the status of corrective actions for each finding must be provided to the DOE cognizant security authority. All survey and self-assessment corrective actions must:

a. be based on documented root cause analyses, risk assessments, and cost-benefit analyses to ensure the survey/self-assessment program objectives are met (see paragraph 1 above) and

b. be reported, entered, tracked, and updated until completed, validated, and closed in SSIMS, where applicable (see paragraph 4b above).

11. UPGRADE OF COMPOSITE RATINGS. When line management determines that the composite rating should be upgraded, the survey/self-assessment team must physically verify the completion and adequacy of corrective actions and make notification of the rating upgrade in accordance with approved local procedures.

12. RECORDS RETENTION. Documentation associated with the conduct of survey and self-assessments must be retained in accordance with approved procedures and appropriate records inventory disposition schedules.

13. CONTINUOUS IMPROVEMENT PROCESS. The cognizant security authority must conduct an annual evaluation of their survey or self-assessment processes. This evaluation must ensure any identified process improvements (i.e., lessons learned) are incorporated in the S&S survey/self-assessment process.

PART 2—SAFEGUARDS AND SECURITY MANAGEMENT

SECTION H—FOREIGN OWNERSHIP, CONTROL, OR INFLUENCE PROGRAM

1. OBJECTIVE. To establish the Foreign Ownership, Control, or Influence (FOCI) program requirements and criteria to facilitate the initial and continued facility clearance (FCL) eligibility of U.S. companies with foreign involvement.

CHAPTER I. GENERAL FOCI PROGRAM INFORMATION

1. GENERAL REQUIREMENTS.

a. Evaluation and adjudication of FOCI compose an essential and critical ongoing element of the FCL program. 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. An FCL may not be granted until all relevant aspects of FOCI have been resolved and, if necessary, favorably adjudicated. If a company with an existing FCL is determined to be under FOCI, the FCL must be suspended or terminated unless security measures are taken to remove the possibility of unauthorized access or adverse impacts to classified contract performance.[3]

b. The determination of whether a U.S. company is under FOCI, its eligibility for an FCL, and the security measures deemed necessary to negate FOCI impacts must be made on a case-by-case basis. The following factors must be considered in the aggregate to determine whether a company is under FOCI, is eligible for an FCL, and the protective measures required:

(1) foreign intelligence threat;

(2) risk of unauthorized technology transfer;

(3) type and sensitivity of classified information or matter, or special nuclear material (SNM);

(4) nature, source, and extent of FOCI, including identification of immediate, intermediate, and ultimate parent organizations;

(5) record of compliance with pertinent laws, regulations, and contracts; and

(6) nature of bilateral and multilateral security and information exchange agreements that may be relevant.

c. Development of security measures to mitigate the impact of unacceptable FOCI must be based on the concept of risk management. DOE has the 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 effectively precluded and the performance of classified contracts is not adversely affected.

d. Changed conditions, such as a change in ownership, indebtedness, or foreign intelligence threat, may justify certain adjustments to the security requirements

[3]Classified contract is defined as any contract, license, or other agreement requiring access authorizations.

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.

2. APPLICABILITY.

a. The entities[4] listed below are required to obtain FOCI determinations.

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

(2) All tier parents located in the United States, Puerto Rico, or a U.S. possession or trust territory

b. A FOCI determination is not required for an individual performing work under a consulting agreement (e.g., an individual awarded a contract).[5] This does not include individuals contracting as a business.

c. When the applicant is a local, State, or Federal agency or department, the contract must contain a security clause. The security clause must state that if the government agency or department subcontracts any work requiring access to classified information or matter by a commercial entity, its acquisition regulation, including FOCI policies, must be followed. 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. When contracts involve access to SNM, DOE will render the FOCI determination.

e. Contractors with existing U.S. Government FCLs are identified in Safeguards and Security Information Management System (SSIMS) and the Department of Defense (DoD) Defense Security Service/Central Verification Activity System (DSS/CVA).

f. No further FOCI review is required for an applicant holding an equal or higher U.S. Government FCL, based upon a favorable FOCI determination.

[4]The entities listed are referred to as "applicants" throughout this section.

[5]The self-employed individual's or consultant's foreign involvement is determined through the background investigation conducted to determine the individual's eligibility for an access authorization.

g. Information submitted with a FOCI package is used for the sole purpose of evaluating FOCI and must be treated by DOE, to the extent permitted by law, as business/financial information submitted in confidence. The information must be protected as Official Use Only (OUO).

h. Personnel responsible for the FOCI program can successfully meet FOCI competencies through training courses offered at the National Training Center (NTC).

3. CONTRACT AWARD MUST NOT BE MADE PRIOR TO FCL ISSUANCE. The DOE Acquisition Regulation (DEAR) prohibits the award of a classified contract until an FCL has been granted. When an existing contract that does not require access authorizations is modified to require access authorizations, the contract modification cannot take effect until an FCL is granted. Contract award/modification cannot be made until:

a. all relevant aspects of FOCI have been resolved and, if necessary, are favorably adjudicated;

b. the signed DOE F 470.1, "Contract Security Classification Specification" (CSCS) is accepted by the cognizant security authority; and

c. the appropriate DEAR security clauses have been incorporated in the contract.

4. ELECTRONIC SUBMISSION/PROCESSING WEB SITE. The Department has an electronic system for applicants to submit FOCI information to DOE in an electronic format. To ensure confidentiality of the information submitted and stored on the system, the site is protected with 128-bit encryption.

a. Applicants may use this system for the submission of FOCI packages, including changes to update their FOCI information. The FOCI Web site maybe accessed via an Internet browser at https://foci.td.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 be submitted to the DOE cognizant security authority.

b. Federal employees and supporting contractors should use the Electronic Submission Processing System Web site at http://greylist.td.anl.gov.

CHAPTER II. FOCI ACTIVITIES

1. DETERMINING THE SECURITY REQUIREMENTS OF THE CLASSIFIED CONTRACT/AGREEMENT.

   a. The procurement request originator (or other individual(s), as designated by line management) must identify and document, on the appropriate procurement form, the security requirements of the classified contract. If the procurement request requires access authorizations, a DOE F 470.1 CSCS[6] must be completed by the procurement request originator.

   b. The procurement request originator submits the appropriate procurement form and DOE F 470.1 CSCS to the contracting officer. Upon receipt of these forms, the contracting officer must incorporate the appropriate security clauses in the solicitation. When the applicant is included in the competitive range, they will be required to complete the SF 328.

2. DETERMINING THE FCL STATUS OF THE APPLICANT. The contracting officer must identify the FCL status of all applicants within the competitive range and preliminary selection criteria for the pending contract. The contracting officer must then verify whether the applicant's FCL meets the appropriate level of the pending contract. Verification of existing FCLs must be obtained through SSIMS or DoD DSS/ CVA.

3. ACCEPTING A FOCI DETERMINATION RENDERED BY ANOTHER FEDERAL AGENCY. The DOE cognizant security authority may accept FOCI determinations granted by another Federal agency when the related requirements of Section I are met.

4. CLASSIFIED CONTRACT.

   a. When the contracting officer determines that the applicant possesses an existing FCL at the same level required by the pending contract, the contracting officer must send a DOE F 470.1 CSCS to the DOE cognizant security authority for review and approval. Contract award cannot be made until the DOE F 470.1 CSCS is signed by the DOE cognizant security authority and returned to the contracting officer.

   b. When the contracting officer determines that the applicant possesses an existing FCL but the pending contract requirements exceed the level of the current FCL, the contracting officer must send a DOE F 470.1 CSCS to the DOE cognizant security authority for review and approval. Contract award cannot be made until the contracting officer has received the signed DOE F 470.1 CSCS from the DOE cognizant security authority.

[6] If a DD F 254, DoD CSCS, has been used by the agency sponsoring the activity; it can be submitted instead of the DOE F 470.1 CSCS, provided it is annotated with the DOE facility code.

c. When the contracting officer determines that the applicant does not possess an FCL based on a FOCI determination, the contracting officer must obtain a
| complete FOCI package. Appendix 6, FOCI Matrix, summarizes the documents and forms required to be completed and submitted by the applicant.

(1) When the applicant is owned by a parent organization(s), a separate FOCI package must be submitted for the applicant and each tier parent located in the United States, Puerto Rico, or a U.S. possession or territory. Foreign tier parents do not need to submit a FOCI package, but each foreign tier parent must be identified in the FOCI submission(s), and details provided as to whether the foreign parent(s) is controlled by any foreign government or any entity that is controlled by a foreign government.

(2) When the applicant is a division or branch of a legal entity (i.e., part of but not a separate legal entity), the division/branch only needs to submit a listing of its key management personnel (KMP) and, if applicable, representative of foreign interest statement(s) and authorizing resolutions[7] for the division/branch's KMP. The legal entity and, if applicable, its tier parents must submit a complete FOCI package.

d. After obtaining the packages from the applicant, the contracting officer must review the submission(s) to ensure the package(s) is complete. When the package(s) is incomplete, the contracting officer must notify the applicant that the package cannot be submitted for a FOCI determination and must request a complete package. After obtaining the required FOCI documentation, the contracting officer forwards the FOCI package to the DOE cognizant security authority for processing.

e. Contracting officers must provide written notice to the DOE cognizant security authority when:

(1) a notice of change has been submitted by the applicant on a FOCI package submitted for FOCI review;

(2) a requested FOCI review is no longer needed;

(3) a FOCI determination was rendered on an applicant that was not awarded the contract; and

(4) all work on a contract requiring access authorizations is within 30 days of the termination or completion. This notification must also be made when access authorizations are no longer required in performance of the contract. (Notification can be accomplished by using DOE F 470.1 CSCS.)

[7]Resolutions (adopted by the governing body) that list the express authority (i.e., duties and responsibilities) of the organization's key management personnel.

Vertical line denotes change.

f. 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.

g. A final FOCI determination can only be requested for the successful applicant. Procurement requesters must allow sufficient lead-time for the processing of the FOCI determination and FCL prior to award of the contract.

5. ADJUDICATION.

a. Adjudication Level.

(1) The DOE cognizant security authority[8] renders the FOCI determination under the following conditions:

(a) the responses to the FOCI questions do not exceed the thresholds established by the Office of Security; and

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

(2) If the FOCI exceeds established thresholds, the DOE cognizant security authority will forward the FOCI submission(s) to the Office of Security with:

(a) the justification for clearance or exclusion, including the nature of business and products or services to be furnished under the classified contract and the technologies involved, and

(b) the DOE cognizant security authority's analysis, including a clear statement of the reason why Office of Security adjudication is required. The Office of Security, in coordination with the Office of the General Counsel when appropriate, will provide a final FOCI determination to the DOE cognizant security authority.

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. In addition, these assessments must be updated periodically under circumstances and at intervals considered appropriate by the

[8]The cognizant security authority must identify key management personnel requiring clearance in conjunction with the facility clearance.

Federal agency granting the FCL. In reviewing non-majority foreign ownership or control packages, the DOE cognizant security authority must also identify information that may be of CI interest.

(1) During FOCI adjudication, the DOE cognizant security authority must identify and forward any information that may be of CI interest to the local Office of Counterintelligence (OCI)/Office of Defense Nuclear Counter Intelligence (ODNCI) for further analysis. The local OCI/ODNCI must analyze the information and, if applicable, provide the FOCI DOE cognizant security authority with threat information relevant to the FOCI case. Local FOCI adjudication is not dependent on and should not be delayed pending feedback from the local OCI/ODNCI. However, if the local OCI/ODNCI provides relevant information, the DOE cognizant security authority must ensure that appropriate security countermeasures are established at the facility.

(2) For FOCI packages requiring Office of Security adjudication, the DOE cognizant security authority will forward available CI information (i.e., local CI feedback) with the FOCI package. The DOE cognizant security authority should not delay submission pending local CI feedback. If additional CI information is expected, that should be noted in the transmittal to the Office of Security. The Office of Security must coordinate with the appropriate intelligence agency(ies), and forward available threat information with the FOCI adjudication through appropriate program channels to the DOE cognizant security authority.

NOTE: The DOE cognizant security authority is responsible for ensuring that the periodic CI threat assessment and technology transfer risk assessment updates are accomplished. These requests must be processed through the Office of Security.

c. Adverse Determinations.

(1) Each FOCI package must be judged on its own merits, and final determination remains the responsibility of DOE. Any doubt as to whether unacceptable FOCI can be effectively mitigated (i.e., whether 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) An applicant that will not implement the security measures determined necessary by DOE to mitigate its foreign involvement to an acceptable level is ineligible for an initial FCL (including a FOCI determination).

(3) Suspension, reinstatement, and termination of an FCL due to unacceptable FOCI are addressed in Section I.

d. Schedule Requirements for Processing Determinations. The following schedule must be observed in processing FOCI determinations.

(1) Within 15 working days of receipt of a FOCI submission from the contracting officer, the initial review and verification procedures must be accomplished.

(2) Within an additional 20 working days, one of the following actions must be taken.

(a) A FOCI determination must be rendered by the DOE cognizant security authority if FOCI thresholds are not exceeded.

(b) If required, additional information must be requested either verbally or in writing from the applicant.

(c) The FOCI package, which has been reviewed for completeness, must be forwarded to the Office of Security if established thresholds are exceeded. For packages forwarded to the Office of Security for action, the foregoing schedule must also be observed.

(3) If, for any reason, a FOCI determination has not been rendered within 90 working days of receipt, the following actions must be taken.

(a) The DOE cognizant security authority must either:

1 provide written notification to the submitting contracting officer regarding the reason for the delay in processing/ completing the submission or

2 return the submission to the submitting contracting officer if the contractor has been nonresponsive to the DOE cognizant security authority's request for additional information or implementation of required security measures. The DOE cognizant security authority should coordinate with the contracting officer for assistance in obtaining information from an unresponsive applicant.

(b) The Office of Security must either:

1 provide written notification to the DOE cognizant security authority regarding the reason for the delay in processing/completing the submission or

2 return the submission to the DOE cognizant security authority if the contractor has been nonresponsive to the Office of Security's request for additional information or

implementation of required security measures. The DOE cognizant security authority must coordinate with the contracting officer for assistance in obtaining information from an unresponsive applicant.

e. Notifying the Requesting Contracting Officer. Upon completion of DOE's review of the applicant's FOCI, the DOE cognizant security authority must provide the contracting officer with written notification as to whether the contractor's FOCI will or will not prevent contract award. If the applicant is granted an FCL, the DOE cognizant security authority must sign and return the DOE F 470.1 CSCS to the contracting officer. Contract award can be made upon:

(1) receipt of the signed DOE F 470.1 CSCS and

(2) inclusion, by the contracting officer, of the appropriate DEAR security clauses in the contract.

6. 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 Treasury under section 721 of the Defense Production Act. Under the CFIUS voluntary process, potential foreign investors submit their proposed merger, acquisition, or takeover for review by executive branch agencies to determine if the President will, as provided by law, disallow the transaction in the interests of national security. By law, CFIUS must notify prospective foreign investors of the results of its review within 30 calendar days of the date of the filing. Therefore, it is imperative that the Department promptly review all cognizant security authority-referred CFIUS cases and, through approved channels, inform the CFIUS staff chair of its questions or concerns within 30 days of the date of the filing (optimally by day 16 of the 30-day review period).

b. If the applicant is a cleared contractor, it is the responsibility of the Federal agency designated as the applicant's cognizant security authority[9] to do the following:

(1) identify all classified contracts and all cleared locations and obtain complete information regarding any contracts requiring access to proscribed information;

[9]A cleared contractor may hold a facility clearance (FCL) granted by more than one agency. In those cases, each agency that granted FCL (based on a FOCI determination rendered by that agency) must fulfill the responsibility listed above.

(2) obtain a shareholder agreement, letter of intent, and a revised SF 328 containing information about the acquisition;

(3) have the contractor submit a proposed plan of action to address the FOCI issue if the contractor has not already done so; and

(4) through approved appropriate channels, promptly inform those departments/agencies responsible for the contracts and/or classified information or matter of the proposed transaction and the FOCI mitigation method proposed if consummation of the proposed transaction would require security measures to be imposed.[10]

c. The CFIUS review and the industrial security review are carried out in two parallel but separate processes with different time constraints and considerations. When FOCI mitigation methods are required to resolve the industrial security concerns of a case under review by CFIUS, ideally there should be an agreement prior to the 30th day of the CFIUS review. When, however, the overall industrial security evaluation process is unable to be completed due to the situations listed below, the situation can be the basis for recommending that the DOE's position be an investigation of the proposed transaction by CFIUS to ensure that national security concerns are protected.

(1) Inability to reach agreement on the FOCI mitigation method, whether because of rejection of the FOCI mitigation action plan by the parties of the proposed transaction under CFIUS review or by a Federal agency or department, and/or failure to attain agreement regarding material terms of such an arrangement.

(2) Failure by the applicant company to comply with the FOCI reporting requirements (see Chapter III of this section).

[10]If a National Interest Determination (NID) or Secretarial waiver is required, notification to the department/agency must include a request asking whether the department/agency will support a NID or Secretarial waiver, as applicable, based on the proposed FOCI mitigation plan.

CHAPTER III. REPORTING REQUIREMENTS

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 to the contracting officer.

2. UPDATES. Contractors holding an FCL based upon a favorable FOCI determination must submit written reports of changed conditions and anticipated changes. Additionally, contractors are required to submit a new FOCI package at least once every 5 years.

   a. Significant Changes. When changes have occurred in the extent and nature of FOCI that affect the information in an applicant's most recent FOCI submission(s), the applicant must provide written notification and supporting documentation relevant to the changes to the DOE cognizant security authority. Significant changes that warrant a new FOCI determination include the following:

      (1) a new threshold or factor exists that did not exist when the previous determination was made (e.g., a "no" answer changes to "yes"), and any additional factors associated with the questions on the SF 328;

      (2) a previously reported threshold or factor that was favorably adjudicated by the DOE cognizant security authority has increased to a level requiring a determination by the Office of Security;

      (3) 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 or end user (i.e., for revenue and/or net income) or lenders (i.e., indebtedness);

      (4) 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

      (5) any changes in ownership or control. 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). Notification of these changes must be made to the cognizant security authority no later than 5 working days after the event or action necessitating the notice.

   b. Anticipated Changes. Anticipated changes are events that arise when the contractor or any of its tier parents enters into formal negotiations toward

agreement, and in any event 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 authority with written notification of anticipated actions including, those listed below.

(1) An action to terminate business or operations of the contractor or any of its parents for any reason; e.g., 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 its business or assets; 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(s).

c. Other Reportable Changes.

(1) Any change of operating name or address of the company or any of its cleared locations. The cognizant security authority must be notified at least 5 working days prior to the effective date of an address change.

(2) Any change to the information previously submitted for KMP, including, as 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 authority.

(a) Date and place of birth, social security number, citizenship, and, if appropriate, personnel security clearance level and issuing agency.

(b) Whether they have been excluded from access to classified information or matter, or SNM.

(c) Whether they have been temporarily excluded from access to classified information or matter, or SNM pending the granting of their DOE access authorization.

(d) A new complete listing of KMP need only be submitted at the discretion of the contractor and/or when requested in writing by the DOE cognizant security authority.

d. Submission of a New FOCI Package. A new FOCI package must be completed by the contractor or tier parent and submitted to the DOE cognizant security authority at least every 5 years or at the request of the cognizant security authority.

3. ANNUAL CERTIFICATION.

a. Each contractor holding an FCL, based upon a favorable FOCI determination, must provide written annual (at least every 12 months) certification to the DOE cognizant security authority acknowledging that:

(1) no significant change has occurred in the extent and nature of FOCI that would affect the organization's answers to the questions provided in its SF 328;

(2) no changes have occurred in the organization's ownership or legal entity name; and

(3) no changes have occurred in the organization's KMP. In addition, when the contractor's governing body has invoked resolutions to process KMP for access authorizations and to exclude from the personnel clearance requirement certain members of its governing body and other officers and executive personnel, the contractor's certification must include statements as to whether:

(a) each of the organization's KMP, required to obtain and retain an access authorization, continues to hold the required access authorization;

(b) any changes have occurred in the positions held by any of the organizations uncleared KMP whereby the duties of such position(s) require the KMP, to be identified by name, to have access to classified information or matter, or SNM or to be involved in the protection of classified information or matter, or SNM;

(c) the invoked resolutions remain in full force and effect; and

(d) there were any acts of noncompliance with these security measures, whether inadvertent or intentional, with a description of steps that were taken to prevent such acts from recurring.

b. Any contractor controlled by a parent organization(s) that has/have been excluded (by formal resolution) must provide written certification on an annual (at least every 12 months) basis to the DOE cognizant security authority acknowledging the continued effectiveness of the resolution. Additionally, the contractor must obtain and provide to its DOE cognizant security authority written certification executed by an authorized official from each such excluded parent that:

(1) no significant changes have occurred in the extent and nature of FOCI that would affect the organization's answers to the questions provided in its SF 328;

(2) no changes have occurred in the organization's ownership or legal entity name;

(3) no changes have occurred in the organization's KMP; and

(4) the exclusionary resolution invoked by the contractor's tier parent's governing body remains in full force and effect.

c. Any contractor that has executed a Board Resolution to reduce FOCI in noncontrolling foreign ownership situations (see paragraph 4a, Chapter IV of this section) must provide written certification on an annual (at least every 12 months) basis to its DOE cognizant security authority acknowledging the continued effectiveness of the resolution.

d. At the end of each year of operation, the trustees, proxy holders, or outside directors, as appropriate, of those organizations operating under a DOE-approved Voting Trust Agreement, Proxy Agreement, Special Security Agreement, or Security Control Agreement[11] must submit to the DOE cognizant security authority an annual (at least every 12 months) implementation and compliance report. The annual implementation and compliance report must include:

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

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

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

[11] A contractor operating under one of these FOCI mitigation plans must also submit the applicable annual certifications mentioned in paragraphs 3a, 3b, and 3c.

(4) any changes or impending changes of senior management officials or key governing body members, including the reasons;

(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 FOCI mitigation agreement.

CHAPTER IV. FOCI MITIGATION ACTION PLANS

1. GENERAL. 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 U.S. national security interests. The following FOCI policy for U.S. companies subject to an FCL is intended to facilitate foreign investment while ensuring that foreign firms cannot undermine U.S. security and export controls to gain unauthorized access to critical technology, classified information or matter, or SNM.

2. MITIGATION ACTION PLANS. The affected U.S. organization or its legal representatives may propose a plan to negate or reduce unacceptable FOCI; however, DOE reserves the right and has the obligation to impose any security method, safeguard, or restriction it believes necessary to ensure that unauthorized access to classified information or matter, or SNM is precluded.

   a. In cases where the FOCI stems from foreign ownership, a plan must consist of one of the methods prescribed in paragraph 3 of this chapter. Amendments to purchase and shareholder agreements may also serve to remove or mitigate FOCI concerns.

   b. When factors not related to ownership are present, the plan must provide positive measures that ensure that the non-U.S. citizen can be effectively denied access to classified information or matter, or SNM and cannot otherwise adversely affect performance of classified contracts. Examples of such measures include:

      (1) physical or organizational separation of the component performing the work requiring access authorizations;

      (2) modification or termination of agreements with non-U.S. citizens;

      (3) diversification or reduction of agreements with non-U.S. citizens;

      (4) diversification or reduction of revenue from non-U.S. citizens;

      (5) assignment of specific security duties and responsibilities to selected officials of the organization; and

      (6) creation of special executive-level committees to consider and oversee classified information or matter, or SNM.

3. FOREIGN OWNERSHIP.

   a. Secretarial Waiver Authority. 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[12] unless a waiver has been granted by the Secretary concerned (i.e., the Secretary of Energy or the Secretary of Defense).

(1) 10 U.S.C. 2536 (b) (1) (A) allows the Secretary concerned to waive the prohibition on the award of contracts (including execution of a novation agreement) set forth in 10 U.S.C. 2536(a), if the Secretary determines that a waiver is essential to the national security interest of the United States. Requests for waivers under 10 U.S.C. 2536(b)(1)(A) must include the following:

(a) identification of the proposed awardee and description of the control by a foreign government;

(b) description of the procurement and performance requirements;

(c) description of why waiver is essential to the national security interests of the United States;

(d) availability of other U.S. companies with the capacity, capability, and technical expertise to satisfy acquisition, technology base, or industrial base requirements and the reasons any such company should be denied the contract; and

(e) description of any alternative methods to accomplish the mission and the reasons why those alternative methods should not be utilized.

(2) 10 U.S.C. 2536(b) (1) (B) allows the Secretary of Energy to waive the prohibition on the award of contracts (including execution of a novation agreement) set forth in 10 U.S.C. 2536(a) for environmental restoration, remediation, or waste management contracts at a DOE facility if the Secretary determines that a waiver will (i) advance the environmental restoration, remediation, or waste management objectives of DOE and (ii) will not harm the national security interest of the United States. Also, the entity to which the contract is to be awarded is controlled by a foreign government with which the Secretary has executed an agreement to exchange Restricted Data (RD) under section 144c of the Atomic Energy Act [42 U.S.C. 2164(c)]. Requests for waivers under 10 U.S.C. 2536(b)(1)(B) must include the following:

[12]Proscribed information is defined as Top Secret (TS); communications security (COMSEC) information, except classified keys used to operate secure telephone units (STU IIIs); Restricted Data/Formerly Restricted Data as defined in the Atomic Energy Act; special access program (SAP) information; or sensitive compartmented information (SCI).

(a) identification of the proposed awardee and description of the control by a foreign government;

(b) description of the procurement and performance requirements;

(c) description of how the Department's environmental restoration, remediation, or waste management objectives will be advanced;

(d) description of why the waiver will not harm the national security interests of the United States;

(e) availability of other U.S. companies with the capacity, capability, and technical expertise to satisfy acquisition, technology base, or industrial base requirements and the reasons any such company should be denied the contract;

(f) description of any alternative methods to accomplish the mission and the reasons why those alternative methods should not be utilized; and

(g) evidence that the U.S. Federal Government and the foreign government involved have entered into an agreement that authorizes the exchange of RD under section 144.c. of the Atomic Energy Act [42 U.S.C. 2164(c)].

If the Secretary decides to grant a waiver under 10 U.S.C. 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.

(3) Proposed Secretarial waivers under 10 U.S.C. 2536(b) must be:

(a) prepared by the contracting officer whose contract is involved;

(b) sponsored by the head of the contracting activity; and

(c) forwarded through the cognizant Departmental element to the Secretary for approval.

When the proscribed information is under the classification or control jurisdiction of another agency, the proposed secretarial waiver must be coordinated with the cognizant Federal agency through the Office of 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 methods listed below.

(1) Voting Trust Agreement. Under this type of agreement, controlling foreign shareholders must transfer legal title of their stock to the trustees. The U.S. organization to be cleared must be organized, structured, and financed to operate as a viable business entity independent from the foreign shareholder(s). The Voting Trust Agreement does not impose any restrictions on the cleared U.S. organization's eligibility to have access to classified information or matter or to compete for classified contracts. The following requirements must be met.

(a) The Voting Trust Agreement must unequivocally provide for the exercise of all prerogatives of ownership by the trustees with complete freedom to act independently and without consultation with, interference by, or influence from foreign shareholders, but nothing herein prohibits the trustee(s) from consulting with the foreign shareholders, or vice versa, where otherwise consistent with U.S. laws and regulations and the terms of the Voting Trust Agreement.

(b) There must be at least three trustees. These trustees must become members of the U.S. organization's governing body. In addition, the trustees must meet the following criteria.

1 Be U.S. citizens residing within the limits of the United States and capable of assuming full responsibility for voting the share and exercising the management prerogatives relating thereto in such a way as to effectively insulate foreign shareholder(s) from the cleared U.S. organization.

2 Be completely disinterested individuals with no prior involvement with the cleared U.S. organization, its foreign-owned tier parent(s), or any of its foreign-owned affiliate(s). These individuals must be approved by the Director, Office of Security.

3 Be issued and be able to maintain an access authorization to the level of the FCL.

4 Be advised by the DOE cognizant security authority of the duties and their responsibilities on behalf of DOE to insulate the cleared U.S. organization from the non-U.S. citizen(s), and indicate, in writing, their willingness to accept this responsibility.

(c) Notwithstanding the foregoing, the Voting Trust Agreement may limit the trustees by requiring them to obtain approval from the foreign shareholder(s) with respect to the following:

1 the sale or disposal of the cleared U.S. organization's assets or a substantial part thereof;

2 pledges, mortgages, or other encumbrances on the capital stock they hold in trust;

3 corporate mergers, consolidations, or reorganizations;

4 the dissolution of the cleared U.S. organization; and

5 the filing of a bankruptcy petition.

(2) Proxy Agreement. Under this arrangement, the voting rights of shares owned by controlling foreign shareholders are conveyed to proxy holders by an irrevocable Proxy Agreement. Legal title to the shares remains with the non-U.S. citizen(s). All other provisions of the Voting Trust Agreement, as they apply 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 cleared U.S. organization's eligibility to have access to classified information or matter or to compete for classified contracts. Conditions for consideration of use of a Proxy Agreement are the same as required for a Voting Trust Agreement.

(3) Special Security Agreement. A Special Security Agreement may be considered when a U.S. organization is effectively owned or controlled by a non-U.S. citizen and the Federal Government has entered into a general security agreement with the foreign government involved.

(a) 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 industrial security and export control measures within an institutionalized set of corporate practices and

procedures. The Special Security Agreement requires the appointment of one or more outside directors who must be:

1 U.S. citizens residing within the United States;

2 completely disinterested individuals with no prior involvement with the applicant company, the corporate body with which it is affiliated, or the non-U.S. citizen;

3 approved by the Director, Office of Security; and

4 eligible for access authorization at the level of the FCL.

(b) A company cleared under a Special Security Agreement and its cleared employees may only be afforded access to proscribed information with special authorization. This special authorization must be manifested by a favorable National Interest Determination (NID) that must be program/project/contract-specific.

(4) Security and Export Control Oversight. The Voting Trust Agreement, Proxy Agreement, and Special Security Agreement, mentioned above in paragraphs 3b(1) through 3b(3), each requires that the following be established.

(a) Government Security Committee (GSC). As part of FOCI mitigation plan, the contractor is required to establish a permanent committee of its governing body, known as the GSC.

1 The GSC normally consists of voting trustees, proxy holders, or outside directors, as applicable, and those officers/directors who hold access authorizations (security clearances). The chairman of the GSC must be a trustee, proxy holder, or outside director, as applicable.

2 Members of the GSC must ensure that the company maintains policies and procedures to safeguard export-controlled information, classified information or matter, or SNM entrusted to it.

3 The GSC must take the necessary steps to ensure that the company complies with U.S. export control laws and regulations and does not take action adverse to its performance on classified contracts. This must include the appointment of a technology control officer (TCO) and the development, approval, and implementation of a technology control plan (TCP).

4 The facility security officer (FSO) must be the principal advisor to the GSC and attend GSC meetings. The chairman of the GSC must concur with the appointment of replacement FSOs selected by management. FSO and TCO functions must be carried out under the authority of the GSC.

(b) Visitation Approval Procedures. Policies and procedures governing visits between the foreign shareholder (including its affiliates) and the cleared U.S. organization must be developed and implemented by the GSC. The visitation approval procedures must be approved by the cognizant Federal agency.

A chronological file of all documentation associated with meetings, visitations, and communications between the cleared contractor and the excluded foreign affiliates, together with appropriate visit approvals or disapprovals and reports, must be maintained by the FSO for review by the DOE cognizant security authority during the annual FOCI compliance meeting.

(c) Technology Control Plan. The TCP developed and implemented by the company must be approved by the Federal agency clearing the company. The TCP must prescribe all security measures determined necessary to reasonably prevent the possibility of inadvertent access by non-U.S. citizen employees and visitors 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 appropriate Federal Government disclosure authorization has been obtained (e.g., an approved export license or Technical Assistance Agreement). The use of unique badging, escorts, segregated work areas, security training programs, or other measures must be documented in the TCP.

(5) National Interest Determination (NID). A special authorization (i.e., a NID) is required prior to providing proscribed information to a company cleared under a Special Security Agreement and its cleared employees. One of the eligibility requirements for clearance under a Special Security Agreement is that the Federal Government must have entered into a general security agreement with the foreign government involved. To be eligible for access to proscribed information, the U.S. Federal Government and the foreign government involved must have entered into an agreement that authorizes the exchange of the applicable proscribed information.

(a) A NID requires the following:

1 approval by the Secretary, Deputy Secretary, or cognizant Under Secretary. This approval may not be delegated;

2 preparation and sponsorship of the Contracting Officer;

3 coordination with the DOE cognizant security authority;

4 program/project justification specific to that contract; and

5 compelling evidence that release of proscribed information under the Special Security Agreement advances the national security interests of the United States.

(b) The request for a NID must include the following information:

1 the identification of the proposed awardee and a synopsis of its foreign ownership (include solicitation and other reference numbers to identify the action);

2 a general description of the procurement and performance requirements;

3 the identification of all national security interests involved and the ways in which award of the contract helps advance those interests;

4 the availability of any other U.S. company with the capacity, capability, and technical expertise to satisfy acquisition, technology base, or industrial base requirements and the reasons any such company should be denied the contract; and

5 a description of any alternate means available to satisfy the requirement, and the reasons alternative means are not acceptable.

c. Noncontrolling Foreign Ownership. A noncontrolling foreign ownership is one in which 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 noncontrolling foreign ownership or control, a FOCI mitigation plan may consist of one of the methods listed below.

(1) Board Resolution. When a non-U.S. citizen does not own voting stock sufficient to elect, or otherwise is not entitled to representation on the applicant company's governing body, a resolution(s) by the applicant's

governing body will normally be adequate. The board resolution acknowledging foreign ownership must:

(a) identify the foreign shareholder and describe the type and number of foreign-owned shares;

(b) acknowledge the organization's obligations to comply with all security program and export control requirements;

(c) certify that non-U.S. citizens will not require, will not have, and can be effectively precluded from, access to all classified information or matter, SNM, or hazardous material presenting a potential radiological, chemical, or biological sabotage threat entrusted to or held by the U.S. organization;

(d) certify that the non-U.S. citizens will not influence the organization's performance of contracts requiring access authorization(s); and

(e) provide for an annual (at least every 12 months) certification to the DOE cognizant security authority acknowledging the continued effectiveness of the resolution. In addition, the U.S. organization will be required to distribute to its directors and its principal officers copies of such resolutions and report in the corporate records the completion of such distribution. The U.S. organization must also ensure that the substance of the resolution(s) adopted by the governing body is brought to the attention of all of company personnel possessing or being processed for access authorizations.

(2) Security Control Agreement. A Security Control Agreement may be considered when a U.S. organization is NOT effectively owned or controlled by a non-U.S. citizen. Contract limitations on access to classified information or matter, or SNM are not required under this arrangement. Likewise, there is no requirement that the Federal Government must have entered into a general security agreement with the foreign government involved.

(a) For a Security Control Agreement to be used, the following information must be provided to the DOE cognizant security authority.

1 Identification of any employees (current and former) of the non-U.S. citizens involved (including all entities that control, are under common control with, or are controlled by the non-U.S. citizens, collectively the "foreign

affiliates") that will be transferred or become employees of the applicant seeking FCL.

2 Written documentation certified by an authorized (and appropriate) official(s) of the former employing organization(s) that states whether the transferred (or former) employee of the foreign affiliate has or has not severed all ties, and/or has or has not been given any guarantee, written or verbal, regarding re-employment by the foreign affiliates. This requirement only applies to employees who are U.S. citizens.

(b) The following are also requirements.

1 Appointment of one or more outside Directors who must meet the eligibility requirements set forth in paragraph 3b(1)(b) above.

2 Establishment of a GSC to oversee classified and export control matters. See paragraph 3b(4)(a) for further details concerning GSC establishment/responsibilities.

3 Development and implementation of a TCP that must be approved by the Federal agency clearing the company. See paragraph 3b(4)(c) above for TCP requirements.

d. Limited FCL.

(1) A limited FCL may be granted to certain contractors who are controlled or owned by a foreign interest where FOCI mitigation is not able to be implemented (e.g., sole source). Access limitations are inherent with granting limited FCLs.

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

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

2 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.

3 Release of classified information or matter must be in conformity with the U.S. national disclosure policy.

(b) A limited FCL may also be granted when the criteria listed in paragraph 3d(1) above cannot be satisfied, provided there exists a compelling need to do so consistent with national security interests.

(2) Each request for clearance under a limited FCL must be accompanied by a statement of compelling need from the government contracting activity (GCA). The GCA's compelling need statement must be signed by the Departmental element and include the following:

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

(b) acknowledgement that the GCA/Departmental element accept the risks inherent in the granting of an FCL where FOCI is not mitigated;

(c) a foreign disclosure determination (i.e., basis for determining that release of classified to the foreign government involved is in conformity with U.S. national disclosure policy).

4. ANNUAL COMPLIANCE MEETING. Representatives of the DOE cognizant security authority must meet annually (at least every 12 months) with senior management officials 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 how they will be implemented within the cleared organization. For the DOE cognizant security authority to make an overall evaluation/analysis of the effectiveness of the security arrangement, the DOE cognizant security authority must obtain an evaluation, before the annual meeting, from other DOE security authorities with cognizance over divisions or subsidiaries under the umbrella of the parent/home office FOCI agreement. Under normal circumstances, the annual meeting should be held at the cleared facility. These reviews must include an examination of the following items.

a. Acts of compliance or noncompliance with the approved security arrangement, standard rules, and applicable laws and regulations.

b. Problems or impediments associated with the practical application or utility of the security arrangement.

c. Whether security controls, practices, or procedures warrant adjustment.

5. NONCOMPLIANCE WITH MITIGATION PLANS. When the DOE cognizant security authority determines that a cleared contractor or its tier parent is out of compliance with the approved FOCI mitigation plan, the DOE cognizant security authority must analyze

and evaluate the overall impact to the protection of security interests. Actions to be taken by the DOE cognizant security authority include:

a. request for corrective action plan and implementation from the contractor;

b. recommendation to the DOE line management for FCL suspension; and

c. recommendation to DOE line management for FCL termination.

The cognizant contracting officer must be notified of any actions taken.

Vertical line denotes change.

SECTION H

APPENDIX 6—FOCI MATRIX CHART

Sole Proprietorship	Privately Owned Corporation	Publicly Traded Corporation	Partnership 1. General 2. Limited 3. Limited Liability	Limited Liability Company	College/University
Completed SF 328, Certificate Pertaining to Foreign Interests Form must be dated and signed by a person legally authorized to represent the business.	Completed SF 328, Certificate Pertaining to Foreign Interests Form must be executed under the corporate seal, dated and signed by a person legally authorized to represent the business.	Completed SF 328, Certificate Pertaining to Foreign Interests Form must be executed under corporation's seal, dated and signed by a person legally authorized to represent the business.	Completed SF 328, Certificate Pertaining to Foreign Interests Form must be dated and signed by a person legally authorized to represent the partnership.	Completed SF 328, Certificate Pertaining to Foreign Interests Form must be dated and signed by a person legally authorized to represent the business.	Completed SF 328, Certificate Pertaining to Foreign Interests Form must be dated and signed by a person legally authorized to represent the college/university.
Summary FOCI Data Sheet	Summary FOCI Data Sheet	Summary FOCI Data Sheet	Summary FOCI Data Sheet	Summary FOCI Data Sheet	Summary FOCI Data Sheet
Representative of Foreign Interest Statement [**when applicable**]	Representative of Foreign Interest Statement [**when applicable**]	Representative of Foreign Interest Statement [**when applicable**]	Representative of Foreign Interest Statement [**when applicable**]	Representative of Foreign Interest Statement [**when applicable**]	Representative of Foreign Interest Statement [**when applicable**]
List of key management personnel [13] In community property states, spousal information is also required on the key management personnel list. If single, so state.	List of key management personnel Stock ownership form (shareholder's form). If there is a Shareholders Agreement, a copy MUST be provided.	List of key management personnel Any authorizing resolutions of governing body that spell out authorities of the key management personnel.	List of key management personnel Stock ownership form (shareholders' form) MUST be provided if partnership has public stock.	List of key management personnel Any authorizing resolutions of the governing body that spell out the authorities of the key management personnel.	List of key management personnel Any authorizing resolutions of the governing body that spell out the authorities of the key management personnel.

[13]Formerly known as the Owners, Officers, Directors, and Executive Personnel (OODEP) List.

Sole Proprietorship	Privately Owned Corporation	Publicly Traded Corporation	**Partnership** **1. General** **2. Limited** **3. Limited Liability**	Limited Liability Company	College/University
State Registration to do business/Tax ID Number.	Certificate of Incorporation (also known as Corporate Charter). Articles of Incorporation (with all amendments).	Certificate of Incorporation (also known as Corporate Charter). Articles of incorporation (with all amendments).	1. **General** – Similar to a sole proprietorship; may only be able to provide Certificate of Fictitious Business Name. 2. **Limited** – Certificate of Limited Partnership. 3. **Limited Liability Partnership** - Certificate of Limited Liability Partnership.	Articles of Organization	College/university charter (similar to articles of incorporation).
	Bylaws (attested copy with all amendments).	Bylaws (attested copy with all amendments).	Partnership Agreement.	Operating agreement.	Charter (or similar document to company's bylaws).
Latest financial report or a copy of the 1040 for the previous year (including Schedule C). NOTE: The most recent IRS tax return may ONLY be submitted if the tax return includes the information required being included on a balance sheet and income statement, and the tax return is a copy of the entire return.	Consolidated financial information, including notes, for the most recently closed accounting year. (If audited report is not available, entity must certify to the unavailability of audited information.) If company stock is not publicly traded but the company has publicly-traded debt, submit the Form 10-K filed with the Securities and Exchange Commission (SEC) for the company's most recently closed accounting year.	Consolidated annual report to shareholders for the most recently closed accounting year. Form 10-K report, and all Form 10-Q reports for financial quarters filed (with the SEC) since the last annual report (Form 10-K).	If publicly traded, submit consolidated annual report to shareholders for most recently closed accounting year; also Form 10-K and Form 10-Q reports for financial quarters filed (with SEC) since the last annual report (Form 10-K). If not publicly traded, submit latest consolidated annual report or audited financial information, including notes, for most recently closed accounting year. (If audited report is not available, entity must certify to the unavailability of audited information.)	Consolidated financial information, including notes, for the most recently closed accounting year. (If audited report is not available, entity must certify to the unavailability of audited information.)	Consolidated financial information, including notes, for the most recently closed accounting year. (If audited report is not available, entity must certify to the unavailability of audited information.)

Sole Proprietorship	Privately Owned Corporation	Publicly Traded Corporation	**Partnership** **1. General** **2. Limited** **3. Limited Liability**	Limited Liability Company	College/University
	Most recent annual stockholders and board meeting minutes that identify directors and officers of corporation and company's voting list. Include any authorizing resolutions of governing body that spell out authorities of the key management personnel.		If required by the partnership agreement: The most recent Annual Stockholders and Board meeting minutes identifying directors and officers and company's voting list.		Most recent annual board meeting minutes identifying governing body and officers of the entity, and entity's voting list.

* FOCI determination is not required of self-employed individuals performing work under a consulting agreement.

** If applicable, each tier parent of the bidder must submit a complete package (i.e., information shown above for the applicable form of business).

*** A publicly traded entity is not required to provide all identifying information on its owners as required on the key management personnel list unless those individuals are key management personnel of the U.S. organization. Instead, submit: (i) most recent Proxy Statement for annual meeting of Shareholders; and (ii) most recent copies of Schedules 13D's and/or 13G's received from any beneficial owner (foreign or domestic) who holds 5 percent or more of the U.S. organization securities.

SECTION I—FACILITY CLEARANCES AND REGISTRATION OF SAFEGUARDS AND SECURITY ACTIVITIES

1. OBJECTIVE. To ensure that safeguards and security (S&S) activities are afforded proper levels of protection consistent with Departmental standards to prevent unacceptable impact to national security, the environment, or the health and safety of the public or employees.

CHAPTER I. FACILITY CLEARANCE (FCL) PROGRAM

1. GENERAL. The FCL program regulates Department of Energy (DOE) approval of a 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 worth more than $5 million, exclusive of facilities and land values (hereinafter referred to as security activities). The following delineates the primary requirements of the FCL program.

   a. Eligibility Requirements.

      (1) 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 the uncleared contractor. A contractor cannot sponsor themselves for an FCL.

      (2) The contractor or prospective contractor must meet the following eligibility requirements prior to being processed for an FCL. The contractor or prospective contractor must:

         (a) need an FCL in connection with a legitimate U.S. Government or foreign requirement;

         (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 (KMP) 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 common defense and national security. This requirement only applies when the contract awarded or to be awarded requires access authorizations.

b. An FCL must be granted before any nuclear or other hazardous materials presenting a potential radiological, chemical, or biological sabotage threat; classified information or matter; or property protection interests are placed on premises occupied by the Department or its contractors.

c. The cognizant security authority must establish and maintain FCLs by registering, updating, suspending, reinstating, and terminating security activities under their cognizance. Each registered FCL must identify the highest security activity approved for that facility.

d. The FCL for a prime contractor must include those instances where classified access will include subcontractors.

e. The Safeguards and Security Information Management System (SSIMS) must be used by all Departmental Elements to register FCL information for which they have cognizant security authority, survey cognizance, or registered security activities.

(1) DOE Form (F) 470.1 Contract Security Classification Specification (CSCS) is used to register information in SSIMS concerning contract vehicles [contracts, subcontracts, solicitations, purchase orders, Work for Others (WFO), leases, Cooperative Research and Development Agreements (CRADAs), etc.] that require access authorizations (personnel security clearances). If a DD Form 254 has been used by the agency sponsoring the activity, it can be submitted instead of the DOE F 470.1 CSCS provided it is annotated with the DOE facility code. DOE F 470.1 and DD Form 254 document specifics concerning each awarded contract (e.g., statement of work, classification, information pertaining to supplies, service, and other matters) to be furnished by the contractor to the government or by the government to the contractor.

(2) DOE F 470.2 “Facility Data and Approval Record” (FDAR) is used to record approvals, changes, and deletions of DOE Federal and DOE contractor security facility information.

(3) The cognizant security authority and surveying offices, as identified by DOE line management, must ensure that SSIMS reflects established facilities and security activities under their jurisdictions by submission of accurate CSCSs and FDARs.

(4) 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 authority. This responsibility may be delegated, by mutual agreement, to another Departmental element.

(5) Any change in the responsible DOE cognizant security authority must include a written transfer of appropriate documentation (e.g., S&S plans; construction project status; FOCI files).

f. Certain company officials must be granted access authorizations in order for a company to qualify for an FCL involving classified information or matter, or special nuclear material (SNM). These company officials include the owners, officers, directors, partners, regents, trustees, or executive personnel (i.e., those considered KMP).

g. A contractor that will not possess classified information or matter, or SNM at the contractor's place of business and will only access such security activities at other cleared facilities must be cleared as a "non-possessing facility." A non-possessing contractor must adhere to the security plans of the facilities where the contractor is afforded access to classified information or matter, or SNM. In addition, a separate security plan must be executed to cover the non-possessing contractor's security responsibilities.

h. A self-employed individual or consultant who will not retain classified information or matter at his/her place of business does not require FCL. For security administration activities, to include the processing for an access authorization, the consultant will be considered an employee of the facility where he/she is afforded access to classified information or matter. The consultant and the cognizant security authority must jointly execute a security plan that sets forth their respective security responsibilities.

(1) A self-employed individual or consultant who will retain classified information or matter at their place of business must be processed and granted an FCL that applies to the premises where the individual or consultant will store, handle, or process classified information or matter.

i. A contractor granted an FCL by another government agency (OGA) may be granted a DOE FCL for processing, using, or storing classified information or matter, based on reciprocity.

j. Verification of the clearance and security capability of an OGA must be based on written assurance from that agency. No classified information or matter may be given to the OGA until the OGA has submitted the required verification of its clearance and security capability and the DOE cognizant security authority has approved and registered an FCL for the OGA in SSIMS.

2. EXCEPTIONS TO REGISTRATION IN SSIMS. Foreign intelligence information, sensitive compartmented information (SCI), special access programs (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. Exceptions to the registration requirements are identified below.

a. SAPs. SAPs are not registered in SSIMS. SAPS are registered in accordance with DOE M 470.4-4, *Information Security.*

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 FDAR.

c. Cover Operations. Classified activities designated as "cover operations" (i.e., activities conducted in secrecy or concealment) are not registered in SSIMS as security activities (i.e., CSCSs). The cognizant security authority must notify the appropriate Departmental element before granting the FCL.

CHAPTER II. IMPORTANCE RATINGS

1. FACILITY IMPORTANCE RATINGS. Importance ratings are used to identify the protection importance of facilities. Each facility's assigned importance rating must be recorded on DOE F 470.2, FDAR. Importance rating criteria are as follows.

   a. "A" Importance Ratings. Ratings 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 Departmental element;

      (2) authorized to possess Top Secret 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. Ratings 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. Ratings 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. Ratings 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. Ratings assigned to a corporate tier parent (of a contractor organization) that has been barred from participation in the activities related to a contract with DOE.

f. "PP" (Property Protection) Importance Ratings. Ratings assigned to those facilities for which a special standard of protection must be applied. Basic considerations include physical protection to prevent or deter acts of arson, civil disorder, riots, sabotage, terrorism, vandalism, and theft or destruction of DOE property and facilities. These special standards are applied when a facility has:

(1) Government property of a significant monetary value (more than $5 million, exclusive of facilities and land values);

(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. Ratings assigned to those facilities that have authorized access to classified information or matter, or SNM at other approved locations. Non-possessing facilities do not themselves possess any classified information or matter, or SNM.

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 authority functions. Changes to the facility importance rating must be registered in SSIMS by the submission of DOE F 470.2, FDAR.

CHAPTER III. ORGANIZATIONAL STRUCTURES AND FCLs

1. FCL FOR SINGLE LEGAL ENTITIES.

   a. Single FCL Registration. Only one FCL registration is required if the company and its classified security activities meet the following criteria.

      (1) 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 single management control).

      (2) The distance between the security activities is such that the contractor is able to maintain daily supervision of its operations, including day-to-day observations of the security program.

   b. Multiple-Facility Registrations for Multiple-Facility Organizations (MFOs).

      (1) When a company is composed of two or more facilities existing as a single legal entity, the home office facility must have an FCL at the same or higher level of any cleared facility within an MFO.

      (2) When branches, divisions, etc. of an MFO are cleared, the corporate headquarters must be registered in SSIMS as the home office.

      (3) Each separate branch, division, etc., of an MFO performing a security activity requiring access authorizations must be processed for an FCL and registered in SSIMS. This FCL registration must reflect the branch or division location and reference the home office.[14]

      (4) Because branches, divisions, offices, etc., of an MFO are not legally accountable in their own right, only the home office facility can execute an agreement/contract with the Government.

      (5) A FOCI determination is not required of the subordinate facility of an MFO. However, a subordinate facility of an MFO must submit a list of its (not its home office's) KMP, and the subordinate facility's KMP must be cleared (and excluded, if applicable) as required by Chapter V of this section.

[14] A multiple facility organization may implement a consolidated security plan applicable throughout the organization, but the security plan must then be adapted as necessary to adequately address the requirements of each operating site.

2. PARENT – SUBSIDIARY RELATIONSHIP.

a. 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.

(1) 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.

(2) Because a subsidiary is legally accountable in its own right, the U.S. Government can permit the parent to remain uncleared or a subsidiary to hold an FCL of a higher level than the parent's.

(3) The DOE cognizant security authority is responsible for determining the necessity for the parent to be cleared:

(a) at the same level as the subsidiary;

OR

(b) at a lower level than the subsidiary;

OR

(c) excluded from access to all classified information or matter available to the subsidiary.

(4) The decision to clear or exclude must be based on:

(a) the parent's requirement for access authorizations to perform tasks or services essential to the fulfillment of a classified contract; and

(b) the parent's eligibility for an FCL, including its FOCI status. Information regarding FOCI negation action plans can be found in Section H.

b. When, pursuant to paragraph 2a(4), above, it is determined that the FOCI for a parent is acceptable, the parent can be either excluded altogether from the requirement for an FCL or excluded from higher-level access by virtue of possessing an FCL at a level below that of the subsidiary. This exclusion must be based on formal action by the governing bodies of the parent and each intervening subsidiary level. Compliance with one or both of the exclusion actions listed below, as applicable, is mandatory before issuance to a subsidiary of an FCL requiring access authorizations.

(1) Parent Organizations.

(a) The parent organization's board of directors (or similar governing body) must adopt a resolution, which cannot be amended or repealed without notification to DOE, that excludes the parent organization, the members of its board of directors, and its officers, employees, representatives, and agents, as such, from access to all classified information or matter, or nuclear and other hazardous material presenting a potential radiological, chemical, or biological sabotage threat or to a higher category of classified information or matter (specifically identified in the resolution) entrusted to or held by the cleared subsidiary.[15]

1 This action must be made a matter of record in the minutes of the board of directors (or similar executive body).

2 A copy of the resolution, dated and identified by the name and address of the organization, must be furnished to the DOE cognizant security authority.

(2) Subsidiaries. The board of directors of a subsidiary whose parent organization (all shareholder firms in the chain of ownership) has executed exclusion resolutions (paragraph 2b above) must adopt a resolution, which cannot be amended or repealed without notification to DOE, that excludes the parent organization(s) from access to classified information or matter, or nuclear and other hazardous material presenting a potential radiological, chemical, or biological sabotage threat, as applicable, and acknowledges (i.e., notes) the exclusion resolution adopted by the parent's board of directors (or similar governing body).

(a) This action must be made a matter of record in the minutes of the board of directors (or similar executive body), and must be furnished to the DOE cognizant security authority.

(b) A copy of the resolution, dated and identified by the name and address of the facility, must be furnished to the DOE cognizant security authority.

[15]The applicable board resolution must be completed by all shareholder firms in the chain of ownership.

CHAPTER IV. INTERIM AND LIMITED FCLs

1. INTERIM FCL. National policy permits the granting of an interim FCL to an eligible contractor. Interim FCLs are granted on a temporary basis, pending completion of full investigative requirements (i.e., final access authorization) for those individuals required to be cleared in connection with the FCL (e.g., KMP). Interim FCLs may be granted only to avoid unacceptable delays in pre-contract negotiation or in performance on a contract and after DOE has granted interim access authorizations to facility personnel requiring interim clearance.

   When final access authorizations have been granted to all facility employees, the DOE cognizant security authority must ensure that final FCL is granted and registered in SSIMS via an updated DOE F 470.2 FDAR.

   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.

   Foreign owned or controlled companies and non-U.S. citizens are not eligible for interim FCL.

2. LIMITED FCL. See Section H, Chapter IV, paragraph 3d, for eligibility criteria, etc., for a limited FCL.

   A limited FCL must be restricted to one security activity involving classified information or matter, or SNM. Award of another security activity involving classified information or matter, or SNM requires separate FCL registration (i.e., under an FCL without restrictions or another limited FCL provided the eligibility criteria set forth in Section H for such FCL are met).

   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 of KMP covered in Chapter V of this section apply to all FCLs, including a limited FCL.

CHAPTER V. ACCESS AUTHORIZATIONS AND EXCLUSION PROCEDURES REQUIRED IN CONNECTION WITH FCLs

1. ACCESS AUTHORIZATIONS REQUIRED IN CONNECTION WITH THE FCL. Certain officials [typically the owners, officers, directors, partners, regents, trustees, and/or executive personnel (KMP)] must be cleared to the level of the FCL and are listed below by type of organization. Based on their need for access, as determined by the DOE cognizant security authority, all other KMP must be cleared commensurate with the FCL level, cleared at a lower level, or excluded from being cleared. KMP exclusion determinations must be made prior to the granting of the FCL.

   a. Sole Proprietorships. The sole proprietor and the facility security officer (FSO) must be cleared commensurate with the FCL. Any KMP designated to succeed the sole proprietor or the FSO during permanent or temporary absence must be cleared commensurate with the FCL.

   b. Corporations, Nonprofit Organizations. The senior management official [i.e., president or chief executive officer (CEO)], chairman of the board, or (if meetings of the board of directors are chaired by a pro tem or rotating chairman), any board members who could serve as board chairman, and the FSO must be cleared commensurate with the FCL. Any KMP designated to succeed the senior management official, board chairman, or FSO during permanent or temporary absence must be cleared commensurate with the FCL.

   c. Partnerships. The managing partner and the FSO must be cleared commensurate with the FCL. Any partner designated to succeed the managing partner or the FSO during permanent or temporary absence must be cleared commensurate with the FCL.

   d. Colleges and Universities. The CEO, chairman of the board, or (if meetings of the board of regents, trustees, or directors are chaired by a pro tem or rotating chairman), any board members who could serve as board chairman, and the FSO must be cleared commensurate with the FCL. Any official or officer designated to succeed the CEO, board chairman, or FSO during permanent or temporary absence must be cleared commensurate with the FCL.

2. MULTIPLE FACILITY ORGANIZATIONS. Any of the business structures mentioned above may be configured as an MFO. Each subordinate facility's KMP must be cleared or excluded as required by paragraph 1 above. Subordinate facilities of an MFO must not be granted higher FCL or access authorizations than held by the home office of the MFO.

3. ACCESS AUTHORIZATIONS 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 access authorizations concurrent with the

FCL. The granting of an FCL is not dependent on the access authorization of such employees.

4. EXCLUSION PROCEDURES. Other officials, as determined by the DOE cognizant security authority, must be cleared commensurate with the FCL level, cleared at a lower level, or excluded from being cleared. When other 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. When formal exclusion action is required, the organization's governing body must affirm the following items.

   a. Such officers, directors, partners, regents, or trustees (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; can be denied access to higher level classified information or matter (specified by level) 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.

      (1) This action must be made a matter of record in the minutes of the governing body.

      (2) A copy of the resolution, dated and identified by the name and address of the facility, must be furnished to the DOE cognizant security authority.

CHAPTER VI. FACILITY CLEARANCE

1. REQUIREMENTS. As part of the DOE Facility Clearance (FCL) Program, facilities are evaluated against a set of requirements to determine their ability to meet Departmental protection standards.[16] Approval of an FCL by DOE is based on a favorable evaluation of all of the following requirements.

   a. DOE F 470.2 FDAR. Completion and registration in SSIMS of DOE F 470.2 FDAR.

   b. DOE F 470.1 CSCS. Completion and registration in SSIMS of DOE F 470.1 CSCS or similar form (e.g., DD F 254) for contractor/subcontractor facilities performing contracts, subcontracts, and other contractor solicitations that require access authorizations.

   c. Security Plan. The security plan describes the controls necessary within the facility to appropriately protect the security activities being performed. Such plans, which are approved by the DOE cognizant security authority, include, but are not limited to, at least one of the following:

      (1) a site safeguards and security plan (SSSP) as required by Section A or

      (2) a site security plan (SSP) as required by Section A.

   d. Survey.

      (1) For facilities with importance ratings of A, B, C, or PP, a comprehensive initial survey must be completed in accordance with Section G. The survey must result in a composite facility rating of "satisfactory" and be conducted no more than 6 months before granting the FCL.

      (2) Completion of an initial review for non-possessing facilities.

   e. FSO. The FSO must be an employee of the company. The FSO must be appointed in writing. As covered in Chapter V of this section, the FSO must be cleared commensurate with the FCL and concurrent with the issuance of the FCL. The FSO and others performing security duties must complete security training in accordance with Section J.

   f. FOCI. A favorable FOCI determination must be rendered in accordance with Section H. A counterintelligence (CI) threat assessment and technology transfer risk assessment must be obtained and considered prior to a final decision to grant

[16] Requirements for non-possessing facilities are covered in Chapter I, paragraph 1g, of this section. Requirements for self-employed individuals or consultants who will not possess classified matter at their places of business are covered in Chapter I, paragraph 1h, of this section.

an FCL to an applicant company under FOCI or to restore an FCL previously suspended because the contractor was determined to be under FOCI.

g. Nuclear Materials Management and Safeguards System (NMMSS). A reporting identification symbol code for NMMSS must be established for facilities authorized to possess SNM and a nuclear materials representative must be appointed in accordance with DOE M 470.4-6, *Nuclear Material Control and Accountability*.

h. Access Authorizations. Granting access authorizations for personnel in connection with the FCL (i.e., KMP) and, as appropriate, company employees requiring access to perform tasks or services related to the fulfillment of a classified contract.

i. Exclusions. Exclusion procedures must be invoked in accordance with Chapters III and V of this section.

2. ISSUANCE OF FCLs. After all requirements (as mentioned above) have been satisfactorily met, the DOE cognizant security authority will notify the contractor in writing of the level of FCL granted. See Chapter IV of this section for requirements on the issuance of an interim FCL.

3. CHANGED CONDITIONS AFFECTING THE FCL. Contractors must report events that will, or may have, an impact on the status of the FCL. (See Section H, Chapter III, paragraph 2.) It is the contractor's responsibility to ensure that any change that might affect the validity of the FCL is reported to the DOE cognizant security authority.

4. INTERFACE WITH FOCI REQUIREMENTS. Procedures must be in place to ensure that coordination is accomplished between the FCL and FOCI programs. This includes notification of FOCI determinations rendered for the company and its tier parents, updating of determination dates, suspension of FCLs, etc. (See Section H for a detailed discussion of the FOCI Program.)

CHAPTER VII. PROCESS FOR FCL AND SECURITY ACTIVITY REGISTRATION

1. ACCEPTING OGA FCLs.

a. Contractor. A contractor with an equal or higher FCL granted by OGAs 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 agreement before acceptance of the FCL [i.e., the requirements identified below must be documented in a letter or memorandum of agreement (MOA) between the DOE cognizant security authority and the cognizant OGA].

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

(a) A limited FCL granted by an OGA cannot be accepted.

(b) An interim FCL at the Secret or Confidential level granted by an OGA cannot be accepted.

(c) An interim Top Secret FCL granted by an OGA may be accepted once the following have been completed:

1 the DOE cognizant security authority has analyzed the conditions of the interim FCL and the scope for the DOE work and determined that the interim FCL status is acceptable.

2 an interim FCL may be withdrawn if the interim personnel security clearance for an individual (KMP) is withdrawn. When an interim personnel clearance is withdrawn, the interim FCL must also be withdrawn unless action is taken to remove the individual from the position requiring access.

3 until a final FCL has been granted, a contractor with an interim FCL may not be eligible for certain categories of classified information such as weapon data [RD, Formerly Restricted Data (FRD)], COMSEC, SCI, SAP, or North Atlantic Treaty Organization (NATO). The names of each individual granted temporary access authorization under the interim FCL are obtained from the OGA and submitted to the Director, Office of Security.

4 The Director, Office of Security confirms, after obtaining and reviewing the OGA's adjudicative files for each individual granted temporary access, that:

a the investigative standards used by the OGA satisfy DOE's requirements; and

b no unfavorable information was developed during the course of the OGA's adjudication.

(d) If cleared under a Voting Trust Agreement, Proxy Agreement, Special Security Agreement, or Security Control Agreement, the DOE cognizant security authority must obtain a copy of the FOCI mitigation plan from the cognizant OGA. The mitigation plan must be submitted for review by the Office of Security. The Office of Security must either determine that the FOCI mitigation plan is acceptable or ensure that additional measures required for the protection of DOE security activities are covered in an addendum to the agreement. This addendum must be signed by the Office of Security, the contractor, and its tier parents. Additional reviews by the Office of Security are required when changes are made to the mitigation plan. A copy of the signed addendum to the agreement must be provided to the OGA.

(e) For DOE contracts involving proscribed information, the following requirements, as appropriate, must be met before accepting an FCL cleared in conjunction with a special security agreement.

1 When the company is controlled by a foreign government:

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

b a waiver must be granted by the cognizant Secretary (i.e., the Secretary of Energy and/or the Secretary of Defense). This waiver is based on 10 U.S.C. 2536(a) Defense Authorization Act, which prohibits contract award involving proscribed information to foreign government-controlled companies; and

c the proposed Secretarial waiver must be prepared by the cognizant contracting officer, sponsored by the head of the contracting activity and appropriate Departmental element, and then forwarded through

appropriate Department channels for approval and/or coordination with all affected agencies.

2 When a company is not controlled by a foreign government, the following activities must be completed prior to contract award:

a a national interest determination (NID) for the specific program/project/contract must be approved by the cognizant DOE Departmental Element and/or OGA official(s);

b a proposed NID must be prepared by the cognizant contracting officer, sponsored by the head of the contracting activity and Departmental element, and then forwarded through appropriate Department channels for approval and/or coordination with all affected agencies.

3 For contracts involving RD/FRD, the additional requirements set forth below in paragraphs 1a(6)(a)–(d) have been met or addressed, as appropriate.

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

(3) Protective Measures. Confirmation is 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 is confirmed by the OGA, and assurance is 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 authority following each scheduled survey.

(5) Access Authorizations. Each employee to be granted access to DOE classified information or matter must have appropriate DOE access authorization or, at a minimum, a Federal personnel security clearance equivalent to the required DOE access authorization. Discrepancies must be reconciled through interagency coordination on a case-by-case basis.

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

(a) An assurance is obtained from the OGA that the facility complies with the requirements of Title 10 Code of Federal Regulations (CFR) Part 1045, *Nuclear Classification and Declassification*.

(b) When the DOE contract involves RD classified at the Secret level or above, an assurance is obtained from the OGA that the facility's protective measures and procedures meet the requirements of the supplement to the National Industrial Security Program Operating Manual (NISPOM).

(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 will be accepting an FCL based on a DoD-approved Voting Trust Agreement, Proxy Agreement, Special Security Agreement, or Security Control Agreement, an assurance is obtained from the OGA that it will invite or 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 FCL holds an FCL granted by another Federal agency, the tier parent(s) does not need to provide DOE with a FOCI package provided the following reciprocity is accomplished with the OGA. Reciprocity between the DOE cognizant security authority and the OGA must be documented in a written agreement prior to DOE granting the subsidiary FCL. The written agreement must contain the requirements listed below.

(1) Classification Level/Category.

(a) When the FCL granted to a tier parent by an OGA is equal to the level of FCL required by the subsidiary, an assurance is obtained from the OGA that the DOE cognizant security authority will be notified prior to any reduction or increase to the level of the OGA-issued FCL that would require parent/subsidiary exclusion resolutions be invoked.

(b) If the FCL granted to a tier parent by an OGA is as an excluded parent or is lower or higher than the FCL required by the subsidiary, DOE must have the subsidiary and its tier parent(s) invoke the required exclusion resolutions.

(2) Validation of the Subsidiary's SF 328. The DOE cognizant security authority must provide the cognizant OGA with a copy of the subsidiary's executed SF 328, and the subsidiary's listing of KMP positions and personnel.

(a) Confirmation must be obtained from the OGA as to whether the agency determined if the tier parent's FOCI package(s) disclosed any FOCI issue(s) applicable to the subsidiary to be cleared by DOE.

(b) An assurance is obtained from the OGA that the DOE cognizant security authority will be notified if any FOCI issue(s) are subsequently reported to or identified by the OGA that will or might affect the DOE-granted subsidiary FCL.

(3) Transfer of Security Cognizance. An assurance must be obtained from the OGA that security cognizance will be transferred to DOE for any tier parent no longer requiring 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 FDAR must be provided.

3. REGISTERING OGA FCLs.

a. An OGA may be registered with an FCL in SSIMS when a mission or programmatic need has been established by DOE line management. The DOE cognizant security authority must obtain a written statement of security assurance from the OGA. This statement must include the following information:

(1) an approved classified mailing address for the facility;

(2) the highest level and category of classified information or matter the facility is authorized to receive and store;

(3) reflect that classified information or matter will be afforded protection according to Executive Order 12958, *National Security Information*, and its implementing Information Security Oversight Office Directives;

(4) the requirements of Title 10 CFR Part 1045, *Nuclear Classification and Declassification*, will be met for RD and FRD; and

(5) the requirements of the Atomic Energy Act, including the mandatory access authorization (personnel security clearance) requirements, will be met for access to RD and FRD.

b. When RD or FRD is involved, the written assurance must include procedures to limit the manner in which the RD/FRD data are to be disseminated.

4. REGISTRATION OF OGA CONTRACTORS IN SSIMS. Classified mail channels must be registered in SSIMS for an OGA contractor organization where the Department does not have a contractual interest. 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 cognizant security authority and by the authorizing government official for the OGA contractor.

   Once the form is completed, the information must be entered into SSIMS. This process may only be used when the contractor facility has been approved by another Government agency and registered in SSIMS. NOTE: Such an FCL cannot be used as a basis for registering additional security activities.

5. 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.

   a. WFO Performed at DOE-Owned or DOE-Operated Facilities.

      (1) OGAs' WFO activities must be based on a determination that the S&S measures to be provided are consistent with DOE policy.

         (a) Before acceptance of WFO activities, the Department and the requesting agency must exchange classification and protection information, including the DD F 254 (or a form similar in content).

         (b) 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.

         (c) These activities must be registered in SSIMS.

      (2) When subcontracting is required in connection with WFO, the subcontractor can be registered based on DOE F 470.2 FDAR and verification of the FCL. In this instance, a security cognizance agreement is not required.

         (a) If the subcontractor has a DOE FCL at the appropriate level, the WFO activity must be registered.

         (b) If the subcontractor has an FCL issued by an OGA, see paragraph 5a(1), above.

         (c) If the subcontractor has no FCL or the FCL is at a lower level than required, see the requirements in paragraph 6 of this chapter.

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. 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. Additionally, the following actions must be completed and documented.

(1) Verification that the FCL for the location where the work is to be performed meets or exceeds the level of clearance required for the WFO activity.

(2) Review and certification that the sponsoring organization has either provided the classification guidance or has stated in writing that the non-DOE-funded work will not entail classified activities as required by DOE M 475.1-1A, *Identifying Classified Information*, dated 2-26-01.

(3) Verification that classified security activities [i.e., those requiring access authorizations (personnel security clearances)] have been recorded as security interests on a DD F 254 (or a form similar in content).

(4) Execution of an agreement between DOE and the other agency with respect to reimbursement for any additional S&S costs incurred by DOE.

(5) The activity must be registered in SSIMS.

6. REGISTRATION OF DOE FCLs. The DOE cognizant security authority must grant an FCL for all DOE and DOE contractor facilities in accordance with the requirements of Chapter I of this section.

a. Actions. The DOE cognizant security authority must perform the following activities.

(1) Initial Registration. The DOE F 470.2 FDAR must be completed and registered in SSIMS.

(2) Modifications. Significant facility changes (e.g., a change in name, address, DOE cognizant security authority, classified mailing/shipping address, SNM categorization, or classification level/category of information authorized) must be documented on an updated DOE F 470.2 FDAR and updated in SSIMS.

(3) Suspensions. When the following conditions occur, the DOE cognizant security authority must suspend the FCL and document this action on an updated DOE F 470.2 FDAR and update SSIMS.

(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 the requirements in paragraphs 6a(3)(b)1 and 2, below, are met. (See Section H for applicable FOCI requirements.)

1 When findings or other deficiencies indicate suspension of an FCL is necessary, the Departmental element, in coordination with the DOE cognizant security authority, may suspend the FCL pending validated corrective actions.

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

a The facility subject to the suspension action must first be notified in writing that:

i. its FCL has been suspended, including the reason for the suspension;

ii. award of new classified contracts to the facility will not be permitted until the facility has been restored to a fully valid status; and

iii. termination of FCL may result if the security issues causing the suspension are not rectified within a time frame and manner specified by DOE line management.

b GCAs must make the final decision regarding a contractor's continued performance of existing contracts and possession of classified information or matter, or SNM associated with those contracts or otherwise retained under GCA authorizations.

c All affected DOE elements and, if applicable, separate OGAs must be notified by the DOE cognizant security authority.

(b) In accordance with the intent of 10 U.S.C. 2536(a), 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 for national security interest contracts or for environmental restoration, remediation, or waste management contracts that involve proscribed information may only continue under FCL suspension if:

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

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

(4) Reinstatement of a Suspended FCL. When the conditions that resulted in the suspension have been resolved in a manner determined acceptable by DOE line management, the FCL may be reinstated. This reinstatement must be based on the necessity to complete or continue work associated with the original FCL. The DOE cognizant security authority must complete a DOE F 470.2 FDAR and update SSIMS to enact the reinstatement.

(5) Termination. The DOE cognizant security authority must complete a termination survey, a DOE F 470.2 FDAR, and update SSIMS to enact the termination.

(6) Reactivation. Reactivations of terminated FCLs must be based on programmatic or mission need and the implementation of current security requirements. The DOE cognizant security authority must validate that all security requirements have been implemented, complete a DOE F 470.2 FDAR, and update SSIMS to enact the reactivation.

(7) Subcontracts. When a subcontract is established between a DOE prime contractor and another contractor for work involving access authorizations, classified information or matter, or nuclear and other hazardous material presenting a potential radiological, chemical or biological sabotage threat, the prime contractor is responsible for ensuring the DOE F 470.2 FDAR is accurate and current. The prime contactor must submit the request for a subcontractor FCL and associated DOE F 470.2 to the DOE cognizant security authority for action.

(8) Records. The DOE cognizant security authority must maintain a copy of the facility's S&S plans, survey reports, notification of a favorable FOCI determination, if applicable, and pertinent correspondence with the DOE

F 470.2 FDAR created for the facility. For FCL termination, a copy of the certificate of non-possession must be maintained.

7. REGISTRATION OF SECURITY ACTIVITIES. Security activities are specific, unrelated tasks or contract elements involving security interests at a facility. Security activities must be registered in association with a specific FCL. The DOE cognizant security authority must ensure that each security activity is recorded on DOE F 470.1 CSCS and registered in SSIMS. If a DD F 254 has been used by the OGA sponsoring the activity, it will be annotated with the DOE facility code, if applicable and submitted instead of the DOE F 470.1 CSCS.

a. Security Activities for Existing FCLs. The DOE cognizant security authority must perform the following actions.

(1) Determine and validate the security requirements, including access authorizations, for the proposed security activity.

(2) Determine the FCL status through SSIMS or the DSS/CVA.

(3) Compare the security requirements for the activity to the approved FCL in the following situations.

(a) When the contractor FCL is granted by an OGA, the requirements of paragraph 1 of this chapter must be met.

(b) When the contractor FCL is granted by DOE, the requirements listed below must be met.

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 applicable cognizant security agency (i.e., DOE cognizant security authority and/or OGA) in the manner set forth in paragraph 1b of this chapter for any tier parent(s) of the contractor holding a DOE or OGA FCL (i.e., FCL granted by the agency that rendered the FOCI determination).[17]

[17]Coordination is required to ensure compliance with national requirements [e.g., fulfill the government's responsibility to validate and verify the company's foreign ownership, control, or influence to determine its initial and continuing eligibility for a facility clearance (FCL), ensure that exclusion resolutions are invoked when the parent organization either holds no FCL or holds an FCL at a lower level than the subsidiary].

b. Registering New Security Activities.

(1) The procurement request originator must prepare a DOE F 470.1 CSCS or submit a DD F 254 to the DOE contracting official. The DOE contracting official must forward the completed DOE F 470.1 CSCS or DD F 254 to the DOE cognizant security authority. Once the DOE F 470.1 CSCS or DD F 254 has been signed by the DOE cognizant security authority and returned to the contracting officer, the contract can be awarded.

(2) When a new activity will exceed the current FCL or an FCL does not exist, the actions required to upgrade the current level or obtain an FCL must be completed as appropriate (these actions are detailed in paragraph 6 of this chapter). Upgrading an FCL may also require transfer of DOE cognizant security authority functions.

c. Changing Security Activity Information. The DOE cognizant security authority who established the security activity is responsible for updating and changing security activity information. Changes must be registered in SSIMS through submission of an updated DOE F 470.1 CSCS or DD F 254.

d. Terminating Security Activities. When a registered security activity is terminated, the organization that established the security activity must ensure that all affected access authorizations are 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 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 facility and maintained by the DOE office that established the security activity. SSIMS must then be updated to reflect the change in status.

SECTION J—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. The Department of Energy (DOE) National Training Center (NTC) provides assistance and resources for the development and instructional needs for security and safety.

2. REQUIREMENTS.

   a. Key Program Elements. The S&S Training Program must encompass the following key S&S program elements.

      (1) Program Planning and Management,

      (2) Personnel Security,

      (3) Physical Protection,

      (4) Protective Force (PF),

      (5) Nuclear Material Control and Accountability,

      (6) Information Security.

   b. Job Analysis. A job analysis must identify, describe, and document major task and skill requirements.

   c. Testing. Knowledge- and/or performance-based testing must be used to measure the knowledge and/or skills acquired from training programs.

   d. Training Content. 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. Performance testing of individual and small unit tactics must be performed as part of initial, refresher, and on-the-job training for the PF.

   e. Training Course Development. A systematic approach must be used to produce training products that ensure the individual acquires the knowledge and skills necessary to perform their assigned duties. The approach used must have the following phases: analysis, design, development, implementation, and evaluation.

      (1) Analyses. Analyses must be conducted to ensure that training courses reflect the requirements of the job competencies. Training requirements must be determined by analyzing needs, the job or function, or performance deficiencies.

Vertical line denotes change.

(a) Needs analyses must be conducted in response to identified performance problems to validate the need for training.

(b) Job analyses must identify critical tasks. Job analyses will determine the frequency and method of training.

(c) Analysis must include determination of delivery method to ensure the most effective training outcomes (i.e., Web-based training, interactive television, classroom-based, or a combination of delivery methodologies).

(2) Design. Instructional objectives must be developed based upon the skills and knowledge associated with a task and must form the basis for the development of all training materials, tests, and strategies.

(3) Development.

(a) Lesson plans must reflect instructional objectives to ensure consistent achievement of those objectives each time the course is taught.

(b) Course design documents and training materials used to support instructional objectives must be technically accurate and current.

(4) Implementation.

(a) Training will be conducted using certified instructors who have appropriate experience and/or training to ensure the accomplishment of instructional objectives. Instructor certification will be obtained through the DOE NTC. Instructors will be recertified at least once every 2 years (at least every 24 months) to maintain technical proficiency.

(b) Qualified personnel whose past experience in training is such that they may be exempted from training may be allowed to do so on a case-by-case basis through testing or equivalency. When testing is used for this purpose, it will consist of the same or equivalent examinations based on instructional objectives as stated for the required training course.

(c) Completion of testing or granting of equivalency will be documented in the training records system.

(5) Evaluations. Evaluations of training must be performed to ensure that instructional objectives are met and to determine the overall effectiveness.

f. Training Approval Program (TAP). A TAP is a process to ensure that established objectives, standards, and criteria are met by validating, through the Office of Security, security training programs conducted by organizations other than the NTC.

(1) Upon the request of the Departmental element the NTC will certify site implementation of NTC-developed courses.

(2) Site programs must be examined by representatives of the NTC every 5 years (at least every 60 months) to verify adherence to Departmental training objectives and standards and to provide program approval recommendations to the Director, Office of Security.

(3) Initial and recurring reviews for training approval must cover all aspects of local training programs including program management and structure, course content, training facilities, observation of course presentations for effectiveness, and evaluation of students.

(4) Training approvals will remain valid for a period of 5 years.

(5) TAPs must be re-evaluated and resubmitted for approval based upon significant changes in operational missions or conditions

g. Training Records Management.

(1) Training records must be maintained.

(2) Training records must contain dates of course attendance, course title, and scores/grades achieved, where applicable.

(3) Training records may be retained in electronic or hardcopy form.

(a) Training provided at the NTC must be recorded by the NTC and the organization sponsoring the individual.

(b) Records of training provided at other facilities, including contractor or other government facilities, must be provided to and retained by the organization sponsoring the individual.

h. Training Plans. Training plans that project training derived from a valid needs analysis for the forthcoming year must be developed annually for each program element. Annual training plans must be approved by the DOE cognizant security authority and must address:

(1) training needs analysis,

(2) critical needs, or those immediate training needs which when met will be effective at improving organizational and workforce performance,

(3) training goals and objectives,

(4) major training delivery programs, projects, and other significant activities,

(5) mandatory training and qualifications for compliance with DOE requirements and any additional requirements directed by DOE line management.

SECTION K—SAFEGUARDS AND SECURITY AWARENESS PROGRAMS

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

2. REQUIREMENTS.

   a. Briefings. S&S awareness programs must include:

      (1) an initial briefing for all DOE Federal and contractor employees;

      (2) comprehensive, refresher, and termination briefings for all Federal and contractor employees and personnel granted Department of Energy (DOE) access authorizations.

      (3) appropriate awareness briefings for any non-DOE personnel granted unescorted access to Departmental security areas (e.g., regarding information on prohibited articles).

   b. Classified Information Nondisclosure Agreement (SF 312). An individual granted a DOE access authorization must execute a "Classified Information Nondisclosure Agreement" (SF 312) or otherwise comply with 32 CFR, Chapter XX, before being granted access to classified information or matter.

   c. Supplementary Awareness Activities. S&S awareness programs must include supplementary activities to keep individuals aware of their responsibilities.

3. PROGRAM DESIGN AND DEVELOPMENT.

   a. Program Design. S&S awareness programs must include objectives designed to meet site-specific needs and Federal requirements, and ensure cleared and uncleared personnel are continuously aware of their S&S responsibilities.

   b. Program Development. Procedures must be developed to ensure implementation of all S&S awareness program requirements.

   c. Program Assessment. S&S awareness programs must be assessed in accordance with Section G.

4. BRIEFINGS. S&S awareness briefings for cleared personnel must address site-specific needs, S&S interests, and potential threats to the facility/organization. Contents must be updated as necessary. Records must be maintained in a manner that provides an audit trail that verifies an individual's receipt of the briefings.

   a. Initial Briefing. Personnel who receive a DOE security badge must receive an initial briefing before they are given unescorted access.

(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 unclassified controlled information;

(h) procedures for reporting incidents of security concerns (e.g., attempts to gain unauthorized access 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 an access authorization 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) Classification and declassification requirements and procedures:

1 definition of classified information or matter,

2 purpose of DOE classification and declassification program,

3 levels and categories of classified information or matter,

4 damage criteria associated with each classification level,

5 authority for classification and declassification, and

6 procedures for challenging the classification status of 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 unclassified controlled information, including telecommunications and electronic transmissions;

8 information pertaining to security badges, access authorization 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.

(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 an access authorization is extended or transferred to another DOE facility/organization. Initial and comprehensive briefings may, at the discretion of line management, be combined only if the access authorization has been extended. 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 may be used to document this briefing.

c. Refresher Briefing. Cleared individuals must receive annual (at least every 12 months) 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.

(1) Content. Refresher briefings must selectively reinforce the information provided in the comprehensive briefing. Refresher briefings must also address current facility-/organization-specific S&S issues and counterintelligence (CI) awareness. The CI awareness component should use material on this topic prepared annually (at least every 12 months) by the NTC or developed in coordination with the local CI Office.

(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 briefings. 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 an access authorization 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 authority or to the DOE.

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

(a) information contained in items 1 through 6 of the "Security Termination Statement" Form (DOE F 5631.29);

(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 of 1954 and 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

an access authorization, 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) 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.

5. 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.

(2) Any individual who refuses to execute an agreement must be denied access to classified information or matter and reported to the cognizant security authority.

(3) Any DOE employee can witness a DOE or contractor employee's agreement, but only an authorized DOE employee may accept a DOE employee's agreement. An authorized DOE employee may also accept a contractor employee's agreement, or a contractor representative may be authorized in writing by the DOE cognizant security authority to witness and to accept an agreement from a contractor employee on behalf of the U.S. Government.

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. The cognizant security authority must ensure SF 312s retained by contractors are sent to DOE upon the terminations of employment of contractor employees.

c. Storage. The SF 312 must be stored in accordance with GRS 18, item 25, as supplemented by the DOE Administrative Records Schedule. Personnel security files must not be used as a storage location for the agreements. 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.

6. SUPPLEMENTARY AWARENESS ACTIVITIES.

a. Purpose. Supplementary S&S awareness activities must be provided between annual (at least every 12 months) and refresher briefings to ensure that individuals are aware of their S&S responsibilities.

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

SECTION L—CONTROL OF CLASSIFIED VISITS PROGRAM

1. OBJECTIVE. To ensure that only persons with the appropriate access authorizations and need-to-know receive access to classified information or matter in connection with visits involving the release or exchange of classified information or matter.

2. REQUIREMENTS.

   a. Procedures. Line management must establish local procedures for the control of classified visits. Procedures must ensure the following actions.

      (1) Verification of the visitor's identity, programmatic need-to-know, and that the visitor's clearance or access authorization is at least equal to the classification of the information to which access is being requested.

      (2) Identification of limitations and enforcement of controls for access to classified information or matter or facilities and submission of appropriate forms, requests, etc., to the cognizant security authority and programmatic line management within the timeframes below.

         (a) Visit requests must be submitted at least 15 working days before the date of a one-time visit or the first day of a recurring visit.

            1 Department of Energy (DOE) and DOE Contractor Employees. DOE Form (F) 5631.20, "Request for Visit or Access Approval," must be used by DOE Federal and contractor employees to obtain programmatic approval for Sigma access. This form does not need to be submitted to visit Department facilities. A DOE security badge will serve as evidence of DOE access authorization.

            2 Other Government Agency (OGA) and OGA Contractor Employees. DOE F 5631.20 (or form similar in content) must be used by employees of OGAs to obtain access approval for visits to DOE facilities.

         (b) Exceptions to required processing times will be allowed only for emergency visits (i.e., visits that must take place as a matter of urgency and importance and the processing lead time cannot be met). Emergency visits will only be approved as one-time visits.

         (c) Requests for visits/access to weapons programs, nuclear materials production facilities, or sensitive nuclear materials production information must be referred to the Associate Administrator for Defense Nuclear Security.

(d) Requests for visits/access to uranium enrichment plants or facilities engaged in uranium enrichment technology development, including advanced isotope separation technology, must be referred to the Office of Nuclear Energy, Science and Technology.

(e) Requests for access to Naval Nuclear Propulsion facilities must be referred to the Deputy Administrator for Naval Reactors.

(3) Continuing visitor access approval is necessary for individuals who frequently visit DOE facilities. However, the access approval cannot exceed a period of 1 year or the final day of a contract for contractors, whichever is less. The approval may be renewed annually (at least every 12 months).

(4) Operational approval of visits.

(5) Maintenance of documentation associated with all classified visits/access.

(a) Records of classified visits by employees and contractors of OGAs must be maintained.

(b) Records of classified visits by DOE Federal and contractor employees that entailed Sigma access must be maintained.

(c) Records of requests for classified visits by DOE Federal and contractor employees to OGAs must be maintained.

(6) Referral of any nonroutine, written, or visual material resulting from classified visits and proposed for public release to the Director, Public Affairs.

(7) Limiting the sending and receiving of a classified visit request to the security office of OGAs.

b. Classified Visits by Departmental Employees, Contractors, and Subcontractors.

(1) Visitors are responsible for making administrative arrangements and obtaining approval from the Departmental element, as appropriate. (The authority granting such approval is responsible for informing the facility to be visited.)

(2) Contractors or subcontractors with mutual program interests may be authorized, subject to the limitations in paragraph 2b(3), below, to arrange for visits without obtaining Departmental approval if such authorization will be advantageous to the Department.

(3) Visitors who require access to weapon data (classified Secret or Top Secret), Top Secret information (non-weapon data), 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.

(a) Facility Visits. When the classified visit is under the auspices of a Departmental element, the programmatic approval for the visit must be obtained from the Departmental element exercising jurisdiction over the facility.

(b) Headquarters Visits. When the classified visit is under the auspices of line management, the programmatic approval for the visit must be obtained from both the responsible line management and the Departmental element being visited.

c. Visits to Department of Defense (DoD) and National Aeronautics and Space Administration (NASA) Facilities. Both agencies accept DOE access authorizations for Restricted Data (RD) and other classified information or matter under their jurisdictions on the same basis as the Department, if access authorization and need to know are properly certified.

(1) DOE Top Secret approvals must be specifically certified in the event access to Top Secret information is required.

(2) A DOE F 5631.20 must be forwarded directly to the military or civilian official with jurisdiction over the information to which access is being requested.

(3) Any exchange of RD occurring during the course of a visit must be accomplished as stated in paragraph 2e below.

d. RD Visits by Nuclear Regulatory Commission (NRC) Employees.

(1) Visits to DOE facilities 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 Department classified weapon or production facility must:

(a) be arranged through the Departmental element coordinating the visit;

(b) have prior approval of the Associate Administrator for Defense Nuclear Security if visiting classified weapon or production facilities; and

(c) have necessary clearance verification and certification by the NRC Director of Security that access to the information requested is required in performance of official duties.

(2) Visits involving access to RD not requiring prior approval from the Departmental element exercising jurisdiction over the facility or the office to be visited may be arranged directly by NRC with the Departmental element provided this procedure does not conflict with the existing visitor control procedures of the cognizant security authority.

(3) The NRC identification badge must not be used as authority for visits in lieu of the aforementioned specific visit approval arrangements.

e. RD Visits by DoD and NASA Employees.

(1) Access to RD is contingent upon submission of a DOE F 5631.20; NASA Form 405, Request for Access Approval; or a memorandum or electronic message signed by or in the name of the certifying official. The request must be forwarded for approval or other action to the Departmental element with jurisdiction over the information to which access is requested.

(2) Requests for access must include the following:

(a) names, citizenship, dates of birth, and social security numbers of persons requesting access and organizations represented (if not Armed Services, relationship to DoD or NASA);

(b) facility and information to which access is requested (access to critical nuclear weapon design information must be specified as requested);

(c) security clearance or access authorization status of each person, including clearance date;

(d) purpose of visit and certification that the person needs the access in the performance of duty;

(e) anticipated date of visit and names of persons to be visited (if a conference is involved, the date, place, and sponsor of the conference must be specified); and

(f) a certification that the matter to which access is requested relates to aeronautical and space activities, for requests from NASA.

(3) The approving official must have the authority to approve such access.

(4) Control of access to RD in the custody of another Federal agency by members of the Armed Services or by DoD or NASA personnel or contractors is the responsibility of the appropriate official or his/her designee (see Appendix 7, Access to Restricted Data in Possession of Other Federal Agencies, for a listing of those officials).

(5) Departmental elements must retain a copy of each visit request they have approved for 3 years. Separate records must be maintained for access approvals issued under emergency conditions.

f. Other Classified Visits by DoD and NASA Employees.

(1) Requests for such visits to DOE, contractor, and subcontractor facilities are approved by line management, or in the case of Headquarters elements, by the cognizant Departmental element after ensuring that each visitor has the appropriate military or NASA security clearance and requires the information in the performance of their duties.

(2) Certification of security clearances may be made by memorandum, electronic message, DOE F 5631.20 or NASA Form 405.

g. Classified Visits by Employees of OGAs.

(1) Requests for visits to DOE facilities by employees, contractors, or subcontractors of Federal agencies other than DoD, NASA, or NRC are approved by the cognizant security authority.

(2) RD may not be exchanged with persons in this category unless they have appropriate DOE access authorization.

(3) Classified information or matter, other than RD, may be exchanged provided the individual has the appropriate Q or L access authorization or a security clearance granted under the provisions of Executive Order 12968, *Access to Classified Information*, and need for such access has been verified.

(4) Certification of security clearances for RD access must be made on DOE F 5631.20.

h. Congressional and State Classified Visits. Requests for visits to DOE, contractor, or subcontractor facilities by members or employees of Congress or congressional committees and by governors or their staffs must be approved by the

Vertical line denotes change.

Departmental element with jurisdiction over the facilities to be visited, provided the following are verified:

(1) visitor's identity;

(2) access authorization or security clearance; and

(3) need-to-know.

i. Emergency Visits to Classified Areas and Facilities.

(1) In an emergency, requests for visit approval may be made by telephone or electronic message.

(2) Telephonic requests must be confirmed by memorandum or electronic message.

j. Classified Visits to DOE Facilities by Non-U.S. Citizens. The exchange of classified information or matter with non-U.S. citizens, whether through visits to DOE or contractor facilities or foreign travel by DOE employees or contractors, is covered in DOE O 142.1, *Classified Visits Involving Foreign Nationals*, dated 1-13-04.

SECTION L

APPENDIX 7—ACCESS TO RESTRICTED DATA IN POSSESSION OF OTHER FEDERAL AGENCIES

The following Federal officials are authorized to permit their Federal and contractor employees with DOE access authorizations to grant access to RD in their possession to members of the Armed Forces and DoD and NASA employees and their contractors, in accordance with Title 42 U.S.C. Section 2163 and 2455(b).

- The Assistant to the President
- Director, Office of Management and Budget
- Executive Secretary, National Security Council
- Director, Central Intelligence Agency
- Director, Federal Emergency Management Agency
- Secretary, Department of Homeland Security
- Secretary of State
- Secretary of the Treasury
- Attorney General of the United States
- Secretary of the Interior
- Secretary of Agriculture
- Secretary of Commerce
- Secretary of Labor
- Secretary of Health and Human Services
- Secretary of Transportation
- Secretary of Education
- Chairman, Federal Communications Commission
- Administrator, Agency for International Development
- President, National Academy of Sciences and National Research Council
- Director, National Science Foundation
- Chairman, Tennessee Valley Authority
- Director, United States Information Agency
- Comptroller General of the United States

Vertical line denotes change.

SECTION M—DEVIATIONS

1. OBJECTIVE. To establish procedures, coordination, and approval levels that must be applied to any deviations from Department of Energy (DOE) safeguards and security (S&S) program directive requirements.

2. REQUIREMENTS. There are 3 categories of deviations: variances; waivers; and exceptions. Deviations from S&S program directive requirements require approval before implementation. Table M-1, Deviation Approval Process, depicts the approval level required for the various types of deviations.

   a. Deviations. Deviations from S&S program directive requirements require approval before implementation. Table M-1, Deviation Approval Process, depicts the approval level required for the various types of deviations. Coordination, approval, and duration limits are as follows.

Table M-1. Deviation Approval Process.

Deviation	Approval Level			
	Related to Protection of Category I and II Quantities of SNM	Related to Other S&S Program Directive Requirements (excludes Exceptions to SECON, see Part 1, Section B)		
		Field	NNSA HQ	Non-NNSA HQ
Variance: Approved conditions that technically vary from S&S directives' requirement, but afford equivalent levels of protection **without compensatory measures**.	**Departmental element** cc: SO	**DOE cognizant security authority** cc: SO, Departmental element, and Associate Administrator for Defense Nuclear Security for NNSA	**Cognizant Deputy Administrator** Concurrence of Associate Administrator for Defense Nuclear Security cc: SO	**Departmental element** SO Concurrence
Waiver: Deviation from S&S directive that **requires compensatory measures** to preclude potential or real vulnerability.	**Under Secretary for Nuclear Security** (for NNSA sites) **Under Secretary for Energy, Science, and Environment** (for non-NNSA sites) cc: SO	**DOE cognizant security authority** With 30-day advance notice to SO and, for NNSA facilities, Associate Administrator for Defense Nuclear Security	**Cognizant Deputy Administrator** With 30-day advance notice to and concurrence of Associate Administrator for Defense Nuclear Security	**Departmental element** SO Concurrence
Exception: Deviation creating vulnerability for which there are no adequate compensatory measures.	**Secretary of Energy** or **Deputy Secretary of Energy** cc: SO	**Under Secretary for Nuclear Security** (for NNSA Sites) **Under Secretary for Energy, Science, and Environment** (for non-NNSA sites) with concurrence of Departmental element cc: SO	**Deputy Secretary** SO Concurrence	**Deputy Secretary** SO Concurrence

   (1) Variances. Variances are approved conditions that technically vary from an Office of Security directive requirement but afford equivalent levels of protection without compensatory measures.

Vertical line denotes change.

(a) Approval Process for Variances.

1 Variances Related to Protection of Category I and II Quantities of Special Nuclear Material (SNM).

a Approval by the Departmental element is required before implementation of any variance related to protection of Category I and II quantities of SNM. Copies of the proposed and approved variance must be provided to the Office of Security. Additional requirements for notification are the same as in paragraph 2a(1)(a)2 a below.

b If the Office of Security disagrees with the variance, written notification will be made to the Departmental element and either the Under Secretary for Nuclear Security or the Under Secretary for Energy, Science, and Environment, of the basis for the disagreement.

2 Variances Related to Other S&S Program Directive Requirements.

a The DOE cognizant security authority may approve variances. The DOE cognizant security authority must send a copy of the variance and approval documentation to the Director, Office of Security; the appropriate Departmental element; and, for NNSA facilities, the Associate Administrator for Defense Nuclear Security, concurrently or as soon as practical after approval.

b For non-NNSA Headquarters (HQ) elements, variances may be approved by the cognizant Departmental element after obtaining the concurrence of the Director, Office of Security.

c For NNSA Headquarters elements, the cognizant Deputy Administrator may approve the variance after obtaining the concurrence of the Associate Administrator for Defense Nuclear Security, who must promptly notify the Director, Office of Security, following approval.

d The Office of Security will notify the responsible Departmental element in writing of concerns about the variance.

e The Director, Office of Security, must concur on variances to national policy requirements, such as the National Industrial Security Program (NISP) or the Personnel Security Program.

(b) Duration of Variances. There is no restriction on the length of time for which a variance can be approved.

(2) Waivers. Waivers are approved nonstandard conditions that deviate from a Departmental S&S program directive requirement that if uncompensated would create a potential or real S&S vulnerability. Waivers, therefore, require implementation of compensatory measures (e.g., additional resources to implement enhanced protection measures) for the duration of the waiver.

(a) Approval Process for Waivers.

1 Waivers Related to Protection of Category I and II Quantities of SNM.

a Approval by the Under Secretary for Nuclear Security for NNSA sites or the Under Secretary for Energy, Science, and Environment (ESE) for ESE sites is required before implementation of any waiver related to protection of Category I and II quantities of SNM. Copies of the proposed and approved waiver must be provided to the Office of Security. Additionally, the requirements and notifications in paragraph 2a(2)(a)2 below a must be followed. The cognizant security authority approval is contingent upon:

i. The presence of adequate compensatory measures in place before waiver implementation; and

ii. The documentation of any appropriate performance testing/vulnerability assessments (VAs).

b If the Office of Security disagrees with the waiver, written notification will be made to either the Under

Secretary for Nuclear Security or the Under Secretary for Energy, Science, and Environment, as appropriate, and the Deputy Secretary of the basis for the disagreement.

2 Waivers Related to Other S&S Program Directive Requirements.

a The DOE cognizant security authority approval is contingent upon:

i. the Departmental element; the Director, Office of Security; and for NNSA facilities, the Associate Administrator for Defense Nuclear Security are notified at least 30 days in advance of such approval;

ii. comments provided by HQ elements are formally reconciled before waiver implementation;

iii. the Departmental element and for NNSA facilities, the Associate Administrator for Defense Nuclear Security, have concurred on the waiver;

iv. adequate compensatory measures are in place before waiver implementation; and

v. documented performance testing/VAs, if appropriate, are accomplished prior to waiver implementation.

b For non-NNSA HQ elements, waivers may be approved by the cognizant Departmental element provided the requirements of paragraphs 2a(2)(a)2 a iv and v, above, are met and provided the concurrence of the Director, Office of Security, is obtained.

c For NNSA HQ elements, waiver approval may be granted by the cognizant Deputy Administrator after the following requirements have been met:

i. the NNSA Office of Defense Nuclear Security is notified at least 30 days before

waiver approval, and the concurrence of the NNSA Associate Administrator for Defense Nuclear Security is obtained.

ii. prior to concurrence, the NNSA Associate Administrator for Defense Nuclear Security sends written notification of the waiver to the Director, Office of Security.

d The Office of Security will provide written notification of concerns about the waiver to the responsible Departmental element and either the Under Secretary for Nuclear Security or the Under Secretary for Energy, Science, and Environment.

e The Director, Office of Security, must concur on waivers to national policy requirements, such as the NISP or the Personnel Security Program.

(b) Duration of Waivers. Waivers must not be approved for periods exceeding 2 years.

(3) Exceptions. Exceptions are approved deviations from a Departmental S&S Program directive requirement that create an S&S vulnerability. Exceptions must be approved only when correction of the condition is not feasible and compensatory measures are inadequate to preclude the acceptance of risk.

(a) Approval Process for Exceptions.

1 Exceptions Related to Security Conditions.

a For non-NNSA HQ facilities, a request for an exception must be sent to the Director, Office of Security for review and approval.

b For other non-NNSA operations, a request for an exception must be sent to the Under Secretary for Energy, Science and Environment for review and approval.

c For NNSA operations, a request for an exception must be sent to the Under Secretary for Nuclear Security for review and approval.

2 Exceptions Related to Protection of Category I and II Quantities of SNM.

a Approval by the Secretary of Energy or the Deputy Secretary of Energy is required before implementation of any exception related to protection of Category I and II quantities of SNM. Copies of the proposed and approved exception documentation must be provided to the Office of Security.

b If the Office of Security disagrees with the exception, written notification of the concern will be made to either the Under Secretary for Nuclear Security or the Under Secretary for Energy, Science, and Environment, as appropriate, and the Deputy Secretary.

3 Exceptions Related to All Other S&S Program Directive Requirements.

a All other non-HQ element exceptions from cognizant security authorities must have the appropriate Departmental element concurrence and the approval of either the Under Secretary for Nuclear Security or the Under Secretary for Energy, Science, and Environment. Copies of the proposed and approved exception must be provided to the Office of Security.

b If the Office of Security disagrees with the exception, written notification of the concern will be provided to Departmental element and either the Under Secretary for Nuclear Security or the Under Secretary for Energy, Science, and Environment, as appropriate.

c Exceptions for HQ elements and facilities must have the concurrence of the Office of Security and the approval of the Deputy Secretary prior to implementation.

d Exceptions to national policy requirements, such as the NISP or the Personnel Security Program, must have the concurrence of the Director, Office of

Security and the approval of either the Deputy Secretary or Secretary prior to implementation.

4 Process for Submitting Exception Requests.

a For cognizant security authorities, exception requests for non-NNSA operations must be submitted through line management to the Departmental element for submittal to the Under Secretary for Energy, Science, and Environment with a copy to the Office of Security. For NNSA facilities, cognizant security authorities must submit exception requests through line management to the cognizant Deputy Administrator and to the NNSA Associate Administrator for Defense Nuclear Security for submittal to the Under Secretary for Nuclear Security.

b For non-NNSA HQ elements, exception requests must be submitted to the Director, Office of Security.

c For NNSA HQ elements, exception requests must be submitted through the Office of Defense Nuclear Security to the Office of Security.

(b) Compensatory Measures. Compensatory measures implemented as the basis for an exception request must be subject to formal VAs. Compensatory measure implementation must be tested and validated.

(c) Duration of Exceptions. Exceptions must not be approved for periods exceeding 3 years (36 months).

(d) Annual Validation. The need for an exception must be validated annually (every 12 months) and documentation submitted to the Office of Security and cognizant Departmental element.

b. Documentation.

(1) Deviation Request Format. Specific information requirements for deviations are provided in Appendix 8, Format for Deviation Requests.

(2) Assessments and Performance Testing. The results of VAs and tests must be documented in the deviation request and in the site safeguards and security plan (SSSP)/site security plan (SSP), as appropriate.

Vertical line denotes change.

(3) Security Plans. Approved deviations must be documented in the SSSP/SSP and site procedures as appropriate. A deviation request approved out of cycle with the S&S plan formulation and approval process must be documented as an attachment to the applicable plan until the next annual update.

(4) Monitoring Implemented Compensatory Measures. Departmental elements must monitor compensatory measures, establish schedules, ensure that funding is effectively managed to address S&S interests, and monitor compliance with schedules.

c. Extensions. Any extension to the approved period of time for deviations requires reapplication of the deviation process.

SECTION M

APPENDIX 8—FORMAT FOR DEVIATION REQUESTS

1. Date. Date the request is signed by the requesting official.

2. Request Number. Alphanumeric identifier beginning with "SO" followed by the routing symbol used in the DOE National Telephone Directory, followed by the last two digits of the year of the request, followed by the three-digit number that is next in the sequence of requests from that cognizant security authority in that calendar year. For example, the third request from Headquarters during 2005 would be SO-HQ-05-003.

3. Deviation Title. Short, concise description of the specific deviation (e.g., Request for waiver of the vault-type-room requirements for building Z3999, Room 101; Request for variance for limited area barrier boundary).

4. Directive Citation. Title and date of the directive from which a deviation is being requested with a citation (paragraph or other provision) and summary of the directive requirement.

5. Impacted Entity. Identification of the specific facility (by SSIMS facility code number), process, procedure, system, etc.

6. Deviation Justification. Specific description of the deviation and the associated reason or rationale for the deviation request. A description of the relationship of the requested deviation to other S&S interests must be included if they are significantly affected.

7. Protection Measures. Description of the current measures used for protection and an evaluation of the effectiveness of such measures; description of alternate/compensatory measures or levels of protection to be provided as an alternative to directive requirements.

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

   NOTE: Waivers cannot be in place for more than 2 years (24 months); exceptions cannot be in place for more than 3 years (36 months).

9. Risks. Evaluation of the risks associated with the deviation, if approved. Results of vulnerability analyses and performance tests conducted on proposed alternatives must be included.

10. Signature. Requesting official's signature.

Vertical line denotes change.

SECTION N—INCIDENTS OF SECURITY CONCERN

1. OBJECTIVES. To set forth requirements for the Department of Energy (DOE) Incidents of Security Concern Program, including timely identification and notification of, response to, inquiry into, reporting of, and closure actions for incidents of security concern.

2. REQUIREMENTS. The broad-based requirements for implementing this section are listed below with elaboration provided in associated chapters. Additionally, there may be instances where security incidents are required to be reported through other department reporting systems (e.g., Computer Incident Advisory Capability, Occurrence Reporting and Processing System).

   a. Any person who observes, finds, or has knowledge or information about a potential incident of security concern must immediately report this information to the facility security officer (FSO) or designee of the facility where the incident occurred. The FSO or designee must make notifications as specified in Chapter I, paragraph 3, of this section.

   b. Any person discovering a potential incident of security concern, including one that involves classified information or matter; special nuclear material (SNM), including material protected, controlled, and accounted for as SNM; or other security interests at risk (e.g., interests not properly controlled), must make reasonable efforts to safeguard the security interests in an appropriate manner. The individual must also ensure evidence associated with the incident is not tampered with or destroyed.

   c. Any person discovering actual or suspected fraud, waste, or abuse of government resources must ensure such incidents are reported to the Office of the Inspector General in accordance with DOE O 221.1, *Reporting Fraud, Waste, and Abuse to the Office of Inspector General*, dated 3-22-01.

   d. Locally developed procedures must be established, documented, approved by the Departmental element, and disseminated to ensure the identification, reporting, root cause analysis, and resolution of incidents of security concern. These procedures must also identify guidelines for corrective actions and documentation of time and funds expended on incidents.

   e. Inquiries must be conducted to establish the facts and circumstances surrounding an incident of security concern.

   f. Appropriate Federal (to include the Office of Security), State, and local organizations must be contacted when a violation of law is suspected or discovered.

g. Appropriate corrective actions must be taken for each incident of security concern to reduce the likelihood of recurrence of the incident, including review and/or revision of applicable safeguards and security (S&S) plans and procedures.

h. The party or parties responsible for an incident of security concern must be subject to appropriate administrative actions, including disciplinary measures, retraining, counseling, or other directed actions necessary to reduce the likelihood of recurrence of the incident.

i. Any disciplinary or adverse actions involving DOE employees must be conducted according to DOE 3750.1, *Work Force Discipline,* dated 8-21-92.

CHAPTER I. IDENTIFICATION AND REPORTING REQUIREMENTS

1. GENERAL.

   a. A system of controls and procedures must be developed, approved, implemented, enforced, and maintained:

      (1) to deter, detect, and prevent recurrence of incidents of security concern and

      (2) for the timely identification and notification of, inquiry into, analysis of, and reporting of incidents of security concern.

   b. Inquiries are used to determine the root causes of and individuals responsible for incidents of security concern.

   c. All discussions and documents associated with an incident of security concern must be classified or controlled according to current classification or control guidance and follow procedures contained in appropriate DOE directives.

2. INCIDENT IDENTIFICATION AND CATEGORIZATION. DOE uses a graded approach for identification and categorization of incidents of security concern. This approach provides a framework for the requirements of reporting time-lines 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 section based on the severity of security incidents. The following paragraphs provide the basis for identification and categorization of incidents of security concern.

   a. Incident Identification. Incidents of security concern are actions, inactions, or events that have occurred at a site that:

      (1) pose threats to national security interests and/or critical DOE assets,

      (2) create potentially serious or dangerous security situations,

      (3) potentially endanger the health and safety of the workforce or public (excluding safety-related items),

      (4) degrade the effectiveness of the S&S program, or

      (5) adversely impact the ability of organizations to protect DOE S&S interests.

   b. Incident Categorization. Incidents of security concern must be categorized in accordance with their potential to cause serious damage or place S&S interests

and activities at risk. Four categories of security incidents have been established based on the relative severity of the incident. Each of the four categories is identified by an impact measurement index (IMI) number as follows (from most severe to least severe): IMI-1, IMI-2, IMI-3, and IMI-4. Each of the four categories is further subdivided into specific subcategories based on the security topical areas of physical protection, protective force (PF), information security, personnel security, and nuclear material control and accountability (MC&A). The categorization of specific security incidents occurs at the time the security incident is discovered. The categorization of specific security incidents can change based on information developed during the inquiry into the incident.

c. IMI. The IMI number is used to identify, trend, and evaluate each security incident or combination of incidents. (Specific information to be used to categorize incidents of security concern is contained in Table 1 through Table 4; however, the IMI subcategories contained in these tables are not all inclusive, and if they overlap, the more stringent reporting category will apply.) The basis for each IMI category is provided below.

(1) IMI-1. Actions, inactions, or events that pose the most serious threats to national security interests and/or critical DOE assets, create serious security situations, or could result in deaths in the workforce or general public. See Table 1, Reportable Categories of Incidents of Security Concern, Impact Measurement Index 1 (IMI-1).

(2) IMI-2. Actions, inactions, or events that pose threats to national security interests and/or critical DOE assets or that potentially create dangerous situations. See Table 2, Reportable Categories of Incidents of Security Concern, Impact Measurement Index 2 (IMI-2).

(3) IMI-3. Actions, inactions, or events that pose threats to DOE security interests or that potentially degrade the overall effectiveness of the Department's S&S protection program. See Table 3, Reportable Categories of Incidents of Security Concern, Impact Measurement Index 3 (IMI-3).

(4) IMI-4. Actions, inactions, or events that could pose threats to DOE by adversely impacting the ability of organizations to protect DOE S&S interests. See Table 4, Reportable Categories of Incidents of Security Concern, Impact Measurement Index 4 (IMI-4).

Table 1. Reportable Categories of Incidents of Security Concern, Impact Measurement Index 1 (IMI-1)

IMI-1 Actions, inactions, or events that pose the most serious threats to national security interests and/or critical DOE assets, create serious security situations, or could result in deaths in the workforce or general public.

DOE O 151.1B, *Comprehensive Emergency Management System,* dated 10-29-03, and facility emergency management plans may require more stringent reporting times for IMI-1 type incidents than listed here. Shorter reporting times should be determined on an individual incident basis and applied accordingly.

Incident Type	Report within 1 hour	Report within 8 hours	Report monthly
1. Confirmed or suspected loss, theft, or diversion of a nuclear device or components.	X		
2. Confirmed or suspected loss, theft, diversion, or unauthorized disclosure of weapon data.	X		
3. Confirmed or suspected loss, theft, or diversion of Category I or II quantities of special nuclear material (SNM).	X		
4. A shipper-receiver difference involving a loss in the number of items which total a Category I or II quantity of SNM.	X		
5. Confirmed or suspected loss, theft, diversion, unauthorized disclosure of Top Secret information, Special Access Program (SAP) information, or Sensitive Compartmented Information (SCI), regardless of the medium, method, or action resulting in the incident.	X		
6. Confirmed or suspected intrusions, hacking, or break-ins into DOE computer systems containing Top Secret information, SAP information, or SCI.	X		
7. Confirmed or suspected physical intrusion attempts or attacks against DOE facilities containing nuclear devices and/or materials, classified information, or other national security related assets.	X		
8. Confirmed or suspected attacks against DOE Federal and contractor employees that adversely impact a facility's or site's security posture.	X		
9. Confirmed or suspected acts or attempts of terrorist-type actions.	X		
10. Confirmed reports of DOE or DOE contractor employees making threats against Departmental facilities, employees, or the U.S. Government.	X		
11. Confirmed threats that immediately endanger personnel health or safety and may require immediate protective force/law enforcement intervention.	X		
12. Dangerous weapons and firearms-related incidents where an individual is killed, wounded, or an intentional discharge occurs.	X		
13. Confirmed or suspected acts of sabotage, at any DOE facility, that places the safety or security of personnel, facilities, or the public at risk.	X		
14. Confirmed compromise of root/administrator privileges in DOE unclassified computer systems that have a significant possibility of being contaminated with Top Secret information, SAP information, or SCI.	X		
15. Confirmed compromise of root/administrator privileges in DOE computer systems containing Secret or Confidential information.	X		
16. Confirmed intrusions into information systems containing classified information.	X		
17. Instances of malicious code that cause disruption, degradation, or compromise of information systems for an entire site/facility.	X		
18. Instances of malicious code that allow unauthorized or undetected access to information systems containing classified information (Top Secret, Secret, Confidential, SAP information, or SCI).	X		

Table 2. Reportable Categories of Incidents of Security Concern, Impact Measurement Index 2 (IMI-2)

IMI-2 Actions, inactions, or events that pose threats to national security interests and/or critical DOE assets or that potentially create dangerous situations.

Incident Type	Report within 1 hour	Report within 8 hours	Report monthly
1. Suspected loss, theft, or diversion of any radioactive material not categorized as special nuclear materials (SNM), or dangerous materials that could pose a health threat or endanger security.		X	
2. Confirmed or suspected intrusions, hacking, or break-ins into DOE computer systems containing Secret or Confidential classified information.		X	
3. Any amount of SNM found in an exceptionally dangerous/hazardous unapproved storage environment, or unapproved mode of transportation/transfer.		X	
4. Alarms or other loss detection indicators for security areas containing a Category I or II quantity of SNM that cannot be proven false within 24 hours.		X	
5. Inventory differences exceeding alarm limits in Category I and II SNM material balance areas, where there is no indication or reason to believe the difference is created by loss, theft or diversion.		X	
6. Confirmed or suspected unauthorized disclosure, loss, or potential loss of Secret matter regardless of the medium, method, or action resulting in the incident.		X	
7. Actual or suspected technical interceptions of any level of classified information.		X	
8. Actions, by electronic or physical means, that interfere with any DOE safeguards and security practices.		X	
9. Notifications, by any media or source, of validated threats that do not appear to immediately threaten personal safety or health.		X	
10. Loss of classified information that must be reported to other Government agencies or foreign organizations.		X	
11. Unsecured classified repositories of any type, including safes, doors, or other protective encasements, that contain Top Secret information, Special Access Program information, or Sensitive Compartmented Information.		X	
12. The loss of any DOE classified interest that requires State or local government or other Federal agency notification.		X	
13. Confirmed compromise of root/administrator privileges in DOE unclassified computer systems.		X	
14. Confirmed compromise of root/administrator privileges in DOE unclassified computer systems that have a significant possibility of being contaminated with Secret or Confidential information.		X	
15. Potential compromise of root/administrator privileges in DOE computer systems containing classified information.		X	
16. Instances of malicious code that cause disruption/degradation or compromise of information systems dedicated to safety, security, or critical operations.		X	
17. Detection of activities involving individuals who have been confirmed as physically watching/casing/surveilling a site in an effort to gather information to aid in the conduct of a terrorist-type attack.		X	

Table 3. Reportable Categories of Incidents of Security Concern, Impact Measurement Index 3 (IMI-3)

IMI-3 Actions, inactions, or events that pose threats to DOE security interests or that potentially degrade the overall effectiveness of the Department's safeguards and security protection program.			
Incident Type	Report within 1 hour	Report within 8 hours	Report monthly
1. A shipper-receiver difference or inventory difference involving a gain in the number of items for which the additional items total a Category I or II quantity of special nuclear material (SNM).		X	
2. Bomb-related incidents at any DOE facility, including location of a suspected device.		X	
3. Confirmed or suspected unauthorized disclosure, loss, or potential loss of Confidential matter by any medium, method, or action.		X	
4. Confirmed or alleged noncompliance with laws or DOE directives/standards that jeopardizes protection of the facility or site security interests.		X	
5. Demonstrators or protestors that cause site and facility damage.		X	
6. Labor strikes that could degrade or impede the required protection of the facility or site.		X	
7. Physical violence or threat of retaliation against facility security personnel.		X	
8. Dangerous weapons and firearms-related incidents involving protective force operations/personnel where an unauthorized weapon discharge occurs.		X	
9. Loss or theft of DOE firearms or ammunition, per DOE M 470.4-3, *Protective Force*.		X	
10. Unplanned/unscheduled power outages that cause a disruption/degradation of physical security systems and that would allow unauthorized or undetected entry to access controlled/protected areas.		X	
11. Incidents involving the attempted or actual introduction of controlled and prohibited items into Limited, Exclusion, Protected, or Material Access Areas, excluding unauthorized cellular phones or personal digital assistants where there is no potential for compromise of classified or unclassified controlled information.		X	
12. Confirmed or suspected malicious activities, including but not limited to stealing badges or vehicle licenses.		X	
13. Discovery of malicious activities, disorderly conduct, or vandalism that disrupts facility activities or causes damage between $10K and $100K.		X	
14. Circumvention of established access control procedures into a security area (excluding Property Protection Area).		X	
15. Inventory differences exceeding alarm limits in Category III SNM material balance areas or inventory differences greater than 50 g of Tritium, where there is no indication or reason to believe the difference is created by loss, theft, or diversion.		X	
16. A shipper-receiver difference involving a loss in the number of items which total a Category III or IV quantity of SNM.		X	
17. Confirmed or suspected loss, theft, or diversion of Category III or IV quantities of SNM.		X	
18. Intrusion attempts into information systems containing classified information.		X	
19. Confirmed intrusions into unclassified information systems that are not publicly available (e.g., behind a firewall).		X	

Table 3. continued

Incident Type	Report within 1 hour	Report within 8 hours	Report monthly
20. Confirmed instances of "denial of service" attacks on information systems that result in disruption of site/facility ability to access the Internet, disruption of site/facility information systems operations, or disruption of site/facility information system protection measures (e.g., firewall).		X	
21. Unauthorized network scans/probes on information systems possessing classified information.		X	
22. Incidents of apparent surveillance of facilities or operations (studying, photographing, low over-flights, outsiders questioning employees or protective force, unusual calls for information, etc.).		X	

Table 4. Reportable Categories of Incidents of Security Concern, Impact Measurement Index 4 (IMI-4)

IMI-4 Actions, inactions, or events that could pose threats to DOE by adversely impacting the ability of organizations to protect DOE safeguards and security interests.

Incident Type	Report within 1 hour	Report within 8 hours	Report monthly
1. Identified special nuclear materials (SNM) inventory differences beyond alarm limits in a Category IV SNM material balance area where there is no indication or reason to believe the difference is created by loss, theft, or diversion.			X
2. Significant shipper-receiver differences that exceed 200g of fissile material and the combined limit of error for the shipment.			X
3. Alarms or other loss detection indicators, excluding inventory differences and shipper-receiver differences, for a security area containing a Category III or IV quantity of SNM.			X
4. A shipper-receiver difference or inventory difference involving a gain in the number of items for which the additional items total to a Category III or IV quantity of SNM.			X
5. Confirmed or suspected unauthorized disclosure of Unclassified Controlled Nuclear Information, Export Control information, and unclassified Naval Nuclear Propulsion Information by any medium, method, or action.			X
6. Non-credible bomb threats at any DOE nuclear or non-nuclear facility.			X
7. Unsecured classified repositories of any type including safes, doors, or other protective encasements in which no likely classified disclosure occurred. If the repository contains Top Secret information, Special Access Program information, or Sensitive Compartmented Information, report under the IMI-1, IMI-2, or IMI-3 category, as appropriate.			X
8. Peaceful demonstrations or protests that do not threaten facility or site security interests or activities.			X
9. Failure to adhere to established procedures contributing to the misuse or misprocessing of or failure to maintain security badges and passes.			X
10. Loss of security badges in excess of 5 percent of total issued during 1 calendar year.			X
11. Failure to adhere to established procedures contributing to the mismanagement or faulty application of the DOE Human Reliability Program.			X
12. Failure to adhere to established administrative procedures contributing to problems with foreign visitors.			X
13. Classified information sent by e-mail that is contained within the firewall. All parties involved are cleared to the level of information transmitted, and the affected systems are identified, taken offline, and appropriately stored in approved areas pending sanitization. If more than 8 hours are required to isolate the affected systems, then such incidents will be handled as suspected compromises in accordance with their classification levels and categories.			X
14. Unauthorized cellular phones and personal electronic devices (e.g., PDAs) introduced into a Limited Area, Protected Area, or Material Access Area, where there is no potential for compromise of classified or unclassified controlled information.			X
15. Circumvent established access control procedures into a Property Protection Area.			X
16. High rate/amount of loss (excluding natural disasters) or theft of Government property.			X

3. REPORTING REQUIREMENTS.

a. 24-hour Determination/Categorization Period. When an incident is suspected to have occurred, the cognizant security authority at the site/facility where the incident occurred has 24 hours to examine and document all pertinent facts and circumstances to determine whether an incident has occurred (see Figure 1, Incidents of Security Concern). During this period, the suspected incident must be categorized by an IMI number. If it is determined that an incident of security concern did not occur, no further action is required.

b. Initial Incident Reporting. Incidents of security concern initial reports for IMI-1, IMI-2, and IMI-3 (as well as those for IMI-4 involving non-U.S. citizens, per paragraph 3d below) must be sent to the DOE Headquarters (HQ) Operations Center (OC) using DOE Form (F) 471.1, "Security Incident Notification Report," in accordance with locally developed procedures approved by line management. Initial security incident reports must be forwarded based on the following criteria.

(1) Within 1 hour following categorization for security incidents determined to be IMI-1 (see Table 1), the cognizant security authority at the originating site/facility must transmit a DOE F 471.1 to the DOE HQ OC. If a verbal notification of the incident is made to the DOE HQ OC, a follow-up transmission of the DOE F 471.1 to the DOE HQ OC must still be made.

(2) Within 8 hours following categorization of security incidents determined to be IMI-2/IMI-3 (see Tables 2 and 3), the cognizant security authority at the originating site/facility must transmit a DOE F 471.1 to the DOE HQ OC. If a verbal notification of the incident is made to the DOE HQ OC, a follow-up transmission of the DOE F 471.1 to the DOE HQ OC must still be made.

c. Reporting Incidents Receiving Media Attention. In addition to the IMI reporting time frames, the Office of Security must be notified within 8 hours of any security incidents that have been or will be reported in the media. The initial DOE F 471.1 and any subsequent updates must clearly identify the fact of media reporting.

d. Reporting Incidents Associated with Non-U.S. Citizens. Security incidents having any association with non-U.S. citizens must be clearly identified and reported on the initial DOE F 471.1 and subsequently in any related update or follow-on activity pertaining to the incident, including incidents categorized as IMI-4. For security incidents involving any credible information that a non-U.S. citizen or an agent of a foreign power is involved, the geographically closest element of the Office of Counterintelligence (OCI)/Office of Defense Nuclear Counterintelligence (ODNCI) must be notified.

e. Numbering Incidents and Changing Categories. When the initial incident notification report (i.e., DOE F 471.1) is transmitted, it must include a local incident tracking number. All subsequent reports pertaining to a security incident (e.g., inquiry and other related activities) must be transmitted to the Office of Security. Changes in IMI categorizations require resubmission of a DOE F 471.1 (or form similar in content) to the Office of Security.

f. Reporting Incidents Associated with Sensitive Programs. Only the initial DOE F 471.1 is required for incidents involving activities associated with sensitive programs. These programs include the Sensitive Compartmented Information (SCI) Program, Special Access Program (SAP), the Technical Surveillance Countermeasures (TSCM) Program, the Counterintelligence (CI) Program, or other programs identified by the Office of Security. All subsequent reporting must be handled "within channels" until such time as the inquiry report has been distributed. The date of the inquiry report must be transmitted to the Office of Security for entry into the Incident Tracking and Analysis Capability database.

g. Closing Inquiries.

(1) IMI-1 and IMI-2 incidents are considered closed upon completion of the inquiry report. The inquiry report must be completed within 60 working days of the incident categorization or a status report must be provided in accordance with paragraph 3k below.

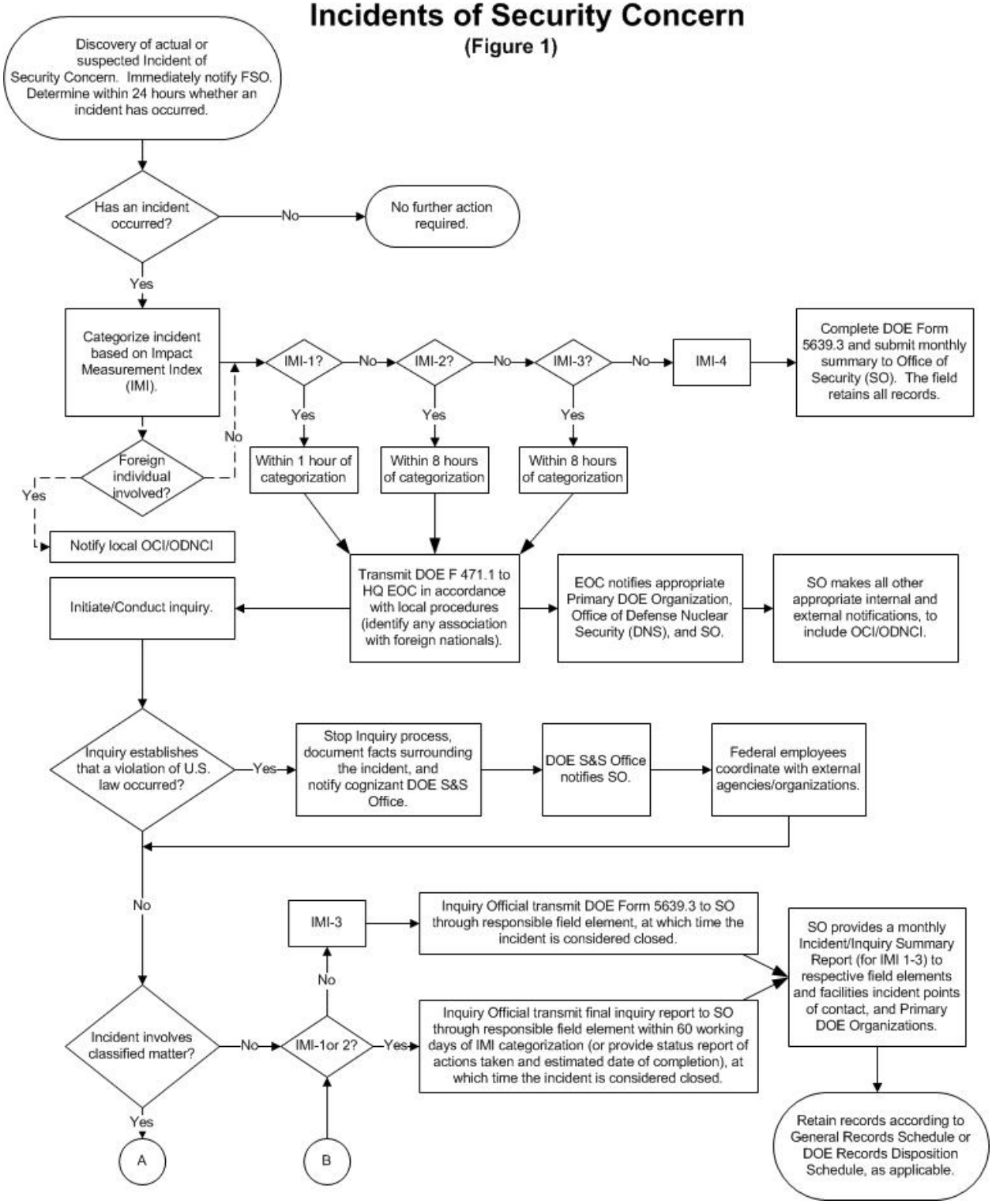
(2) IMI-3 incidents are considered closed upon completion of DOE F 5639.3, "Report of Security Incident/Infraction," and transmission of the completed DOE F 5639.3 to the Office of Security. The completion of the section on assignment and acceptance of security infractions (Part II, DOE F 5639.3) must be completed as required in local procedures.

(3) IMI-4 incidents are considered closed upon completion of the DOE F 5639.3 in accordance with associated local procedures.

(4) A sanitized (unclassified) copy of the DOE F 5639.3 must be provided to the responsible personnel security office for placement in the appropriate personnel security file.

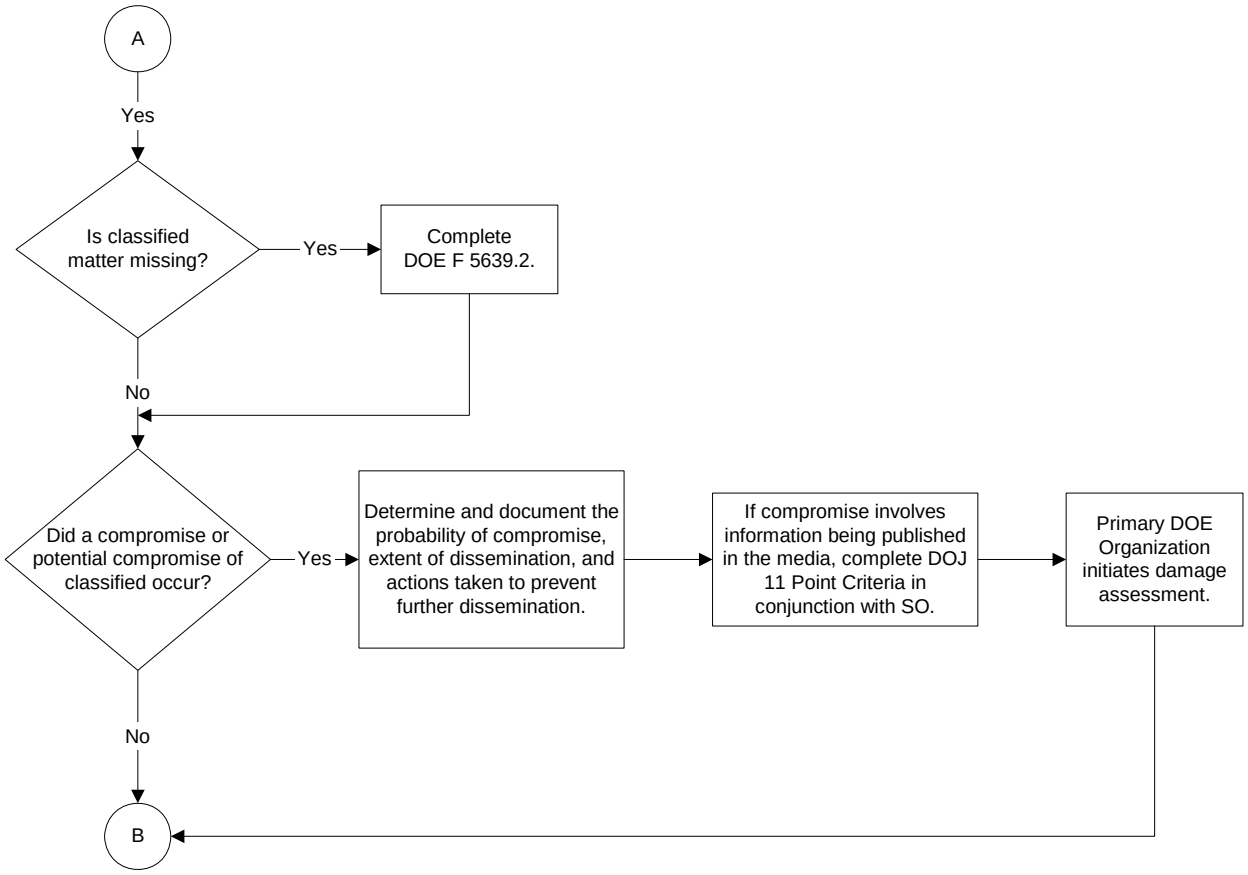
h. Final Inquiry Reports. Inquiry officials must forward final inquiry reports in accordance with local procedures to line management for action and to the Office of Security.

Incidents of Security Concern
(Figure 1)



Incidents of Security Concern

(Figure 1 continued)



i. Office of Security Monthly Incident Summary Report. By the 10th working day of each month, the Office of Security will e-mail a summary status report of the previous month's recorded incidents and inquiries to the cognizant security authority and Departmental elements.

(1) New closures during the current month and all open incidents will be reflected in the monthly update.

(2) These monthly updates will be used to ensure the Office of Security and the cognizant security authority maintains accurate, coordinated, and reconciled incident/inquiry status information.

j. Status/Summary Reports.

(1) IMI-1 and IMI-2. A monthly status report must be provided to the Office of Security and the Departmental element for IMI-1 and IMI-2 incidents that have not been closed within 60 working days of notification of the incident.

(a) Status reports must include as a minimum, the local tracking number (if applicable), date of incident categorization (not discovery), completed and planned actions, identification of issues precluding closure, and estimated date of closure. A copy of the original DOE F 471.1 (or form similar in content) may be included also.

(b) Status reports are due by the fifth working day of each month.

(2) IMI-3. Status reports are not required for IMI-3 incidents.

(3) IMI-4. The cognizant security authority at each facility must maintain a compilation of IMI-4 incidents by month. These monthly summaries, which must contain the number of open and closed security incidents by IMI-4 subtopic, the total initiated for the calendar month, and a running total of open and closed incidents for the calendar year, must be provided to the Office of Security. If no reportable incidents occurred during the calendar month, a summary stating "no reportable incidents" must be forwarded to the Office of Security by the fifth working day of each month.

k. Separate but Related Reporting.

(1) Occurrence Reporting Processing System. To eliminate reporting redundancy and centralize the reporting of security-related occurrences, all occurrences previously reported within the "Group 5—Safeguards and Security" category once contained in cancelled DOE M 231.1-2,

Occurrence Reporting and Processing of Operations Information, dated 8-19-03 are now incorporated into this section. Because an event meets the criteria for reporting as an incident of security concern does not negate the responsibility to report it as an occurrence under DOE O 231.1A, Chg 1, *Environment, Safety, and Health Reporting,* dated 6-3-04 (i.e., event affects both safety and security).

(2) DOE O 151.1B, *Comprehensive Emergency Management System*, dated 10-29-03. Incidents that are reportable under the provisions of DOE O 151.1B, *Comprehensive Emergency Management System*, must continue to be reported in accordance with that Order and this section.

(3) Flash Reporting. National Nuclear Security Administration (NNSA) "Flash Reporting" procedures are not affected by the requirements in this section.

(4) Special Reporting Situations. Under certain circumstances, related incidents of security concern, that are anticipated to recur over a long period of time, may be consolidated into a single monthly reports. This situation will be handled on a case-by-case basis between the cognizant security authority, the Departmental element, and the Office of Security. Specific plans for this reporting process must be developed by the cognizant security authority and submitted through the Departmental element to the Office of Security.

l. Documenting Corrective Actions. Corrective actions identified in response to an incident of security concern must be documented. For incidents categorized as IMI-1, IMI-2, or IMI-3, a copy of the documentation must be forwarded to the Office of Security if this information is not included in the inquiry report. Documentation on corrective actions for IMI-4 incidents does not have to be forwarded to the Office of Security.

m. Reporting to Congress. Section 3150 of the Defense Authorization Act requires the Secretary of Energy to notify the Committees on Armed Services of the Senate and House of Representatives of each "significant nuclear defense intelligence loss." A "significant nuclear defense intelligence loss" is defined in the Defense Authorization Act as "any national security or counterintelligence failure or compromise of classified information at a facility of the Department or operated by a contractor of the Department that the Secretary considers likely to cause significant harm or damage to the national security interest of the United States."

(1) The Department regards the loss or compromise (i.e., disclosure of classified information to unauthorized persons) of Top Secret information; SCI; SAP information; and Weapon Data Sigmas 1, 2, 14, and 15 as reportable under Section 3150.

(2) Within 30 days of discovery of Section 3150 reportable incidents, the Office of Security, after consultation with the Director, Central Intelligence, and the Director, Federal Bureau of Investigation (FBI), must provide notification to Congress.

4. INQUIRY OFFICIALS.

a. Inquiry officials must conduct inquiries to establish the pertinent facts and circumstances surrounding incidents of security concern.

b. Inquiry officials may be either Federal or contractor employees but must have previous investigative experience or Department inquiry training and must be knowledgeable of appropriate laws, executive orders, Departmental directives, and/or regulatory requirements.

(1) Contractors may conduct inquiries into incidents of security concern; however, if a violation of law is determined or suspected or the inquiry establishes information that a foreign power or an agent of a foreign power is involved, the contractor must stop further inquiry actions and notify the DOE cognizant security authority, which will assume further notification and reporting responsibilities, to include coordination with OCI/ODNCI. In such instances, the contractor must document the known circumstances surrounding the incident of security concern and submit all accumulated data to the DOE cognizant security authority.

(2) In all instances where the DOE cognizant security authority disagrees with the contractor report, the DOE cognizant security authority must assume supplemental inquiry responsibilities.

(3) When the inquiry into an incident of security concern necessitates communication with Agencies/organizations external to the Department (e.g., the U.S. Postal Service, the FBI, or other Federal agencies), a Federal employee must be responsible for performing all such communication.

(4) Contact with Federal, State, and local law enforcement officials may be made by contractors with the written concurrence of the DOE cognizant security authority and DOE line management.

c. Inquiry officials are not authorized to detain individuals for interviews or obtain sworn statements; however, they may conduct consensual interviews and obtain signed statements.

d. Inquiry officials must be appointed in writing by the DOE line management, the head of the Office of Headquarters Security Operations, or the Office of Security.

e. Inquiry officials are responsible for conducting the inquiry and maintaining records and documentation associated with the inquiry (e.g., logs of events, notes, recordings, and statements).

f. When inquiry officials discover suspected or confirmed violations of law, they must immediately notify the Office of Security.

5. FEDERAL, STATE, OR LOCAL LAW ENFORCEMENT PERSONNEL.

a. If a violation of law has occurred and the preservation of evidence requires the immediate notification of Federal, State, or local law enforcement agencies (e.g., theft of SNM, homicide, assault, location or detonation of an explosive device), the DOE cognizant security authority must perform all necessary referrals and notifications, including notification to the Office of Security. The Office of Security will notify the HQ elements of all referrals to other Federal law enforcement agencies, including the FBI.

b. Federal, State, or local law enforcement agency personnel requiring access to limited areas or higher for investigative actions must be escorted, have a current access authorization passed to DOE, or possess an active DOE access authorization. Such personnel will be approved for access to classified information or matter only if they possess the appropriate access authorization, the matter directly pertains to the investigation, and appropriate programmatic approvals have been granted if such approvals are required. Access to Restricted Data (RD) and Formerly Restricted Data (FRD) requires a DOE Q or L or appropriate personnel security clearance.

c. When authorized and approved Federal, State, or local law enforcement personnel are given access to classified information, they must be immediately advised of the classification level and category. They must also be informed of the protection and control requirements associated with the classified information they possess.

d. When an inquiry establishes information that a foreign power or an agent of a foreign power is involved, the Office of Security must immediately notify OCI/ODNCI, which in turn will notify the FBI in accordance with 50 U.S.C. 402a.

e. When an inquiry surrounding an incident of security concern establishes information indicating that fraud, waste, or abuse has occurred, the Office of the Inspector General must be notified for information and/or action.

f. The DOE cognizant security authority must make arrangements for the issuance of standard DOE security badges, the granting of access to classified information, and any other necessary agreements or items requested or required by Federal, State, or local law enforcement agencies involved in investigations.

6. CONDUCT OF INQUIRIES.

a. If an incident affects more than one site/facility, the following criteria must be used in determining the lead organization responsible for conducting the inquiry.

(1) If the sites/facilities fall under the purview of a single DOE cognizant security authority, that DOE cognizant security authority must assign responsibility to a lead organization.

(2) If the sites/facilities fall under the purview of multiple DOE cognizant security authorities, those DOE cognizant security authorities must, by mutual agreement, decide on a lead organization with responsibility for the inquiry.

b. The following actions must be taken when conducting inquiries into incidents of security concern and be reflected in the inquiry report (see Chapter II for additional requirements).

(1) Data Collection.

(a) Collect all data/information relevant to the incident, such as operations logs, inventory reports, requisitions, receipts, photographs, signed statements, etc.

(b) Conduct interviews to obtain additional information regarding the incident.

(c) Collect physical evidence associated with the inquiry, if available. (Examples of physical evidence include, but are not limited to, recorder charts, computer hard drives, defective/failed equipment, procedures, and readouts from monitoring equipment, etc.)

(d) Ensure physical evidence is protected and controlled and a chain-of-custody is maintained. (See Figure 2 for an example of a Chain-of-Custody Form.)

(2) Incident Reconstruction.

(a) Reconstruct the incident of security concern to the greatest extent possible using collected information and other evidence.

(b) Develop a chronological sequence of events that describes the actions preceding and following the incident.

(c) Identify persons associated with the incident.

Figure 2. Example Chain-of-Custody Form

EVIDENCE/PROPERTY CUSTODY DOCUMENT **For use of this form see ISC-301 Conduct of Inquiries Course Manual.** **Proponent is the DOE Computer Forensics Laboratory.**	DOE TRACKING NUMBER: CFL CASE NUMBER
RECEIVING ACTIVITY	LOCATION
NAME, GRADE AND TITLE OF PERSON FROM WHOM RECEIVED ☐ OWNER ☐ OTHER	ADDRESS *(Including Zip Code)*
LOCATION FROM WHERE OBTAINED	REASON OBTAINED / DATE/TIME OBTAINED

ITEM NO.	QUANTITY	DESCRIPTION OF ARTICLES *(Include model, serial number, condition and unusual marks or scratches)*

CHAIN OF CUSTODY

ITEM NO.	DATE	RELEASED BY	RECEIVED BY	PURPOSE OF CHANGE OF CUSTODY
		SIGNATURE NAME, GRADE OR TITLE	SIGNATURE NAME, GRADE OR TITLE	
		SIGNATURE NAME, GRADE OR TITLE	SIGNATURE NAME, GRADE OR TITLE	
		SIGNATURE NAME, GRADE OR TITLE	SIGNATURE NAME, GRADE OR TITLE	
		SIGNATURE NAME, GRADE OR TITLE	SIGNATURE NAME, GRADE OR TITLE	
		SIGNATURE NAME, GRADE OR TITLE	SIGNATURE NAME, GRADE OR TITLE	

Figure 2. Example Chain-of-Custody Form (continued)

		CHAIN OF CUSTODY *(CONTINUED)*		
ITEM NO.	DATE	RELEASED BY	RECEIVED BY	PURPOSE OF CHANGE OF CUSTODY
		SIGNATURE	SIGNATURE	
		NAME, GRADE OR TITLE	NAME, GRADE OR TITLE	
		SIGNATURE	SIGNATURE	
		NAME, GRADE OR TITLE	NAME, GRADE OR TITLE	
		SIGNATURE	SIGNATURE	
		NAME, GRADE OR TITLE	NAME, GRADE OR TITLE	
		SIGNATURE	SIGNATURE	
		NAME, GRADE OR TITLE	NAME, GRADE OR TITLE	
		SIGNATURE	SIGNATURE	
		NAME, GRADE OR TITLE	NAME, GRADE OR TITLE	
		SIGNATURE	SIGNATURE	
		NAME, GRADE OR TITLE	NAME, GRADE OR TITLE	
		SIGNATURE	SIGNATURE	
		NAME, GRADE OR TITLE	NAME, GRADE OR TITLE	

FINAL DISPOSAL ACTION

RELEASE TO OWNER OR OTHER (Name/Organization) _____

DESTROY _____

OTHER (Specify)

FINAL DISPOSAL AUTHORITY

ITEM(S)_____ON THIS DOCUMENT, PERTAINING TO THE INQUIRY/INVESTIGATION INVOLVING:

_____(IS)(ARE) NO LONGER
(Grade) *(Name)* *(Organization)*

REQUIRED AS EVIDENCE AND MAY BE DISPOSED OF AS INDICATED ABOVE. *(If articles must be retained do not sign, but explain in separate correspondence.)*

_____
(Typed/Printed Name, Grade, Title) *(Signature)* *(Date)*

WITNESS TO DESTRUCTION OF EVIDENCE

THE ARTICLE(S) LISTED AT ITEM NUMBER(S)_____(WAS) (WERE) DESTROYED BY THE EVIDENCE CUSTODIAN IN MY PRESENCE, ON THE DATE INDICATED ABOVE.

_____
(Typed/Printed Name, Grade, Title, Organization) *(Signature)* *(Date)*

(3) Incident Analysis and Evaluation. This analysis determines which systems/functions performed correctly or failed to perform as designed. It provides the basis for determining the cause of the incident and subsequent corrective actions. Inquiry officials must:

(a) analyze the information collected during the inquiry to determine whether it describes the incident completely and accurately;

(b) collect additional data and reconstruct the incident if more information is required; and

(c) identify any collateral impact with other programs or security interests.

7. INQUIRY REPORT CONTENT/CLOSURE CONSIDERATIONS.[18] Inquiry reports must describe the conduct and results of the inquiry and include the following information for the incident to be closed.

a. An executive summary.

b. A narrative, which must include the following items.

(1) The date and time of incident discovery, any notifications, the incident inquiry, and other time-related actions pertaining to the incident (WHEN).

(2) All data pertinent to the location of an incident, including the facility name and facility code [as registered in the Safeguards and Security Information Management System (SSIMS)], building/room numbers, and other identifying information as appropriate. Such information is required for all facilities affected by the incident (WHERE).

(3) A complete discussion of the facts and circumstances surrounding the incident, including a description of all supporting information (WHAT), such as the following:

(a) detailed description of the incident of security concern;

(b) identification of all personnel involved in the incident and when they were notified, including those associated with the inquiry process (i.e., inquiry officials and assisting personnel);

(c) identification of the causes for the incident (direct and contributing factors) and descriptions of the mitigating or aggravating factors that may reduce or increase the impact of the incident;

[18] A fully completed Incident Tracking Analysis Capability (ITAC) report form may be used in lieu of a standard narrative report.

(d) descriptions of the actions that precipitated the incident;

(e) descriptions of all physical evidence, including all records/documents reviewed (e.g., training records, policies/procedures);

(f) results of any interviews performed;

(g) descriptions of actions taken to minimize vulnerabilities created by the incident and prevent further loss/compromise of the security interest; and

(h) if the incident involves classified information or matter, the following must also be included:

1 a description of the potentially compromised classified information or matter, including but not limited to classification level, category, caveats (if any), and form of information (e.g., document title, date, and description). [A copy of the evidence (or photograph) must be retained and provided to the Office of Security, if requested.];

2 the classification guide and topic or source document, including date, of guide or source document;

3 known recipients of potentially compromised matter; and

4 owner of the classified information or matter [e.g., program office or Other Government Agency (OGA)].

(4) An inquiry official's conclusion and the basis/facts that support the conclusion are essential.

(a) Given the facts determined through the inquiry, the conclusion of the final report must address the potential risk to the security interest based upon a subjective analysis of the facts and circumstances surrounding the incident of security concern.

(b) The final report must also identify the line management responsible for corrective actions and disciplinary actions.

c. The following must be included as attachments to the report of inquiry:

(1) a copy of the documentation appointing the inquiry official;

(2) a copy of any signed statements of involved individuals;

(3) a description of the compromised or potentially compromised information (as appropriate);

(4) a copy of the DOE F 471.1 and other documents obtained during the data collection phase of the inquiry;

(5) a copy of any DOE F 5639.3, or a form comparable in content, issued as a result of the inquiry; and

(6) a copy of any DOE F 5639.2, "Reporting Unaccounted for Documents," or a form comparable in content, if applicable.

8. ADMINISTRATIVE ACTIONS.

a. Whenever possible, the responsibility for an incident of security concern must be assigned to an individual rather than to a position or office.

(1) When individual responsibility cannot be established and the facts show that a responsible official allowed conditions to exist that led to an incident of security concern, responsibility must be assigned to that official.

(2) Security infractions are issued to document the assignment of responsibility for an incident of security concern. Individuals who do not possess an access authorization may be issued a security infraction.

b. Corrective actions taken in response to incidents of security concern must be documented, and for incidents categorized as IMI-1, IMI-2, or IMI-3, a copy of the documentation must be forwarded to the Office of Security. Documentation on corrective actions for IMI-4 incidents does not have to be forwarded to the Office of Security.

c. A copy of Part 1 of DOE F 5639.3, or similar form, must be placed in the employee's DOE personnel security file. If an employee does not have an access authorization, it must be placed in his/her personnel file.

9. RECORDS RETENTION.

a. Records pertaining to incidents of security concern must not be sent to Federal Records Centers.

b. Records must be dispositioned in accordance with an applicable General Records Schedule (GRS), published by the National Archives and Records Administration (NARA), or in accordance with a DOE Records Disposition Schedule approved by NARA, whichever is applicable.

c. The site records manager or similarly titled person should be routinely consulted regarding the maintenance and disposition of records.

CHAPTER II. INCIDENTS OF SECURITY CONCERN INVOLVING COMPROMISE OR POTENTIAL COMPROMISE OF CLASSIFIED INFORMATION

1. INQUIRIES INTO COMPROMISE OF, POTENTIAL COMPROMISE OF, OR MISSING CLASSIFIED INFORMATION. The following requirements are in addition to those contained in Chapter I of this section. Inquiry officials must perform the following actions.

   a. Interview custodians and others having knowledge of the incident. When necessary, records must be audited for evidence of destruction, transmission, or other disposition.

   b. Ensure a DOE F 5639.2. "Reporting Unaccounted for Documents," or a form comparable in content, is completed if classified information or matter is missing.

   c. Determine which Departmental element has programmatic responsibility for the information or whether the information was originated by another Government agency or foreign government.

   d. Determine whether a compromise or potential compromise occurred. If there was a potential compromise, seek to determine the probability of compromise. Document the basis for such findings (i.e., potential compromise is defined as an incident of security concern where circumstances exist that cannot rule out the compromise of classified information).

   e. If an inquiry determines that a compromise or potential compromise has occurred, document the extent of the dissemination of the classified information and the actions taken to prevent further dissemination.

   f. When an inquiry establishes that classified information has been compromised by being published in the media, the questions contained in the Department of Justice (DOJ) Eleven-Point Criteria, which are listed below, must be answered and coordinated with the Office of Security. When completing the questions, provide all documentation and appropriate information to support affirmative responses. Each question must be answered affirmatively before the DOJ will initiate a formal investigation into the compromise; however, failure to affirmatively answer all the DOJ criteria does not preclude the DOJ from pursuing administrative or criminal action.

      (1) Could the date and identity of the article or articles disclosing the classified information be provided?

      (2) Could specific statements in the article that are considered classified be identified? Was the data properly classified?

(3) Is the classified data that was disclosed accurate? If so, provide the name of the person competent to testify concerning the accuracy.

(4) Did the data come from a specific document, and, if so, what is the origin of the document and the name of the individual(s) responsible for the security of the classified data disclosed?

(5) Could the extent and official dissemination of the data be determined?

(6) Has it been determined that the data has not been officially released in the past?

(7) Has it been determined that prior clearance for publication or release of the information was not granted by proper authorities?

(8) Does review reveal that educated speculation on the matter cannot be made from material, background data, or portions thereof which have been published officially or have previously appeared in the press?

(9) Could the data be made available for the purpose of prosecution? If so, include the name of the person competent to testify concerning the classification.

(10) Has it been determined that declassification had not been accomplished prior to the publication or release of the data?

(11) Will disclosure of the classified data have an adverse impact on the national defense?

2. DAMAGE ASSESSMENTS. Damage assessments determine potential damage to national security when classified information has been compromised or potentially compromised. Damage assessments are performed to evaluate and document possible countermeasures and conduct actions to limit potential damage. The Departmental element must use the damage assessment to determine future courses of action within the affected program. Additionally, damage assessments are used by appropriate authorities when criminal prosecution is sought. Classification guidance must be evaluated and updated, as appropriate, based on damage assessments. Damage assessments must be conducted when:

a. inquiries disclose evidence that classified information, including Weapon Data (Sigmas 1, 2, 14, and 15), SCI, or SAP data have been compromised or potentially compromised;

b. analysis reveals similar information has been compromised frequently or when the information has been compromised to a wide audience (e.g., public media, international conference, Internet);

c. a violation of laws appears to have occurred and criminal prosecution is contemplated; or

d. the Departmental element determines one is necessary.

3. CONDUCT OF DAMAGE ASSESSMENTS. The Departmental element with programmatic responsibility for the compromised or potentially compromised classified information must designate, in writing, a Federal employee from the DOE cognizant security authority who will be responsible for conducting the damage assessment. The Departmental element must also appoint an assessment team consisting of a derivative classifier and appropriate technical experts (e.g., experts in weapons design, nuclear policy, material production communications, intelligence, counterintelligence) to assist in assessing the value of the compromised information to foreign governments and/or hostile organizations and the impact on the affected program.

4. PROCEDURES. The following damage assessment procedures must be followed.

a. The originator of the compromised information must provide the DOE cognizant security authority with a copy of the compromised or potentially compromised information, if available. If no other copy exists, the originator must provide a detailed description of the compromised information.

b. The originator must coordinate with a derivative classifier to confirm the classification level and category of the compromised information according to current classification guidance and policy. The derivative classifier must provide the basis for the classification determination (i.e., the classification guide used).

c. The team performing the damage assessment must prepare a draft assessment and coordinate it with the originator of the compromised or potentially compromised information.

d. The damage assessment must be approved by the Departmental element with programmatic responsibility for the compromised or potentially compromised information, and at a minimum, copies will be submitted to the Director, Office of Security and the DOE cognizant security authority responsible for the inquiry. The Director, Office of Security will coordinate with the Departmental element and distribute additional copies as appropriate.

5. CONTENT OF DAMAGE ASSESSMENT REPORTS. Damage assessment reports must contain the following information.

a. Identification of the source, date, and circumstances of the compromise or potential compromise.

b. Classification of the specific information compromised or potentially compromised.

c. Description of the specific information compromised or potentially compromised.

d. Analysis and statement of the known or probable damage to national security that has resulted or may result.

e. Analysis and statement of the known or probable impact to the affected program.

f. Assessment of the possible advantage to foreign governments and/or hostile organizations as a result of the compromise or potential compromise.

Recommendation to the Office of Classification and Information Management Control regarding whether the classification of specific information should be modified to minimize or nullify the effects of the reported compromise or potential compromise, to include downgrading, declassification, or upgrading.

g. Assessment of whether countermeasures are appropriate and feasible to negate or minimize the effect of the compromise or potential compromise.

h. Assessment of other appropriate corrective actions.

6. COMBINING SIMILAR INCIDENTS. Damage assessments may be completed for a group of similar incidents when such grouping is a logical method of meeting this requirement. A logical grouping includes a situation where multiple matters requiring a damage assessment are related to a programmatic area and would result in the same or similar damage to national security or advantage to foreign governments and/or hostile organizations.

7. CASES INVOLVING OTHER GOVERNMENT AGENCY INFORMATION. Whenever a compromise or potential compromise involves the classified information of an other Government agency (OGA), the DOE cognizant security authority responsible for the inquiry must provide the facts and circumstances that affect the OGA's information or interests to the Director, Office of Security. The Director, Office of Security, must coordinate with the OGA, as appropriate.

8. CASES INVOLVING FOREIGN GOVERNMENT INFORMATION. Whenever a compromise or potential compromise involves the information of a foreign government that requires protection [e.g., Confidential Foreign Government Information Modified Handling (C/FGI-Mod)], the DOE cognizant security authority responsible for the inquiry must provide the facts and circumstances that affect the foreign government's information or interests to the Director, Office of Security. The foreign government, however, will not normally be advised of any Departmental security system vulnerabilities that allowed or contributed to the compromise or potential compromise. The Director, Office of Security will coordinate with the Department of State and the foreign government, as appropriate.

9. JOINT DAMAGE ASSESSMENT WITH ANOTHER GOVERNMENT AGENCY. Whenever a compromise or potential compromise involves classified information or interests of more than one Government agency, the following requirements apply:Each Government agency is responsible for conducting the assessment of damage resulting from its compromised or potentially compromised information.

b. If a compromise or potential compromise involves the classified information of DOE and another Government agency, and if more than one damage assessment is performed, the Departmental element responsible for the Department's damage assessment must provide the damage assessment to the Director, Office of Security, who will coordinate with the OGA.

c. When a joint damage assessment is to be made, the Office of Security will coordinate assignment of responsibility between the Department and the OGA.

d. If a compromise or potential compromise of Departmental classified information is the result of actions taken by non-U.S. citizens, foreign government officials, and/or U.S. nationals employed by international organizations, the Director, Office of Security, through coordination with OCI/ODNCI, must ensure, through appropriate intergovernmental liaison channels, that information pertinent to the assessment is obtained.

e. If a compromise or potential compromise of SCI has occurred, the Director, Office of Intelligence must consult with the designated representative of the Director, Central Intelligence and other officials responsible for the information involved.

SECTION O—RESTRICTIONS ON THE TRANSFER OF SECURITY-FUNDED TECHNOLOGIES OUTSIDE THE DEPARTMENT AND ITS OPERATIONAL FACILITIES

1. OBJECTIVE. To establish Technology Development Program (TDP) procedures and criteria for disseminating classified and/or unclassified controlled Office of Security and Safety Performance Assurance (SSA)-funded technology, other TDP-related information, and/or protection practices/expertise to any recipients who are not Department of Energy (DOE) Federal or contractor employees.

2. REQUIREMENTS.

   a. General. The dissemination in any form of SSA-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 safeguards and security (S&S) and classification and control policies;

      (2) verification 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 set forth in this section (see paragraph 2c, below) and Export Control Laws and Regulations.

   b. Risk Assessment.

      (1) A risk assessment of the unauthorized use/transfer of classified technology, information, or practices must be conducted before release of the technology/information and used as the basis for approving or denying proposed transfers.

      (2) The risk assessment must be used to determine whether an applicant is eligible to receive a specific type of information/technology.

      (3) Proposed release must be handled on a case-by-case basis because eligibility criteria are determined by both the type of information/ technology and the intended recipient. Additionally, the risk assessment must address the following factors.

(a) No person is entitled solely by virtue of rank, position, or access authorization (security clearance) to have access to classified or unclassified controlled SSA-funded technology, information, or protection practices/expertise.

(b) Relevance of the subject information to the protection of Department facilities and assets.

(c) Ability of the intended recipient to protect the information/technology in a manner equivalent to minimum security standards required by the Department.

c. Review and Approval Process. Coordination and approval must include the Departmental element and the Director, Office of Security.

d. Centralized Reporting. Written reports of each approval or denial of a request for technology subject to the requirements of this section must be sent to the Office of Security within 30 days of the decision.

e. Documentation.[19] The records listed below must be completed to document each receipt of a request for transfer of technology subject to the requirements of this chapter and to document the Department's transfer decision.

(1) Technology Transfer Approval Requests. The information in Appendix 9, Technology Transfer Approval Requests, must be included in all technology transfer approval requests.

(2) Basis for Approving or Denying a Transfer. A record of the concurrences, nonconcurrences, reviewer comments, executed Nondisclosure Agreement (if applicable), risk assessment (see paragraph 2b above), and approval or denial of the transfer must be created and maintained.

f. Records Retention. Each element requesting, reviewing, approving, and/or denying technology transfer requests must maintain a documented audit trail of requests initiated or handled by that office. Records, including the documentation cited in paragraph 2e above, must be retained for a minimum of 5 years.

[19] A nondisclosure agreement form will be provided upon request.

Vertical line denotes change.

SECTION O

APPENDIX 9—TECHNOLOGY TRANSFER APPROVAL REQUESTS

1. Name of Individual Requesting the Transfer:						**Date:**__/__/
2. Proposed Technology for Transfer:						
3. Proposed Recipient and Address:						
4. Type of Technology or Information:						
DOE Proprietary Protection Capability	Vulnerability Fix Information	Vulnerability Information	Best-In-Class Protection Capability & Technical Advances	Risk Analysis & System Modeling Information	Performance Information	Fundamental Protection Capability
5. Method of Transferring the Technology or Information:						
Briefing	Written Report	Design Documents	Source Code	License	Course	Hardware
6. Type of Recipient:						
Domestic	DOE Employee or Contractor	Federal Employee	Domestic Users & Academia	Manufacturer	Other (specify) _____	Public Fora
Foreign	Foreign Government Official	Non-Government User	Foreign Manufacturer	Other (specify) _____	Export License Required? Yes/No Basis for determination__ _____	
7. Level of Classification or Control	Unclassified	OUO	UCNI*	Confidential*	Secret*	Top Secret*
8. Type of Agreement Proposed:		Written Instructions	License	Nondisclosure	Sales Limitation	None
9. Estimated U.S. Taxpayer Investment to Develop this Technology: $ _____						
10. Has This Technology Been Previously Transferred to this Recipient? YES ☐ NO ☐						

*Also requires a documented need to know.
Abbreviations: OUO=Official Use Only; UCNI=Unclassified Controlled Nuclear Information.

Vertical line denotes change.

DEPARTMENTAL ELEMENTS TO WHICH DOE M 470.4-1,
***Safeguards and Security Program Planning and Management* IS APPLICABLE**

Office of the Secretary
Departmental Representatives to the Defense Nuclear Facilities Safety Board
Energy Information Administration
National Nuclear Security Administration
Office of Civilian Radioactive Waste Management
Office of Congressional and Intergovernmental Affairs
Office of Counterintelligence
Office of Economic Impact and Diversity
Office of Electricity Delivery and Energy Reliability
Office of Energy Efficiency and Renewable Energy
Office of Environment, Safety and Health
Office of Environmental Management
Office of Fossil Energy
Office of General Counsel
Office of Hearings and Appeals
| Office of Human Capital Management
Office of Intelligence
Office of Legacy Management
| Office of Management
Office of Nuclear Energy, Science and Technology
Office of Policy and International Affairs
Office of Public Affairs
Office of Science
Office of Security and Safety Performance Assurance
| Office of the Chief Financial Officer
Office of the Chief Information Officer
Office of the Inspector General
Secretary of Energy Advisory Board
Bonneville Power Administration
Southeastern Power Administration
Southwestern Power Administration
Western Area Power Administration

Vertical line denotes change.

CONTRACTOR REQUIREMENTS DOCUMENT

DOE M 470.4-1, *Safeguards and Security Program Planning and Management*

This Contractor Requirements Document (CRD) establishes the requirements for Department of Energy (DOE) contractors, including National Nuclear Security Administration (NNSA) contractors. Contractors must comply with the requirements listed in the CRD to the extent set forth in their contracts.

Regardless of the performer of the work, contractors with this CRD incorporated into their contracts are responsible for compliance with the requirements of the CRD. Affected contractors are also responsible for flowing down the requirements of the CRD to subcontracts at any tier to the extent necessary to ensure the contractors' compliance with the requirements. In so doing, contractors must not unnecessarily or imprudently flow down requirements to subcontractors. That is, contractors will ensure that they and their subcontractors comply with the requirements of the CRD and incur only those costs that would be incurred by a prudent person in the conduct of competitive business.

A violation of the provisions of this 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. 228b.). The procedures for the assessment of civil penalties are set forth in Title 10, Code of Federal Regulations, Part 824, *Procedural Rules for the Assessment of Civil Penalties for Classified Information Security Violations*, (10 CFR Part 824).

PART 1—PLANNING AND EVALUATIONS

SECTION A—SAFEGUARDS AND SECURITY PROGRAM PLANNING

1. OBJECTIVE. To establish a standardized approach for protection program planning that will provide an information baseline for use in integrating Departmental safeguards and security (S&S) considerations, facilitating management evaluation of program elements, determining resources for needed improvements, and establishing cost-benefit bases for analyses and comparisons.

2. REQUIREMENTS. The following are essential elements for planning for S&S programs.

   a. S&S Philosophy. S&S interests and activities must be protected from 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. DOE protective forces (PFs) that protect Category I quantities of special nuclear material (SNM); credible rollup of SNM to a Category I quantity; or those facilities that meet or exceed the Threat Level 2 criteria specified in DOE O 470.3A, *Design Basis Threat Policy*, dated 11-29-05, for chemical, radiological, or biological thresholds, must employ the DOE Tactical Doctrine contained in Appendix 2 of Section A.

   b. S&S Management Plan. This Plan must provide a description of the implementation of S&S policy and provide detailed information on the assignment of roles, responsibilities, and authorities as well as the development of budgets and allocation of resources. The Safeguards and Security Management Plan must be updated annually (at least every 12 months) and must document:

      (1) roles, responsibilities, delegations, and authorities for the S&S program;

      (2) organizational structure and accountability; and

      (3) planning and budget (including personnel resources).

      See Appendix 1, S&S Management Plan, for content requirements and suggested format. However, if a *Functions, Responsibilities, and Authorities Manual* for S&S has been approved and issued, and it meets the requirements stated above, it can be used in place of a Safeguards and Security Management Plan.

   c. S&S Program Operations. Actions must be taken to ensure an acceptable S&S program, including curtailment or suspension of operations when such operations

Vertical line denotes change.

would result in an immediate and unacceptable impact to national security, the environment, or the health and safety of the public or employees.

(1) Site-Specific Characterization. Protection programs must be tailored to address specific site characteristics and requirements, current technology, ongoing programs, and operational needs to achieve acceptable protection levels that reduce risks in a cost-effective manner.

(2) Threat Policy/Guidance. DOE O 470.3, *Design Basis Threat (DBT) Policy* must be used with local threat guidance during the conduct of vulnerability assessments (VAs) for protection and control program planning. The DBT must be the baseline threat definition but local threat guidance may be used to increase the level of threat to be analyzed.

(3) Targeted Protection Strategies.

(a) Strategies for the physical protection of special nuclear materials (SNM) and vital equipment must incorporate the applicable contractor requirements established in DOE M 470.4-2, *Physical Protection*.

(b) Protection strategies must be implemented as specified in the DBT. PF resources must focus on decisively defeating the terrorist threat, which is facilitated by positioning posts so there is little or no delay in responding to critical targets, eliminating posts which detract from constant readiness, and maximizing use of physical protection systems to enhance PF effectiveness. PF resources must be positioned to interdict and neutralize the adversary threat as far as possible outside the boundaries of the target location.

(c) Protection program elements must be designed to prevent and/or mitigate the consequences of acts of radiological, chemical, or biological sabotage that would cause unacceptable impact to national security, the environment, or the health and safety of the public or employees. Protection elements, such as active denial systems, must be designed and deployed to minimize the need for PF recapture/recovery operations.

(d) Strategies for the protection and control of classified information or matter must incorporate the applicable contractor requirements established in DOE M 470.4-4, *Information Security*.

(e) Security systems must be used that prevent, detect, or deter unauthorized access, modification, or loss of classified information

or matter and unclassified controlled information or matter and its unauthorized removal from a site or facility.

(f) Strategies for the protection of government property not covered above must reflect a graded approach. DOE offices, facilities, and property protection areas (PPAs) must meet or exceed General Services Administration (GSA) minimum security standards.

(g) Security countermeasures for explosive threats must address a range of activities including hand-carried, mailed, and vehicle-transported devices.

d. Graded Protection. The Department recognizes that risks must be accepted (i.e., that actions cannot be taken to reduce the potential for or consequences of all malevolent events to zero); however, an acceptable level of risk must be determined based on evaluation of a variety of facility-specific goals and considerations. By a graded approach, the Department intends that the highest level of protection be given to security interests and activities whose loss, theft, compromise, and/or unauthorized use would seriously affect the national security, the environment, Departmental programs, and/or the health and safety of the public or employees. Protection of other interests and activities must be graded accordingly.

e. Risk Management. S&S programs must be based on the results of vulnerability and risk assessments, the results of which are used to design and provide graded protection in accordance with an asset's importance or the impact of its loss, destruction, or misuse. The results of the assessments, to include the determination of system effectiveness, are one of the key considerations the manager must evaluate when establishing the level of risk. For example, if it is determined that there is high risk that is not being mitigated by compensatory measures, reporting must be made to the Secretary of Energy or the Deputy Secretary who can accept high risk. Cognizant Under Secretaries can accept moderate risk.

(1) Vulnerability and risk assessments must be conducted and documented to support the identification of risks to be accepted by the Department.

(2) To determine the appropriate level of protection against risk, line management must consider the threat, the vulnerability of the potential target, and the potential consequences of an adversarial act.

f. Site-Specific Programs.

(1) S&S programs must address site-specific characteristics.

(2) Performance assurance programs must be developed, managed, and implemented to ensure that S&S programs and protection program elements protect security interests and activities. These programs must ensure intensive, frequent performance testing of PF individual and unit tactics with oversight by line management and independent oversight organizations.

(3) A management and planning process to achieve integrated, site-specific protection from unauthorized actions must be implemented. This process must be based on a graded approach that implements the integrated concepts of deterrence, prevention, detection, and response.

(4) The DBT must be used as the basis for planning protection programs.

3. PLANNING.

a. S&S plans must be developed for facilities with any of the following S&S interests:

(1) Category I quantities of SNM or credible roll-up quantities of SNM to a Category I quantity;

(2) Category II, Category III, or Category IV SNM;

(3) radiological, chemical, or biological sabotage threats;

(4) critical mission disruption threats;

(5) intra/intersite transportation of SNM;

(6) classified information or matter;

(7) facilities engaged in the protection of Government property; and

(8) facilities that the Secretary, Deputy Secretary, or Under Secretaries deem appropriate.

b. Site Safeguards and Security (SSSP). The SSSP is a 5-year master planning document that must be prepared by the contractor for sites with facilities described in paragraphs 3a(1), (3), (4), or (8) above. The SSSP must depict the existing condition of site protection programs and when the DBT performance standard cannot be met, establish improvement priorities and resource requirements for the necessary improvements. Plan composition is reflected in Part 1, Section C, 5 of this CRD.

Vertical line denotes change.

c. Site Security Plan (SSP). At locations where an SSSP is not required because of the limited scope of interests [i.e., criteria contained in 3a(2), (5), (6), or (7) above apply], an SSP must be developed by the contractor to describe the protection program. SSPs must be approved by the local DOE cognizant security authority. In addition, specialized plans must be developed to address protection programs for other protection operations. Requirements for specialized plans that may or may not be components of the SSSP are set forth in other contractor requirements, including CRDs for other directives.

d. Planning Inputs. The documents listed below must be used to support program forecasts and information input used in the protection program planning process.

(1) Applicable contractor requirements, including CRDs for other directives, guidance, and intelligence assessment information developed and disseminated by line management or the Office of Security.

(2) Programmatic guidance and forecasts of significant changes planned in site operations as communicated through line management.

(3) Current and projected operational constraints and resources.

(4) Analysis of cost and effectiveness of security technologies versus traditional protection methodologies.

e. Plan Review and Approval.

(1) The SSSP requires approval by DOE line management and concurrence by the cognizant Head of the Departmental element. Such approval authority must be formally delegated to line management.

(a) Copies of approved SSSPs must be provided to the Office of Security for review and comment.

(b) Other security plans may be approved by line management or as stipulated in the applicable contractor requirements. If approving authority not otherwise stipulated, these security plans may be approved by DOE line management.

(2) The SSSP must be submitted to DOE line management within 150 days of the termination date of data collection and approved within 120 days of the submittal date. Changes to contractor requirements, facility reconfiguration, a new VA, or other activities that occur after the stated effective date will not be considered for purposes of reviewing/approving the plan.

(3) The SSSP must be reviewed annually (at least every 12 months). Updates to the SSSP that may significantly alter the agreed-upon protection philosophy or performance standards of protection systems must be subjected to the formal VA process, and if changes are shown to significantly alter system effectiveness performance, the update(s) will be subject to the same concurrence and approval as stated in paragraph 3e(1), above, communicated by DOE to the contractor.

(4) An information copy of approved modifications must be provided to the Office of Security.

SECTION A

APPENDIX 1—SAFEGUARDS & SECURITY MANAGEMENT PLAN

The Safeguards and Security (S&S) Management Plan provides a description of the contractor's implementation of S&S policy and provides detailed information on the assignment of roles, responsibilities, and authorities as well as the development of budgets and allocation of resources. The following outline delineates the content requirements and provides a suggested format.

1. EXECUTIVE SUMMARY.

   a. Program Mission Statement. Briefly describe the program mission and how the mission relates to national security. Describe the major elements or activities performed in terms of program mission and its relationship to the DOE national security mission.

   b. S&S Program Structure. Briefly describe the strategy and organizational elements used to implement the S&S program under their cognizance.

   c. Management and Planning Assumptions. Briefly describe those assumptions that affect the management and planning of the implementation of the S&S program. These assumptions should include items such as:

      (1) future of the program (mission, staffing levels, site status, etc.);

      (2) current and planned S&S projects; and

      (3) status of the organization's S&S budget.

2. PART 1—ORGANIZATIONAL STRUCTURE AND ACCOUNTABILITY

   a. Line Management Organization. Describe the structure and relationship of line management. Identify the roles, responsibilities, and authorities of these line management elements to include organizational charts.

   b. Cognizant Security Authority Organization. Describe the structure of line management that is specifically responsible for implementing the contractor's S&S program. Identify the individuals and positions responsible for committing resources and directing the activities of personnel associated with the S&S program. Provide an organizational chart to show the S&S organization and management structure and the lines of authority and points of interface with other programs which affect S&S (e.g., safety, facility operations, and the cognizant security authority's material control and accountability (MC&A) organization (if independent of the security organization). Describe the functions and

responsibilities of S&S personnel and indicate how S&S activities are integrated with those of other facility organizations; include organizational responsibilities for line management overseeing the program as well as the interface points with the respective Departmental Headquarters and Field elements.

3. PART 2 - ROLES, RESPONSIBILITIES, DELEGATIONS, AND AUTHORITIES. Delegations must be documented in writing and delineate all assigned S&S roles, responsibilities, and authorities for the S&S program. This section:

   a. documents offices/positions affected by the S&S Management Plan;

   b. establishes the approval chain for S&S plans, procedures and implementation policy;

   c. establishes the approval chain for S&S policy deviations;

   d. assigns reporting requirements for incidents of security concern; and

   e. provides a list of roles and responsibilities for key positions and the delegated authorities for each.

4. PART 3 - S&S PROGRAM IMPLEMENTATION. This section of the S&S Management Plan documents the processes and methods used to implement the Department's security policies. This section identifies:

   a. the methods used for ensuring all applicable programmatic requirements are implemented throughout the organizational element;

   b. the methods used for ensuring effective integration of S&S programmatic elements; and

   c. SSSPs and SSPs used to implement S&S policy requirements.

5. PART 4 - PLANNING AND BUDGET (INCLUDING PERSONNEL RESOURCES). This section of the S&S Management Plan documents the key processes of planning and budgeting, including strategic planning, budget formulation, budget execution, and program evaluation.

   a. Describe the strategic planning assumptions used to ensure the S&S program will meet mission objectives.

   b. Provide a 5-year plan that describes the budget formulation priorities for future S&S resources and programs.

   c. Provide the current year plan for executing the S&S budget. This plan details the allocation of resources that support S&S functions and missions.

d. Provide a program evaluation plan that details how the cognizant security authority will assess the implementation of the S&S program and the organization's progress toward meeting established missions/goals.

e. Briefly describe any changes to operational requirements which affect S&S program operations or would require increments or decrements to operational accounts (e.g., program direction, operational support, etc).

SECTION A

APPENDIX 2—DEPARTMENT OF ENERGY TACTICAL DOCTRINE

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 appendix is the condensed expression of the Department‘s fundamental approach to protecting nuclear weapons and components, special nuclear material, or targets subject to radiological or toxicological sabotage. 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 is supported by fixed strong points, obstacles/barriers, advanced detection and assessment capabilities, coordinated fire planning, updated weapon systems, and armored vehicles.

   b. Purpose of an Armed 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. When availability of armed PFs is limited, 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) pct 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. TACTICAL DOCTRINE.

   a. Concept. In general, at Category I/II 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. A TRF 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 mobile response teams using fire and

Vertical line denotes change.

maneuver techniques to deny further access to adversaries and/or to channel them into attrition areas covered by interlocking bands of fire from fixed, 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.

Vertical line denotes change.

(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 a decisive engagement with the adversary.

(h) Protect defenders by employing hardened fighting positions situated for mutual support.

(i) Establish supplementary defensive positions.

(j) Prepare to maneuver offensive 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) Assign sufficient resources to be able to assess remote alarms to identify the number of adversaries, thereby helping to differentiate between diversionary attacks and the main force.

(c) Plan for staged withdrawal of forces dispatched to assess remote alarms to prepared supplementary defensive positions.

(d) Plan for overwatch of assessment forces with long range weapons from within the defensive perimeter.

(e) 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.

(f) Ensure adequate standoff for vehicle-borne improvised explosive devices (VBIEDs).

(g) 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.

Vertical line denotes change.

(5) Manage the Site Population.

(a) Limit the number of personnel, vehicles, and equipment in the target area at all times.

(b) Develop formal site-specific procedures for the disposition of workers in the event of an attack.

(c) If the tactical conditions permit, workers may be evacuated to safe areas from prospective target locations and likely avenues of approach.

(d) 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 Tactical Response Force (TRF) is deployed in a strategic posture to interrupt, interdict, deny, and neutralize an adversary force attack. The TRF is armed and equipped with state of the art weaponry, tactical equipment, vehicles, and communication systems. The TRF is adept at implementing approved Security Incident Response Plans under adverse emergency conditions. The primary mission of the TRF is the protection of nuclear weapons, weapons components, and SNM from theft, sabotage, and unauthorized control. Ancillary duties include the safeguarding of classified information and other classified assets.

(1) Tactical Response Force Characteristics.

(a) Survivability

(b) Mobility

(c) Lethality

(d) Flexibility

(e) Speed

(f) Unpredictability

(g) Mutual Support

(h) Reliable communications

Vertical line denotes change.

(2) Tactical Response Force Element Missions. A site TRF is composed of small units/teams of no fewer than two SPO II and/or SPO III personnel, deployed in configurations that provide tactical advantages for both defensive and offensive operations.

(a) Special Response Team (SRT).

Mission: The SRT executes recapture/recovery and pursuit operations and supports interruption, interdiction, neutralization, containment, and denial strategies.

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.

Mission: Executes interruption, interdiction, neutralization, containment, and denial strategies and supports recapture/recovery and fresh pursuit operations.

Capabilities: SPO II personnel operate in small units with specialized weapons and equipment from mobile patrols/tactical vehicles and fixed posts.

(3) Tactical Response Force Support. All site Security Police Officers and Security Officers have a key role in supporting the overall site security posture and the TRF.

(a) Security Police Officer-I.

Mission: Supports interruption, interdiction, neutralization, containment, and denial strategies.

Capabilities: SPO I personnel operate from mobile patrols and fixed posts. SPO I personnel perform routine S&S related functions and are capable of performing specialized active defense functions such as staffing defensive fighting positions, operating Remotely Operated Weapon Systems (ROWS), and performing Central Alarm Station (CAS) duties.

(b) Security Officer.

Mission: Ensures routine security-related functions are maintained (e.g., access/egress control, escort duties, CAS operations).

Vertical line denotes change.

Capabilities: Unarmed SOs perform observation and reporting activities, logistical re-supply to other PF elements, message courier duties, and provide transportation support.

(4) Deployment Considerations.

(a) A layered, or zone, defensive strategy is implemented that maximizes the TRF'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.

(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 TRF member is issued at least one primary weapon along with a secondary firearm, such as a handgun, used principally for close quarters engagement or for transition in the event of a stoppage of the primary weapon.

(g) TRF weapons are capable of tactical operations in both day and night conditions.

(h) The TRF employs direct-fire weapons (e.g., machine guns, precision rifles, battle rifles, etc.) to engage and to neutralize adversary forces out to the maximum effective range of the weapon.

(i) As prescribed by the SSSP, the TRF employs indirect-fire or explosive projectile weapons (i.e., M3 MAAWS, MK19/GMG, M203, etc.) to deny access to target locations and to suppress and to neutralize adversary forces occupying positions of cover and/or concealment.

(j) TRF members are knowledgeable of adversary attack methods identified in the Design Basis Threat (DBT) 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."

(5) 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 (for a two-person crew, usually the gunner).

(d) Potential target access points are covered by suppressive fire weapons.

(e) TRF members utilize positions of cover and maximize the element of surprise to the extent possible.

(f) The TRF initiates a decisive engagement with adversary forces as far as possible outside the target location.

(g) nce an adversary has been identified and engaged, TRF elements never lose contact.

Vertical line denotes change.

(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) TRF teams, using suppressive fire weapons, maneuver in force against adversaries occupying covered positions.

(j) The TRF has plans in place to transition quickly from defensive to offensive operations.

(6) Recapture/Recovery Operations.

(a) The site PF is staffed and deployed in sufficient strength to ensure the protection of sensitive assets. The dedicated recapture/recovery element of the SRT is established with additional resources sufficient to ensure that recapture/recovery 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/recovery operations within identified target locations.

(c) SRTs possess the 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 SNM is at risk, regaining control of the SNM is the primary consideration.

(e) SRTs are supported by other TRF elements to the maximum extent possible as they move toward the target objective.

(f) TRF members provide overwatch for the assault team(s) movement, cover avenues of approach, and provide support by fire to the SRT as they breach/enter the target location.

(g) All TRF personnel are capable of providing direct support to the recapture/recovery mission by supplementing the main assault force, controlling the target area, and suppressing enemy defensive positions.

(7) Pursuit Operations.

(a) TRF members are trained and equipped to conduct Fresh Pursuit operations, on and off DOE property in accordance with DOE

M 470.4-3, Section A, Appendix A-1, "Guidelines for Fresh Pursuit."

(b) Fresh Pursuit operations are coordinated with responding Federal, State, and local law enforcement agencies according to approved agreements.

(c) TRF members use vehicle immobilization techniques and/or other means of applying deadly force to terminate the pursuit.

(d) TRF members maintain control of sensitive assets until relieved by cognizant Federal authorities.

(8) Weapons of Mass Destruction.

(a) All TRF and SPO-I personnel are trained and equipped to operate within an environment where weapons of mass destruction (WMD) (i.e., chemical, biological, or radiological weaponry) have been employed. PF training programs include tactical deployment in WMD personal protective equipment.

(b) TRF 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.

3. 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. A requirement for increased FOFs for training purposes does not always have to involve the very large scale exercises that are conducted during inspections and annual SSSP validations. 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.

Vertical line denotes change.

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 small and as few 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) There are inherent, but reasonable, risks of injury that must be accepted in the conduct of realistic PF training and operational performance while maintaining a prudent safety posture.

(4) Persons assigned as full-time staff PF instructors must be qualified in accordance with the provisions of DOE M 470.4-3, *Protective Force*, Section A, Chapter II, paragraph 9.

SECTION B—SECURITY CONDITIONS

1. OBJECTIVE. To ensure that the Department uniformly meets the requirements of the Homeland Security Advisory System outlined in Homeland Security Presidential Directive-3, (HSPD-3), dated 3-11-02, and provides the responses specified in Presidential Decision Directive 39, *U.S. Policy on Counterterrorism* (U), dated 6-21-95. The contractor is responsible for assisting the Department of Energy (DOE) in meeting its requirements under these documents as outlined in this contractor requirements document (CRD) and in other contractor requirements documents.

2. THREAT INDICATORS. While the DBT provides specific description of threats that all components of the safeguards and security (S&S) system must be capable of defeating, analysis of terrorism should be an ongoing process. Although each analysis relies on information included in previous assessments, judgments with respect to threats to Federal and DOE-affiliated personnel, facilities, and assets begin anew with each analysis.

   a. Homeland Security Threat Conditions [known in DOE as Security Conditions (SECONs)] 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. A threat indicator is a condition that when present increases the possibility of a terrorist incident. Seldom does one single indicator suggest that the threat is imminent, but when a number of indicators are present, the level of concern should increase correspondingly. A decision on assigning SECON must integrate a variety of considerations. This integration will rely on qualitative assessment, not quantitative calculation. Higher SECONs indicate greater risk of a terrorist act, with risk including both probability and gravity. Despite best efforts, there can be no guarantee that, at any given SECON, a terrorist attack will not occur. An initial and important factor is the quality of the threat information itself. The evaluation of this threat information includes, but is not limited to, the following factors.

      (1) To what degree is the threat information credible?

      (2) To what degree is the threat information corroborated?

      (3) To what degree is the threat specific and/or imminent?

      (4) How grave are the potential consequences of the threat?

   b. Local and site-specific threat analysis is a dynamic process because the threat and the countermeasures used to combat the threat are constantly changing. To keep up with possible changes in the threat, security professionals should develop a predetermined list of general and specific threat indicators. Threat indicators

should be revised according to site/facility situations and needs. They should be reviewed at least every 6 months or when a significant incident or change in conditions indicates that the threat level is increasing or decreasing. Examples of threat indicators that can be used to develop a site-/facility-specific assessment are listed below.

(1) International incidents or indicators against U.S. interests, personnel, or facilities.

(2) Domestic incidents or indicators against Federal or State interests countrywide.

(3) Local incidents or indicators directed against Federal or DOE interests.

(4) Specific targeting of DOE-affiliated personnel, facilities, or materials.

3. SECURITY CONDITIONS. The DOE SECON system has been aligned with the Homeland Security Advisory System.

a. The DOE SECON system describes a progressive level of common sense protective measures that may be implemented in response to a malevolent or terrorist threat to any or all DOE-affiliated facilities, assets, and personnel. The purpose of the SECON system is to establish standardized protective measures for a wide range of threats and to help disseminate appropriate, timely, and standardized information for the coordination and support of DOE crisis or contingency activities. Once a SECON level is declared, the associated protective measures should be implemented as soon as possible to the extent they apply to the individual site or facility. Cognizant security authorities must coordinate SECON status through their DOE points of contact as appropriate and notify the DOE Headquarters (HQ) Operations Center (OC) and Departmental element of the site/facility SECON status. Measures associated with each SECON are not prioritized but should be initiated concurrently when practical.

b. The National Nuclear Security Administration (NNSA) facilities must be prepared to respond to contractor requirements in SECON directives provided by the Under Secretary for Nuclear Security/Administrator, NNSA. Non-NNSA facilities must be prepared to respond to SECON directives provided by the Under Secretary for Energy, Science and Environment for their individual facilities. HQ facilities must be prepared to respond to SECON directives provided by the Director, Office of Security. At their discretion, DOE line management may increase protection measures for facilities under their cognizance if they determine that the local threat situation warrants additional security. In this event, the DOE HQ OC and Departmental element must be notified of the SECON level. If DOE line management or Departmental elements believe that their facilities' SECON levels should be less than those issued by the

Under Secretary for Energy, Science and Environment or the Under Secretary for Nuclear Security/Administrator, NNSA, a request for exception must be submitted for consideration (see paragraph 3c, below).

c. Any departure from the requirements of this section must be considered an exception which must be approved in accordance with the requirements set forth in Section M of this CRD. No exception is permitted to the protective measures when under SECON 1, Severe Condition (Red).

d. To the extent possible throughout each increase or decrease in SECON, the cognizant security authority must:

(1) keep employees informed;

(2) coordinate when appropriate with State and local officials' actions taken regarding security and emergency planning; and

(3) at each level of SECON, review Security Plans, and vulnerability assessments (VAs), emergency response procedures, public affairs guidance and plans, legal authorities, and Continuity of Operations Plans.

e. A record of specific actions taken for each measure must be maintained. A description of each SECON, including the necessary circumstances for implementing, the impact on operations, and the purpose of each protective posture, is outlined below.

(1) **SECON 5, LOW CONDITION (GREEN).** This condition is declared when there is a low risk of terrorist attacks. SECON 5, Low Condition (Green) exists when a general threat of possible malevolent or terrorist activity exists, but warrants only a routine security posture.

(2) **SECON 4, GUARDED CONDITION (BLUE).** This condition is declared when there is a general risk of terrorist attacks. SECON 4, Guarded Condition (Blue) applies when there is an increased general threat of possible malevolent or terrorist activity against personnel and facilities, the nature and extent of which are unpredictable, and circumstances do not justify full implementation of SECON 3, Elevated Condition (Yellow) measures. It may be necessary, however, to implement certain selected measures from higher SECONs to address intelligence received or to act as a deterrent. All measures selected for use under SECON 4, Guarded Condition (Blue) must be capable of being maintained indefinitely.

(a) Measure 1. At regular intervals, warn all personnel to report the following to security:

1 suspicious personnel, particularly those carrying suitcases or other containers, or those observing, photographing, or asking questions about site operations or security measures;

2 unidentified vehicles parked or operated in a suspicious manner on or in the vicinity of the site or near site facilities;

3 abandoned parcels or suitcases; and

4 any other activity considered suspicious.

(b) Measure 2.

1 Ensure that security personnel have immediate access to building floor plans and emergency/evacuation plans for all site facilities.

2 Ensure that security personnel are able to seal off an area immediately.

3 Ensure that key personnel required to implement security plans are on-call and readily available.

4 Maintain the site Emergency Management Team (EMT) on 2-hour recall.

5 Expand Operations Security measures.

6 Exercise bomb threat procedures.

(c) Measure 3. Secure and seal buildings, rooms, and storage areas not in regular use. Maintain a list of secured facilities.

(d) Measure 4. Increase unannounced security spot checks (inspection of personal identification; vehicle registration; and the contents of vehicles, suitcases, briefcases, and other containers) at access points for the site and facilities.

(e) Measure 5. Reduce the number of access points for vehicles and personnel to minimum levels consistent with the requirement to maintain a reasonable flow of traffic.

(f) Measure 6. As a deterrent, randomly apply measures 14, 15, 16, 17, or 18 from SECON 3, Elevated Condition (Yellow) either individually or in combination.

(g) Measure 7. Review all operations plans, personnel details, and logistics requirements that pertain to implementing higher SECONs.

(h) Measure 8. Review security measures for critical/sensitive personnel (e.g., directors, managers, members of special access/ security programs, etc.) and implement additional measures warranted by the threat and existing vulnerabilities (e.g., identified personnel should alter established patterns of behavior when traveling in public areas).

(i) Measure 9. Increase liaison with local law enforcement, intelligence community, security agencies, and the Federal Bureau of Investigation, (FBI) to monitor the threat to site personnel and facilities. Notify local law enforcement agencies and the FBI concerning SECON 3, Elevated Condition (Yellow) measures that, if implemented, could affect their operations in the local community.

(j) Measure 10. Reserve for site/facility use.

(3) **SECON 3, ELEVATED CONDITION (YELLOW).** A SECON 3, Elevated Condition (Yellow) is declared when there is a significant risk of terrorist attack. Elevated Condition (Yellow) applies when an increased and more predictable threat of malevolent or terrorist activity exists. The measures in this SECON must be capable of being maintained for lengthy periods without causing undue hardship, affecting operational capability, or aggravating relations with the local community. For measures requiring an increase in the frequency of a specific action, the new frequency is to be more often than in the lower-level security condition. In addition to the measures required by SECON 4, Guarded Condition (Blue), the following measures should be implemented.

(a) Measure 11. Increase the frequency of warnings required by Measure 1 and inform personnel of additional unclassified threat information, if available. Encourage increased community security awareness of suspicious persons, vehicles, and activities.

(b) Measure 12. Maintain EMT personnel on 2-hour recall; periodically exercise recall to ensure readiness. Keep all other personnel involved in implementing special response/contingency plans on call. Identify, contact, and brief specialists that may be required for unique contingencies; coordinate lines of communication.

(c) Measure 13. Review provisions of all operations plans and orders and special operating procedures associated with implementing SECON 2, High Condition (Orange).

(d) Measure 14. Move automobiles and objects such as trash containers, newspaper boxes, crates, etc., at least 30 yards from all facilities, particularly buildings of a sensitive or prestigious nature. Identify any areas where an improvised explosive device could be hidden (i.e., pallet stacks, trash piles, stacked construction supplies, etc.). If the configuration of the facility or area precludes implementation of this measure, take appropriate compensatory measures per local plans [frequent inspection by Explosive Ordnance Disposal (EOD) teams, if available, controlled access to parking areas, etc.]. Consider centralized parking.

(e) Measure 15. Secure, seal, and regularly inspect all buildings, rooms, and storage areas that can be isolated with minimum site impact.

(f) Measure 16. At the beginning and end of each work day and at frequent intervals, inspect the interior and exterior of buildings in regular use for suspicious activity or unattended packages and for signs of tampering or indications of unauthorized entry.

(g) Measure 17. Implement screening procedures for all incoming official mail to identify possible explosive or incendiary devices or other dangerous material. If available, have EOD-trained teams inspect suspicious items and screen mail periodically. Provide guidance concerning suspicious packages. Encourage employees to inspect their individual mail, report suspicious items to security, and refrain from handling such items until cleared by the appropriate authority.

(h) Measure 18. Inspect other deliveries and locally designated common-use facilities to identify explosives and incendiary, biological, or chemical devices. Use EOD-trained teams for some screening inspections when available. Instruct site personnel to report suspicious packages to security and refrain from handling them until cleared by the appropriate authority.

(i) Measure 19. Increase both overt and covert security force surveillance of locally designated soft targets to improve deterrence and build confidence among site personnel. (Covert surveillance must comply with DOE directives and appropriate regulatory restrictions.)

(j) Measure 20. Inform employees of the general threat situation. Limit visitors and escorted uncleared personnel. Periodically update all personnel as the situation changes to stop rumors and prevent unnecessary alarm.

(k) Measure 21. Brief representatives of all activities on the site concerning the threat and security measures implemented in response to the threat. Explain reasons for actions. Implement procedures to provide periodic updates for these activity representatives.

(l) Measure 22. Verify the identity of all personnel entering property protection areas (PPAs) and other sensitive activities specified in local plans (i.e., inspect identification badges and grant access based on visual recognition). Use of automated access control systems at interior security areas is acceptable and encouraged, where practical.

On a random basis, visually inspect the interior of all vehicles and the exterior of all suitcases, briefcases, packages, and other containers. Increase the frequency of detailed vehicle inspections (trunk, undercarriage, glove boxes, etc.) and the frequency of detailed inspections of suitcases, briefcases, and other containers.

(m) Measure 23. Increase the frequency of random identity checks (inspection of security badges and vehicle registration documents) conducted by security force patrols on the site.

(n) Measure 24. Remind all personnel to lock parked vehicles and inspect vehicles for suspicious items before entering and driving them.

(o) Measure 25. Implement additional security measures for critical/sensitive personnel in accordance with existing plans.

(p) Measure 26. Brief all security force personnel concerning the threat and policies governing rules of engagement, use of deadly force, and fresh pursuit. Ensure there is no misunderstanding of these instructions. Repeat this briefing on a periodic basis.

(q) Measure 27. Increase liaison with local police, intelligence, security agencies, and the FBI to monitor the threat to site personnel and facilities. Notify local police agencies concerning SECON 2, High Condition (Orange) or SECON 1, Severe

Condition (Red) measures that, if implemented, could affect their operations in the local community.

(r) Measure 28. Survey the surrounding area to determine whether operational activities near the area might create emergencies or contingencies that could affect the site/facility (e.g., airports, military/other Government facilities, industrial facilities, railroads or pipelines, etc.).

(s) Measure 29. Reserve for site/facility use.

(4) **SECON 2, HIGH CONDITION (ORANGE).** A SECON 2, High Condition (Orange) is declared when there is a high risk of terrorist attacks. This condition applies when an incident occurs or intelligence is received indicating that some form of malevolent or terrorist action against personnel and facilities is imminent. Implementation of measures in this security condition for more than a short period probably will create hardship and affect the routine activities of the site and its personnel. For measures requiring an increase in the frequency of a specific action, the new frequency is to be more often than in the lower level SECON. The following measures should be implemented.

(a) Measure 30. Continue all SECON 4, Guarded Condition (Blue) and SECON 3, Elevated Condition (Yellow) measures or introduce those that have not already been implemented.

(b) Measure 31. Recall staff representatives and initiate 24-hour operation of the EMT. Place the Special Response Team (SRT) on standby alert. Keep all personnel responsible for implementing special/response contingency plans at their places of duty. Review site evacuation plans.

(c) Measure 32. Reduce site access points to the absolute minimum necessary for continued operation.

(d) Measure 33. Verify the identity of all personnel entering the site/facilities, including appropriate offsite facilities under DOE control. Inspect all security badges for tampering. On a random basis, visually inspect the interior of all vehicles and the exterior of all suitcases, briefcases, and other containers. Increase the frequency of detailed vehicle inspections (trunk, undercarriage, glove compartments, etc.) and the frequency of inspections of suitcases, briefcases, and other containers.

(e) Measure 34. Implement centralized parking and shuttle bus service, where required.

(f) Measure 35. Ensure that security personnel have been briefed concerning policies governing the rules of engagement, use of force, and fresh pursuit, particularly criteria for use of deadly force. Ensure that non-security supervisory personnel are familiar with above policies and procedures, if applicable. Ensure that special equipment and ammunition are available for immediate issue.

(g) Measure 36. Increase security patrol activity to the maximum level sustainable. The concept of continuing random security patrol activity is encouraged.

(h) Measure 37. Position security force personnel in the vicinity of critical facilities.

(i) Measure 38. Erect barriers required to control direction of traffic flow and to protect facilities vulnerable to bomb attack by parked or moving vehicles.

(j) Measure 39. Consult local authorities about closing public roads and facilities that might make sites more vulnerable to terrorist attacks.

(k) Measure 40. Consider canceling public events.

(l) Measure 41. Consider initiating Continuity of Operations plans

(m) Measure 42. Reserve for site/facility use.

(5) **SECON 1, SEVERE CONDITION (RED).** A SECON 1, Severe Condition (Red) reflects a severe risk of terrorist attacks. This condition applies in the immediate area where a malevolent or terrorist attack has occurred that may effect the site or when an attack is initiated on the site. Implementing SECON 1, Severe Condition (Red) will create hardship and affect the activities of the site and its personnel. Normally, this SECON is declared as a localized response. For measures requiring an increase in the frequency of a specific action, the new frequency is to be more often than in the lower-level SECON. The following measures should be implemented.

(a) Measure 43. Continue all previous SECON measures and introduce those that have not already been implemented.

(b) Measure 44. Augment security forces to ensure absolute control over access to the site, facilities, and other potential target areas. Establish surveillance points; use night-vision devices.

(c) Measure 45. Working closely with facility management, identify the owners of all vehicles already on the site. In those cases where the presence of a vehicle cannot be explained (owner is not present and the vehicle has no obvious site affiliation), inspect the vehicle for explosives; incendiary, chemical, or biological devices; or other dangerous items and remove the vehicle from the vicinity of facilities, soft targets, and other sensitive areas as soon as possible.

(d) Measure 46. Inspect all vehicles entering the site. Inspections should include cargo storage areas, undercarriage, glove boxes, and other areas where explosives, incendiary, chemical, or biological devices or other dangerous items could be concealed.

(e) Measure 47. Limit access to the site, facilities, and other areas to those personnel with a legitimate and verifiable need to enter. Implement positive identification of all personnel. No exceptions.

(f) Measure 48. Inspect all baggage such as suitcases, packages, and briefcases brought on the site for explosives, incendiary, chemical, or biological devices, or other dangerous items.

(g) Measure 49. Implement frequent inspections of the exterior of buildings (including roof areas) and parking areas. Conduct inspections at facilities and in the vicinity of soft targets.

(h) Measure 50. Coordinate with the Operations Center to establish communications, responsibilities, and authorities before, during, and after attack.

(i) Measure 51. Request that local authorities close those public roads and facilities in the vicinity of the site/facilities that might facilitate execution of a malevolent or terrorist attack.

(j) Measure 52. Cancel public events.

(k) Measure 53. Execute Continuity of Operations plans.

(l) Measure 54. Reserve for site/facility use.

SECTION C—SITE SAFEGUARDS AND SECURITY PLANS

1. OBJECTIVE. The Site Safeguards and Security Plan (SSSP) is a risk management document that provides summary information used to describe safeguards and security (S&S) programs and vulnerability and risk assessments at applicable sites. The objective of this section is to delineate SSSP content and establish a standard approach to presenting site protection information and vulnerability assessment (VA) results. The results and conclusions contained in the plan are intended to guide long-term planning for site S&S operations. This is accomplished during plan development by identifying: key site protection elements; annually (at least every 12 months) evaluating site protection in terms of its adequacy to meet continued mission and threat parameters; and, identifying resource requirements.

2. APPLICATION. The SSSP is used to evaluate site and facility program elements and resources as they relate to identified threats and risks. The protection measures identified in approved SSSPs become the basis for executing, and reviewing site protection programs.

3. SCOPE. The approved SSSP provides assurance that S&S measures address identified threats and risks. To provide this assurance, the plan must reiterate the assumptions identified to and agreed upon by line management. These assumptions must include reference to the contract under which the site is operated and those contractual issues that may impact S&S, applicable contract requirements, the threat upon which VAs are based, the methodology used to conduct VAs, deviations and proposed deviations, and any unique S&S impacting issues and assumptions that were addressed and agreed to by the responsible parties.

4. PURPOSE. The SSSP describes the graded protection of DOE assets required to be implemented by line management. The SSSP identifies site risks, cost-benefit analyses, and comparison of proposed upgrades. The resource plan (RP) must identify near- and long-term resource requirements needed to ensure the integrity of existing and planned S&S upgrades. The annual (at least every 12 months) review serves as the basis for tracking the implementation of protection measures and strategies necessary to maintain system effectiveness and identifies unfunded requirements.

5. PLAN COMPOSITION. The SSSP includes:

   a. references to implementing documents and evidence files;

   b. descriptions of site protection strategies, key site S&S programs, approved and pending deviations, plans and procedures designed to implement, manage and maintain S&S programs;

c. system effectiveness determinations for the protection of special nuclear material (SNM), prevention of mitigation of sabotage events, and prevention and/or timely detection of the loss of classified information or matter based on the status of performance indicators, such as results of VAs, performance tests, surveys, inspections, and evaluations of personnel qualifications and training;

d. proposed S&S program upgrades;

e. VA results that support conclusions reported in the SSSP;

f. assumptions used as part of the VA process;

g. threat parameters used for VAs that are described in the current DBT, regional threat assessments, and impacts made by local area threat assessments, if applicable;

h. the details of the changes in the protection through the spectrum of SECON (1-5), to include effects on the calculated baseline system effectiveness;

i. a description of the evidence files containing material that supports the VAs; and

j. a RP that describes S&S upgrades programmed for completion, upgrades being introduced as a result of planned and unplanned site changes impacting the protection program or deficiencies identified as a result of the annual (at least every 12 months) review of the SSSP, a description of the funding source to implement the upgrades, and unfunded requirements.

6. EVIDENCE FILES. Supporting documentation that validates data/information used in the VA process and in other protection program planning presented in the plan and that may require corroboration must be available in evidence files. Evidence files must be maintained to provide VA process and other protection program planning documentation in a logical and readily retrievable form to validate assumptions, modeling input data, test results, and other data that may be used to support protection systems design or conclusions regarding protection effectiveness.

7. DATA COLLECTION. The effective date (snapshot in time) of the data contained in the SSSP must be specified.

8. FORMAT. Information provided in the SSSP should be brief, accurate, and concise. Implementing plans and procedures should be referenced in the plan where appropriate. A brief overview of a plan or procedure is adequate.

Duplication of information should be avoided. Information already included in other sections of the plan may be referenced or summarized for clarity.

A cover letter must be attached to the plan indicating that the plan has been reviewed, risks acknowledged and accepted (if appropriate), and signed by line management. For example, the SSSP should be approved by the Head of the Field Element and submitted for concurrence to the Departmental element. If high or marginal risk acceptance is needed, the correspondence must be routed for signature to the Secretary of Energy or Deputy Secretary or Under Secretaries, respectively.

The use of charts, plats, graphs, drawings, videos, photographs, and matrixes is encouraged wherever appropriate to clarify or satisfy the intent of plan objectives. References to sources of information and the location of supporting documentation should be provided to assist in verifying information contained in the plan.

The SSSP is divided into 12 chapters. Each chapter provides specific information relevant to site security. Use of this layout will ensure a uniform SSSP for review and comment or during an emergency.

a. Chapter 1, Site Description and Mission.

(1) Site Mission Statement. Describe the site mission and how the mission relates to national security and the health and safety of the public, employees, and the environment. Describe the major programs or activities performed at the site in terms of mission and their relationship to the DOE national security mission.

(2) Site Description and Area Layout. Describe the physical and geographical area in which the site and the S&S program are located. Provide a map, photograph, or drawing of the site that identifies locations of Category I facilities, facilities with credible roll-up of SNM to a Category I quantity, the central alarm station (CAS) and secondary alarm stations (SAS), security-related communications facilities, and other facilities of security interest. Show the location of barriers defining the site protected area (PA). A small-scale map or drawing should be used to show the relationship of the site to the surrounding area and be of sufficient detail to orient the user.

(3) Management Organization, Planning Assumptions and Evidence File.

(a) Site Management Organizations. Identify the contract name, number, and other information that describes the authority under which the contractor executes management functions. Identify site contractors responsible for S&S programs and describe their S&S activities. Provide Federal and contractor organization charts and identify key positions and the relationships between the organizations for S&S activities. Provide a list of roles and responsibilities for key positions. Describe Federal and contractor involvement in the development of S&S resource requirements.

(b) Management and Planning Assumptions. Describe those assumptions that were addressed and agreed to during the SSSP scoping, preparation, or other SSSP management related meetings.

Describe all relevant S&S-related planning assumptions that were formerly agreed to and included in a Memorandum of Agreement (MOA) by the responsible organization representatives who are party to the development and review of the SSSP. These assumptions should address the following issues:

1 site SECON;

2 VA methodology used for insider, neutralization, outsider, and collusion analyses;

3 identified credible targets;

4 protection strategies;

5 approved compensatory measures; and

6 performance testing conducted or to be conducted.

(c) Evidence Files. Describe and identify the contents, location, and control mechanisms for the SSSP evidence files. Reference approved standard operating procedures (SOPs) as applicable. Supporting documentation that validates data/information used in the VA process should not be included in the SSSP. However, this data/documentation should be available in a logical and readily retrievable arrangement in evidence files, for use in review and validation of the SSSP.

b. Chapter 2, Site Threat Description and Target Identification.

(1) Threat Description. Establish a graded approach to protection for Category I SNM and SNM facilities with credible roll-up of SNM to a Category I quantity and facilities having radiological, biological, or chemical sabotage event potential and facilities having disruption of critical mission event potential. Use the DBT as the baseline for threat determination, along with higher levels of threat dictated by local and regional threats (when available), and describe the site-specific threats used as the basis for conducting VAs and for which the protection program is designed.

(2) Target Identification. Identify, describe, and prioritize targets of security interest that meet the following criteria.

(a) Category I quantities of SNM and the facilities with credible roll-up of SNM to a Category I quantity.

(b) A radiological, biological, or chemical sabotage inventory that, if released, would cause an unacceptable impact on national security or the health and safety of employees, the public, or the environment.

(c) Critical national security facilities, and assets (as defined in the DBT), designated by the Department (e.g., or each disruption of critical mission target) that would impact DOE programs supporting national defense and security.

(d) Those facilities possessing automated information systems that process or contain Sensitive Compartmented Information (SCI), Special Access Program (SAP), and weapon data classified Secret/Restricted Data (S/RD) Sigma 1, 2, 14, and 15 or higher.

(e) Temporary recurring targets. When predictable programmatic operations can reasonably be expected to present temporary SNM, sabotage, or information targets such as those permanent locations previously described, these targets must be described and analyzed at the same level of detail and in the same manner as permanent locations.

Provide a brief introductory description of the targets and a chart or list, such as shown below, that indicates the type of target, its location, attractiveness level, size, and configuration. Include SNM theft/diversion targets; radiological, biological, and chemical targets; and disruption of critical mission targets and those facilities possessing automated information systems that process SCI, SAP, weapon data classified S/RD Sigma 1, 2, 14, and 15 or higher.

(3) Theft or Diversion of SNM. Describe how Category I SNM targets and credible roll-up quantities of SNM to a Category I quantity have been identified and evaluated as potential abrupt theft targets. Also, describe how these SNM targets have been identified and assessed for protracted theft (diversion), if applicable.

For each identified SNM target, provide a description of the following, using a table similar to Table C-1, SNM Theft/Diversion Targets: physical location of identified SNM; the type of material, as described under the

several material listings in the contractor requirements in DOE M 470.4-6, *Nuclear Material Control and Accountability*, such as pure products, high-grade material, weapons, including pits, ingots, oxide fuel elements, etc.; and the Category (I through II) and attractiveness level (A through C) of the target material.

Table C-1. SNM Theft/Diversion Targets

Location	SNM Type	Category/ Attractiveness Level	Goal Quantity/ Portability
Bldg. 1, Vault	Pu-239 ingots	Cat. I/B	2 ingots/ man portable
Bldg. 1, Assay Room	Pu-239 ingots	Cat. I/B	2 ingots/ man portable
Bldg. 1, Fabrication Room	Pu-238 oxide powder	Cat. II/ D	2 canisters/ man portable
Bldg. 2	U-235 fuel elements	Cat. II, roll-up to Cat. I/C	20 fuel elements/ not man portable
Bldg. 3	U-235 fuel elements	Cat. II, roll-up to Cat. I/C	20 fuel elements/ not man portable

(4) Radiological Sabotage. Indicate the process or methodology used to identify and evaluate radiological sabotage targets.

For each identified radiological sabotage target, provide a description using a table similar to Table C-2, Radiological Sabotage Targets, of the following: the physical location of all identified targets; the type of material; the maximum inventory level; and the material size and configuration.

(5) Biological or Chemical Sabotage. Describe the methodology used to evaluate biological or chemical targets. Using the criteria referenced in the DBT, determine the sabotage threat level (STL) for each location. Reference the plans and procedures that govern the biological or chemical sabotage assessment program.

For each identified target type not addressed by the commercial equivalency protection program, provide a description of the following using a table similar to Table C-3, Biological/Chemical Sabotage Targets: the physical location of additional identified biological or chemical sabotage material targets; the type of material; the maximum inventory

level; the material size and configuration; and, the exposure level at the near-site boundary (NSB) for maximum inventory release.

Table C-2. Radiological Sabotage Targets

Location	Material Type	Maximum Inventory	Material Size and Configuration
Bldg. 1, Fabrication Room	Pu-238 oxide powder	10 kg	Paint Cans, at 50 g each
Bldg. 4	H_3 gas	10 kg	Cylinders, at 500 g each

Table C-3. Biological/Chemical Sabotage Targets

Location	Material Type	Maximum Inventory	Material Size and Configuration	Exposure Level at NSB
Bldg. 5	Chlorine	10,000 lb	55-gal drums, at 350 lb each	>ERPG III Levels

(6) Disruption of Critical Mission Sabotage. Describe how potential disruption of critical mission sabotage production and process components (machinery, equipment, flow process, power sources, ventilation, waste handling, etc.) have been identified and evaluated for inclusion as disruption of critical mission targets. Ensure that the evaluation includes how the sabotage event would affect production (at the facility, on intersite processes, and on overall national level inventory needs) and, if so, what areas, processes, and/or components within the facility affect those necessary production level capabilities and inventory needs.

For each disruption of critical mission target, provide a description, using a chart similar to Table C-4, of the following: the physical location of essential production components; the type of equipment, process, power sources, or vital components; and the dollar value or production capability loss.

(7) Intra-Site Transportation of SNM. Describe in a brief narrative the Category I SNM targets and credible Category II SNM targets that roll up to Category I quantity that are moved from one location to another on the site on a recurring basis.

Using a chart, identify the type of SNM, attractiveness level, and size and configuration of the material.

Table C-4. Disruption of Critical Mission Targets

Location	Equipment Type	Loss of DOE Mission Capability and Mission Impact
Bldg. 1, Fabrication Room	Fuel Fabrication Presses	100% loss of capability for 360 days with moderate mission impact
Lab. A	Laser Tunnel	100% loss of capability for 360 days with low mission impact

c. Chapter 3, Site Protection Strategies. Identify the protection strategies employed that address the overall protection program and enhance the concept of graded protection. Describe the protection program strategies employed. The basic strategies pertaining to protection are denial of access, denial of task and containment that upon failure could evolve into recapture/recovery or pursuit strategies. Protection programs and tactical deployments designed to prevent unauthorized control of material and devices and to prevent acts of radiological, biological, chemical, and disruption of critical mission must be integrated with protection strategies. These activities could include protection layers of intrusion detection systems (IDS) and concentric security areas, access control measures, compartmentalization, insider protection programs, and procedural measures. The plan should clearly convey the strategy to be employed, and plan reviewers will anticipate that procedures are available to ensure implementation of these strategies. Display in a chart similar to Table C-5, Site-Wide Protection Strategies, the protection strategy used, the facility and target involved, and the title and responsible office for each plan or procedure. Ensure the information provided is consistent with that found in Chapter 2, Site Threat Description and Target Identification.

d. Chapter 4, Physical Protection Systems.

(1) Summary of Physical Protection Systems Used for Category I and Credible Roll-Up Quantities of SNM to a Category I Quantity, Sabotage, Classified Information or Matter, and Classified Automated Information Protection. Describe the physical protection systems for each facility that has Category I quantities of SNM; credible roll-up quantities of SNM to a Category I quantity; and radiological, biological, chemical, and sabotage targets (including disruption of critical mission) and those facilities possessing automated information systems that process or contain SCI, SAP, weapon data classified S/RD Sigma 1, 2, 14, and 15, or higher. Provide a narrative description of the physical protection systems and how these systems are integrated at the site and facility level. Describe how

Vertical line denotes change.

physical protection systems (access control, intrusion detection, assessment, etc.) are implemented to allow the PF to focus resources on its primary mission of defeating an armed terrorist threat. Describe how the barriers are protected by an IDS, security lighting, protective force (PF), and assessment systems and how structures located in or on the barrier are protected so as not to degrade protective systems. Describe the design of barrier systems used to deny vehicle approach routes to critical targets.

Following the narrative, complete a chart similar to Table C-6, Facility Protection Systems, that includes the following facility protection systems: security areas and their barriers, access controls (automated card access for both interior and exterior locations and contraband screening by the PF at Protected and Material Access Areas); assessment [closed circuit television (CCTV) and/or PFs both interior and exterior]; security computer system integrator/ processor; CAS and SAS; CCTV cameras monitoring and switching systems; security lighting; electrical and back-up power sources (emergency batteries and/or generators); and communications. In the chart, list the major physical protection systems, the location of the systems, and a brief description of the type of equipment installed.

Table C-5. Site-Wide Protection Strategies

Protection Strategy	Facility or Activity	Target Type	Implementing Plan or Procedure	Responsible Office
Denial of Access	Facility ABC	Cat. I: Pu metal oxide Cat. II: nitrate UF_6	Plan ABC 1.3	Protective Force Manager
Containment	Vault storage Areas 301, 302, and 303	Weapon parts and Pu metallic buttons	Plan ADC.1	Protective Force Manager
Denial of Task	SNM in transit	Weapon parts	Plan CFE 1.5	Protective Force Manager

(2) Physical Protection Measures for Category I and Credible Roll-up Quantities of SNM to a Category I Quantity in Transit (Onsite). Describe the types, frequency, and protection measures used for the intra-site shipment of Category I SNM and credible roll-up quantities to a Category I quantity. Provide a narrative that describes the typical physical

Vertical line denotes change.

protection measures taken to ensure the integrity of those shipments from their point of loading, through transit, and at the off-load destination. If other materials are transported onsite that would represent a STL-1 concern, provide a narrative that describes the typical physical protection measures from their point of loading, through transit, and at the off-load destination.

Table C-6. Facility Protection Systems

Protection System	Equipment Description	Location	Responsible Office
Exterior Intrusion Detection	"H" Field	Protected Area Perimeter Associated Areas	Office of the Plant Engineer
Exterior Assessment/ CCTV	Microwave Taut Wire CCTV System	Protected Area Perimeter Associated Areas	Office of the Plant Engineer
Interior Intrusion Detection	Volumetric Infrared Motion Detectors	All Material Access Areas	Office of the Plant Engineer

e. Chapter 5, Site PF.

(1) PF Mission, Organization, and Capabilities. Describe the PF organization and equipment deployed to perform 24-hour-per-day protection. Confirm that the basis for PF organization and planning is based on the identified site threat. Provide a narrative summary of the PF mission(s), capabilities, and deployment concepts used for site protection. Describe the methods used to review and prioritize post assignments priorities and eliminate posts that detract from combat readiness at high priority sites. Indicate the availability of plans and procedures that address normal and emergency deployment. Describe the PF equipment used including firearms, communications, vehicles, and any special items. Provide an organization chart of the PF, including response forces, showing the management and organization structure and key organizational interface positions with the cognizant security authorities and site operations and safety organizations. Using a schematic, display the PF communications network and include available secure networks and linkages to offsite law enforcement organizations with whom support agreements exist. In a chart, show the weapons and special equipment assigned to PF personnel, including members of the response force.

(2) Qualifications and Training. Indicate that the qualifications for hire and training of the PF conform to current policy requirements. In a chart similar to Table C-7, Qualifications and Training, list the titles and offices

responsible for implementing and maintaining the plans or procedures that describe the following pertaining to the PF: qualifications for employment and the hiring process; initial, specialized and advanced training; tactical performance testing program; and other relevant written documentation, such as post and general orders that enhance the efficiency and effectiveness of the PF.

(3) Special Response Teams (SRT) and Plans. Ensure the availability of SRTs and current response plans and procedures for implementing site-specific S&S program strategies and tactics for denial of access, denial of task, containment, recapture/recovery, pursuit, and contingency operations, as described in current DOE policy. Indicate that requalification training and exercises are used to verify the effectiveness of SRTs. Identify and document agreements and MOUs with local, State and Federal law enforcement agencies regarding requests for on-site support during a contingency event. Ensure that a VA was used to assist management in determining the equipment and deployment of SRTs. In a brief narrative, confirm the availability of personnel and response plans and procedures that provide assurance of adequate protection. Indicate that contingency plans and procedures are available to respond to the activities listed below.

(a) Containment/denial of access/denial of task (includes a range of tactical options designed to either preclude adversary force access to nuclear weapons/materials or to deny unauthorized removal).

(b) Recapture/recovery or pursuit operations (used when containment/ denial fail and could involve SRTs and other force options including the use of off-site law enforcement agencies).

Describe the organization, equipment, and training provided to SRTs and how training and performance testing are used to verify the effectiveness of SRT planning in the strategies described above. Describe the role of vulnerability analysis in determining SRT deployment, equipment, and training.

In a chart similar to Table C-7, list tactical response plans and procedures and the office responsible for implementing and maintaining them.

Use a similar chart to list memoranda or letters of understanding and other agreements with local, State, or Federal law enforcement agencies regarding requests for onsite support during a contingency event.

Vertical line denotes change.

Table C-7. Qualifications and Training

Plan/Procedures Title	Responsible Office
Specialized Training Plan	Training Department
Tactical Response Plan	

f. Chapter 6, MC&A Program.

Describe the MC&A management program and summarize the results of the MC&A vulnerability analyses and other MC&A program planning activities. Describe the mission of the site MC&A organization. Summarize current and planned nuclear materials processing and storage activities. Using an organization chart, show the MC&A organization and management structure and the lines of authority and points of interface with other S&S programs, facility operations, and the cognizant security authorities' MC&A organization. Describe the functions and responsibilities of safeguards personnel and indicate how MC&A activities are integrated with those of site protection programs and other facility organizations; include organizational responsibilities for those program elements that support multiple S&S programs (e.g., portal monitors and access controls). Confirm that MC&A personnel complete required training.

List, in a chart similar to Table C-8, MC&A Plans and Procedures, the facilities required to develop and maintain MC&A plans and procedures, the titles of those plans and procedures, and the office(s) responsible for approving and maintaining them.

Table C-8. MC&A Plans and Procedures

Facility Name	Plan/Procedure Title	Responsible Office(s)
ABC Facility	ABC Facility MC&A Plan, 1/1/99	S&S Director
XYZ Facility	XYZ Facility MC&A Plan, 6/9/99	S&S Director

Give the name(s) and date(s) of reports of MC&A VAs and other planning exercises. Summarize the results of these assessment(s). Identify those components of the MC&A system that provide the greatest effectiveness against theft and diversion. Describe actions taken to remediate identified program deficiencies or to prepare for planned changes in facility nuclear materials processing and storage activities.

g. Chapter 7, Site Personnel Security/Human Reliability Programs (HRP). Describe the site-wide program for personnel security that, in conjunction with information and physical security programs, ensures only authorized access to classified information or matter, or SNM and confirms that the personnel security program is in conformance with and implements the requirements prescribed in current DOE policy. Describe the key elements of the site-wide personnel security program for access authorizations and, if applicable, the key elements of the site's HRP. Describe the method(s) used at the site to ensure the appropriate level of access authorizations are issued for the category of material processed or stored at the site and for approving justification, processing, and reevaluating the need for such access authorizations. Indicate how the effectiveness of the program is assessed. Indicate the site procedures that require contractors to perform pre-hire checks to ensure proper qualifications and suitability of the applicant before submitting requests for access authorizations. Briefly describe the programs used to mitigate the effectiveness of potential "insider" activities and the application of these programs in addressing insider concerns. Provide an organization chart showing the location of the personnel security organization in relationship to the cognizant security authority and other contractor S&S organizations. Provide an organization chart identifying the designated HRP management official in relationship to the cognizant security authority and the designated HRP certifying official. Verify that the site has a current HRP implementation plan. List, in a chart similar to Table C-9, Personnel Security/Human Reliability Program Implementation, the titles of site-wide personnel security-related plans and procedures, the HRP implementation plan, if applicable, and the office(s) responsible for implementing and maintaining them.

Table C-9. Personnel Security/Human Reliability Program Implementation

Plan/Procedure Title	Responsible Office
XYZ Implementation Plan	Security Department

h. Chapter 8, Automated Information Security Program. Briefly describe the automated information systems for those facilities possessing automated information systems that process SCI, SAP, weapon data classified S/RD Sigma 1, 2, 14, and 15, or higher. Provide an organization chart showing the responsible automated information systems security program and its relationship to the cognizant security authority and contractor organizations.

List, in a chart similar to Table C-10, Automated Information Systems Security Programs, the title of the automated information systems security program plans and procedures with the associated office responsible for implementing and

maintaining the plan and procedures, the plans and procedures governing the automated information system VAs with the associated office responsible for implementing and maintaining the plan and procedures, and the reports containing the results of the VAs.

i. Chapter 9, S&S Equipment Maintenance and Testing Programs. Describe maintenance and testing programs and life cycle planning, designed to enhance the continuous operability of S&S-related equipment used in the protection of Category I SNM, (including areas with credible rollup of SNM to a Category I quantity), and classified automated information systems. Summarize, in a narrative, the maintenance and testing programs that ensure the availability and operability of S&S-related equipment and systems. Indicate the availability of compensatory measures/procedures that are used when equipment is taken out of service or otherwise not available. Describe how S&S maintenance and testing programs are incorporated into the Performance Assurance Program Plans. Indicate how the performance testing and other S&S site and facility maintenance programs comply with DOE policy.

Describe the life cycle planning conducted for major S&S equipment and component replacement. Relate how this planning is used to support and validate S&S equipment budget requirements.

Table C-10. Automated Information Systems Security Programs

Plan/Procedure/Report Title	Responsible Office	Date (if pertinent)

List, in a chart similar to Table C-11, the maintenance, testing, and records management programs; the relevant plans and procedures that implement the programs; and the responsible office, as these programs apply to equipment used by the PF, security related systems, and equipment and instrumentation used for MC&A. Many of these may be addressed in a single maintenance and testing program.

Describe the records management program used for scheduling, recording, and tracking identified S&S maintenance requirements, deficiencies, and testing schedules.

j. Chapter 10, Site Protection Evaluation Program. Chapter 10 is designed to ensure the availability and use of testing and evaluation programs for site S&S programs and systems.

In a narrative, describe the programs available and used to evaluate the effectiveness of S&S protection programs and the interaction of these evaluation tools (i.e., surveys may focus on shortfalls found in security inspections). Include in this narrative outline the PF tactical performance testing program describing the evaluation mechanisms used by line management. At a minimum, the programs described in Chapters 4, 5, 6, and 8 of the SSSP should be addressed and the evaluation plan or procedure identified. In a chart similar to Table C-12, Site Protection Program Evaluation Program, list the names of the evaluation plans/procedures used by the cognizant security authority to assist in determining the effectiveness of site and facility protection programs and systems. List the office responsible for the evaluation plan/procedure and its purpose.

Indicate, in a brief description, that performance testing is used to verify the effectiveness of S&S systems/programs and to validate vulnerability analysis activities. Additionally, briefly describe barriers and other systems that cannot be adequately performance tested to demonstrate protection capabilities and their integration into protection strategies due to physical, operational, or policy parameters.

k. Chapter 11, Deviations from DOE Contractor Requirements.

List all deviations that have been approved. In a table similar to Table C-13, Deviations from DOE contractor requirements, list the deviation, the officially assigned deviation number, the directive reference (DOE contractor requirement and section within the contractor requirement), and the dates the deviation was approved and expires.

Provide similar information for those deviations pending approval. This information should be displayed in a chart similar to Table C-14, Pending Deviations from DOE Contractor Requirements.

l. Chapter 12, Summary of Vulnerability Analyses and Risk Assessment Results.

(1) Executive Summary. Summarize the vulnerability analyses and risk assessments results for Category I SNM, (including credible roll up of SNM to a Category I quantity), theft targets, radiological, biological, and chemical sabotage targets, and disruption of critical missions.

Confirm in the narrative that performance testing was used to validate VA input data and the results of the vulnerability analyses. Following the narrative, complete a matrix similar to Table C-15, Summary of Identified Risks, which identifies the risk associated with the results of the vulnerability analyses. In Part 10 of the matrix, summarize the proposed corrective actions or upgrades. For line item construction project (LICP)

Vertical line denotes change.

work or other major capital expenditures, cite the source of the required funding. Use the RP information as the basis for this summary.

(2) Scope. Describe the targets to be covered, the items/issues to be excluded, and the limits on the conduct of the VAs in this SSSP.

Table C-11. S&S-Related Maintenance, Testing, and Records Management Programs

Program Area	Plan/ Procedure Title	Test Plan or Management Plan	Responsible Office/Organization
PF - Equipment - Training Courses - Firearms Qualification - Other			
Vehicles/Aircraft			
Communications			
MC&A			
Security Systems - Personnel Access and Inspection Equipment - Security Lighting - Intrusion Detection and Assessment Systems - Electrical Power Supplies			
Sensitive Area Access Control			
Survey/Inspection Deficiencies			

Table C-12. Site Protection Program Evaluation Program

Plan/Procedure Name Or Title	Responsible Office	Plan or Procedure Goal/Purpose
Performance Assurance Program	Contractor Manager	Establish/confirm system effectiveness
DOE/Contractor Self-Assessment Program	Program Manager	Identify program strengths/weaknesses
Facility Approval, Security Surveys	Cognizant Security Authority	Confirm availability and adequacy of required S&S programs
Force on Force Exercises	Contractor Manager	Confirm system effectiveness
Limited Scope Performance Tests	Contractor Manager	Confirm system effectiveness
Joint Tactical Simulation Model	Contractor Manager	Confirm system effectiveness

Table C-13. Deviations from DOE Contractor Requirements

Deviation Description	Deviation Number	CRD Directive Reference	Approval and Expiration Dates

Table C-14. Pending Deviations from DOE Contractor Requirements

Deviation Description	Deviation Number	CRD Directive Reference	Approval And Expiration Dates

(3) Methodology.

(a) Theft or Diversion of SNM. Identify the SNM targets subject to theft and/or diversion. Describe the rationale and mechanism used to identify these targets.

Using a table similar to Table C-16, SNM Theft/Diversion Targets, provide a description for each identified SNM target consisting of the following: the physical location of identified SNM; the type of material (such as pure products, high grade material, weapons, etc.) which could include pits, ingots, oxide fuel elements, etc.; the Category (I through II) and attractiveness level (A through E) of the target material; and the size and portability of the theft target.

(b) Radiological Sabotage. Identify the radiological targets subject to sabotage. Describe the rationale and mechanism used to identify these targets. A key source of information to assist in the identification and/or elimination of radiological targets is the facility safety analysis report. Using a table similar to Table C-17, Credible Radiological Sabotage Targets, provide a description for each identified radiological sabotage target consisting of the following: the physical location of all identified targets, the type of material, the maximum inventory level, and the material size and configuration.

(c) Biological Sabotage. Identify the biological targets subject to sabotage. Describe the rationale and mechanism used to identify

these targets. Reference any policy and analyses external to the SSSP that address biological targets.

Using a table similar to Table C-18, Credible Biological Sabotage Targets, provide a description for each identified biological sabotage target consisting of the following: the physical location of all identified targets, the type of material, the maximum inventory level, and, the material size and configuration.

(d) Chemical Sabotage. Identify the chemical targets subject to sabotage. Describe the rationale and mechanism used to identify these targets. Indicate whether security protection provided for chemical sabotage targets is comparable to that provided by the commercial sector for similar materials. A key source of information to assist in the identification and/or elimination of chemical targets is the facility safety analysis report. Reference any policy and analyses external to the SSSP that address chemical targets.

Using a table similar to Table C-19, Credible Chemical Sabotage Targets, provide a description for each identified chemical sabotage target consisting of the following: the physical location of all identified chemical sabotage targets, the type of material, the maximum inventory level, how the security provided is not comparable to that of the commercial sector, the material size and configuration, and the exposure level at the NSB for maximum inventory release.

(e) Disruption of Critical Mission. Identify the disruption of critical mission targets. Describe the rationale and mechanism used to identify these targets. Ensure that the evaluation includes how the disruption would cause an unacceptable impact on national security.

Using a table similar to Table C-20, Disruption of Critical Mission Targets, provide a description for each identified target consisting of the following: the physical location of the target; a description of the function of the target; the impact to national security; and the estimated time for recovery.

Table C-15. Summary of Identified Risks

Target Number	Target Location and Description	Threat Type and Number		Risk Rating (High, Moderate, Low) Base Case	Current Modif. Rating (date)	Protected Action and Adjusted Rating: Near-Term (<2 yr) (date)		Protected Action and Adjusted Rating: Long-Term (>2 yr) (date)		Remarks	Analyses Validated by Perf. Testing
(1)	(2)	(3)		(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)
SNM Theft Targets											
1	Glovebox 112-A Bldg. 222	Terrorist, X outsiders with help of insider	High	High	Relocate SI to access door	Mod	Harden access portal	Low		Install hardware to allow SL relocation (FY-89 GPP)	Yes
2	Test samples in NDA room, Bldg. 222	Criminal Insiders	High	High	Enhance HRP for NDA technicians and supervisors	High	Install CCTV recording for post-review of activities in NDA room	Mod		SNM protection unchanged, but probability of attempt reduced thru HRP and delayed assessment capability	Yes
Radiological Sabotage Targets											
3	Test reactor #5 North Area, Bldg. 408	Inside	Mod	Mod	Reinforce SI number when in use	Low	None	Low		Use overtime when reactor in use-3 times per year	No
Chemical Sabotage Targets											
4	Laboratory Bldg. 4	Insider	Mod	Mod	None	Low	None	Low		None	No
Biological Sabotage Targets											
5	Fabrication Room, Bldg. 1	Insider	Mod	Mod	None	Low	None	Low		None	No
Disruption of Critical Mission Targets											
6	Access port 4 D-line process line, Bldg. 460	Disgruntled employee	High	Mod	Implement 2-man rule	Low	Harden and remote control of portal	Low		Install hardware to reduce high manpower costs (use FY-92 GPP)	Yes
7	Extrusion equipment in fuel manufacturing area, Bldg. 97	Psychotic employee	High	High	Establish spares inventory for long lead time parts	Mod	Identify alternate extrusion capability off-site	Low		Additional physical protection not cost-effective. Improved spares also provide repair capability for non-sabotage outages	Yes

Table C-16. SNM Theft/Diversion Targets

Location	SNM Type	Category/ Attractiveness Level	Goal Quantity/ Portability
Bldg. 1, Vault	Pu-239 ingots	Cat. I/ B	2 ingots/ man portable
Bldg. 1, Assay Room	Pu-239 ingots	Cat. I,/B	2 ingots/ man portable
Bldg. 1, Fabrication Room	Pu-238 oxide powder	Cat. II, D	2 canisters/ man portable
Bldg. 2	U-235 fuel elements	Cat. II, roll-up to Cat. I/ C	20 fuel element/ not man portable
Bldg. 3	U-235 fuel elements	Cat. II, roll-up to Cat. I/ C	20 fuel element/ not man portable

Table C-17. Credible Radiological Sabotage Targets

Location	Material Type	Maximum Inventory	Material Size and Configuration
Bldg. 1, Fabrication Room	Pu-238 oxide powder	10 kg	Paint Cans, at 50 g each
Bldg. 4	H_3 gas	10 kg	Cylinders, at 500 g each

Table C-18. Credible Biological Sabotage Targets

Location	Material Type	Maximum Inventory	Material Size and Configuration
Bldg. 1, Fabrication Room	Anthrax solution	10 g	20 petri dish, at 0.5 g each
Bldg. 4	Botulism aerosol	20 g	10 2-liter cylinders, at 5 kg each

Table C-19. Credible Chemical Sabotage Targets

Location	Material Type	Maximum Inventory	Commercial Sector Security Difference	Material Size & Configuration	Exposure Level at NSB
Bldg. 5	Chlorine	10,000 lb	Lack of access control	55-gallon drums, at 350 lb each	>ERPG III levels

Table C-20. Disruption of Critical Mission Targets Table

Location	Target Function	Impact to National Security	Estimated time for Recovery
Site A, Bldg. 4	Fuel cell production	Increased reliance on fossil fuels	180 days

(f) VA Parameters and Planning Assumptions. Describe/list the baseline parameters and planning assumptions used in conducting the VAs. Provide a summary list of parameters and planning assumptions used in completing VAs. These should include assumptions discussed and concurred in by appropriate DOE offices or planning assumptions identified as a result of data collection/discovery during the VA process.

(g) Critical Path Protection Elements. Describe the process used to identify critical path protection elements and the types of tests to which site protection elements are subjected (procedural, simulation, barrier, equipment, PF, etc.). Using a table similar to Table C-21, Performance Testing Results of Site Specific Essential Protection Element Values, provide a list of: physical security system components for each protection layer [Limited Area (LA), PA, material access area (MAA), and Target Area], the critical protection element tested, if any, as determined from performance testing. Also, indicate the number of tests conducted to obtain results and the testing frequency used to monitor the protection element specific value.

(h) Single Point Failure Analysis. Describe the analyses used to determine any single-point failures identified during the VA. Describe/list the single-point failure(s) to include the nature of the vulnerability, measures to mitigate the vulnerability and the potential exploitability by an adversary.

(i) Critical Path Scenarios. Describe and provide the critical path scenarios, including the bounding scenarios, developed during the VA for each target. Identify the protection system effectiveness (P_E) value for each of these targets. Describe and identify the critical detection points along each adversary path.

Should multiple targets exist within the same security area, such as several SNM targets within the same MAA and same building, bounding critical path scenarios may be described. Provide justification that supports bounding cases.

For each critical path scenario, provide floor plans, diagrams, sketches, or an adversary path description (as shown in Table C-22), or, if appropriate, refer to the descriptions that may have been used previously to illustrate the critical path and protection elements described in the scenarios.

Identify and describe the point along the adversary path at which detection is required to allow for sufficient response time for adversary neutralization to be effected for each of the critical path scenarios (i.e., critical detection point).

Table C-21. Performance Testing Results of Site-Specific Essential Protection Element Values

Protection Layer and Physical Security System Components Tested	Critical Elements Tested	No. of Tests Used as Basis for VA values	Test Frequency	Value used in VA
PA - Identification and Intrusion Element	Attempt to smuggle firearms through Portal 1.	36	Quarterly	0.6
	Attempt to defeat door contacts Bldg. 1, door 3.	34	Quarterly	0.7
MAA - Search Component	Attempt to smuggle firearms through MAA portal	24	Once every 2 months	0.8
Target Area - Identification Component	Attempt to gain unauthorized vault access	48	Monthly	0.9

(j) Protection System Effectiveness (P_E). Verify that the P_E values identified for each critical path scenario were used to calculate conditional risk for each identified target. Using tables similar to those on the following pages (Table C-23, Protection Effectiveness (P_E) for the Theft of Diversion of SNM, Table C-24, Protection Effectiveness (P_E) for Radiological Sabotage, Table C-25, Protection Effectiveness (P_E) for Biological Sabotage; Table C-26, Protection Effectiveness (P_E) for Chemical Sabotage; Table C-27, Protection Effectiveness (P_E) for Disruption of Critical Missions; Table C-28, Protection Effectiveness (P_E) for Theft or Espionage of Classified Information or Matter; and Table C-29, Protection

Effectiveness (P_E) for Other Losses), show the targets and P_E values for each target.

(k) Neutralization Analyses. Identify and describe the mechanism(s) used to determine/calculate the neutralization value(s) used in the risk evaluation. Identify and describe the basis for the neutralization values, parameters that impact the neutralization calculations and any site-specific issues that modify neutralization calculations.

(l) Insider Analysis. Describe the analysis for determining the insider threat for each target class included in the SSSP. This analysis must include the programs supporting the elimination/mitigation of select insider groups from the threat spectrum, identification of the potential insider population, and insider protection programs that were not included in other protection system elements. Describe the programs that are factored into the VA process and provide justification for their use. Identify, by position and title, the participants in the HRP.

(m) Conclusions. Provide a summary of system effectiveness for the identified targets. Document VA analyst's observations and recommendations developed as a result of the VA process. Summarize the system effectiveness using a table similar to C-30, System Effectiveness Summary.

Table C-22. Critical Path Scenarios

Scenario Title:	Base Case 1	Results	
Facility:	Building XYZ	P_I	.
Target Location:	Room,123 State, Open	P_N	
Adversary Threat/Adversary:	Terrorist w/insider: X# outsider, Y# insiders		
Goal Type/Quantity:	Oxide, Xx kg	P_E	
VA Path Analysis Tool:	ASSESS	C	
Computer File ID:	.PPS, .OUT; .NEU	Sys. Eff.:	
Neutralization Tool:	JTS	Sys. Eff.:	

Time (Sec)			SCENARIO ACTIONS
Total	ADV	PF	
			Adversary pre-positions escape vehicles
			Adversary mails weapons and explosives into PA (No x ray or explosives detection capability)
			Adversary proceeds to access control portal
0	20		Adversary attempt to deceit through portal (P_D = 0.xx – badge check with xxxx at access portal). If detected, adversary begins overt actions CRITICAL DETECTION POINT
		25	CAS receives alert and begins to annunciate alert.
20	25		Adversary proceeds to target building XYZ, door 7 on the NE corner
25			Protective Force units begin response.
		70	Unit A responds to NE corner of building XYZ
		55	Unit B responds to SE corner of building XYZ
		80	Unit C responds to SE corner of building XYZ
		60	Unit D responds to SE corner of building XYZ
45	5		Adversary reaches door 7 to building XYZ, insider opens door 7 into building XYZ (P_D = 0.xx – BMS)
50	5		Adversaries enter building XYZ and transverse to vault room 123. CAS receives BMS door alarm and annunciates the alarm
55	50		Adversaries collect target material
80			Unit B reaches response position
85			Unit D reaches response position
95			Unit A reaches response position
105	5		Adversaries proceed to door 7 to exit building XYZ. Unit C reaches response position.
110			Adversary exits building XYZ via door 7. (P_D = xxx - ,)
112			Unit A engages adversary
			Etc.

Table C-23. Protection Effectiveness (P_E) for Theft or Diversion of SNM

Location	Material Type	Facility Condition	Adversary Type	Adversary Scenario Summary	Protective Force Response Summary	P_E Value
Bldg. 1, Vault	Pu-239 ingots	Open	Terrorist	Vault open. Outsiders deceit into PA. Insider crashes out of Bldg. 1 MAA with material. Hands off to outsiders. Adversaries leave PA/site by vehicle.	Armed response to BMS door alarm. Containment at MAA boundary. Positioning of blocking forces at PA boundary if MAA containment defeated. Pursuit in PPA if escape from facility.	.7
Bldg. 1, Assay Room	Pu-239 ingots	Open	Terrorist	Scenario same as vault open scenario.	Scenario same as vault open scenario	.7
Bldg. 1, Fabrication Room	Pu-238 oxide powder	Open	Terrorist	Scenario same as vault open scenario.	Scenario same as vault open scenario.	.7

Table C-24. Protection Effectiveness (P_E) for Radiological Sabotage

Location	Material Type	Facility Condition	Adversary Type	Adversary Scenario Summary	Protective Force Response Summary	P_E Value
Bldg. 1, Fabrication Room	Pu-238 oxide powder	Open	Terrorist	Building open. Outsiders deceit into PA. Outsiders force MAA boundary by foot. Insider allows access into Bldg. 1. Outsiders enter fabrication room, obtain Pu-238 oxide, defeat HEPA filters, and vent material to environment through building ventilation.	Armed response to MAA boundary alarm.	.4
Bldg. 4	H_3 gas	Open	Terrorist	Building open. Outsiders deceit into PA. Outsiders force MAA boundary by foot. Insider allows access into Bldg. 4. Outsiders disperse H_3 to the environment with explosives.	Armed response to MAA boundary alarm.	.4

Table C-25. Protection Effectiveness (P_E) for Biological Sabotage

Location	Material Type	Facility Condition	Adversary Type	Adversary Scenario Summary	Protective Force Response Summary	P_E Value
Bldg. 5	Anthrax	Open	Terrorist	Building open. Outsiders deceit into PA. Insider allows access into Bldg. 5. Outsiders disperse anthrax to the environment with explosives.	Building Containment	.2
		Closed	Terrorist	Outsiders deceit into PA. Outsiders breach door into Bldg. 5. Outsiders disperse anthrax to the environment with explosives.	Building Containment	.2

Table C-26. Protection Effectiveness (P_E) for Chemical Sabotage

Location	Material Type	Facility Condition	Adversary Type	Adversary Scenario Summary	Protective Force Response Summary	P_E Value
Bldg. 5	Chlorine	Open	Terrorist	Building open. Outsiders deceit into PA. Insider allows access into Bldg. 5. Outsiders disperse chlorine to the environment with explosives.	Building Containment	.2
		Closed	Terrorist	Outsiders deceit into PA. Outsiders breach door into Bldg. 5. Outsiders disperse chlorine to the environment with explosives.	Building Containment	.2

Table C-27. Protection Effectiveness (P_E) for Disruption of Critical Missions

Location	Equipment Type	Facility Condition	Adversary Type	Adversary Scenario Summary	Protective Force Response Summary	P_E Value
Bldg. 1, Fabrication Room	Fuel Fabrication	Open	Nonviolent Insider	Insider enters Fab. Room. Starts fire to destroy equipment located in room.	Building Containment	.2

Table C-28. Protection Effectiveness (P_E) for Theft or Espionage of Classified Information or Matter

Location	Classified Information or Matter	Facility Condition	Adversary Type	Worst-case Scenario Summary	Protective Force Response Summary	P_E Value
Bldg. 5, Office Area	TSRD Documents	Open	Nonviolent Insider	Insider obtains TSRD, makes copies, encloses copies in envelope, and hand-carries out of Bldg. 5. Insider mails classified documents out of PA to off-site location.	None	.2

Table C-29. Protection Effectiveness (P_E) for Other Losses

Location	Item	Facility Condition	Adversary Type	Worst-case Scenario Summary	Protective Force Response Summary	P_E Value
Bldg. 5, Lab Area	R&D Laboratory	Open	Nonviolent Insider	Insider starts fire in laboratory.	Building Containment	.2

Table C-30. System Effectiveness Summary

Goal	Target	Location	Operations	P_E
Theft of SNM	Bldg. 1	Vault	Day Shift	.8
Theft of SNM	Bldg. 1	Assay Room	Day Shift	.8
Theft of SNM	Bldg. 1	Fab. Room	Day Shift	.75
Rad. Sabotage	Bldg. 1	Fab. Room	Day Shift	.85
Rad. Sabotage	Bldg. 4	Bldg. 4	Day Shift	.9
Chem. Sabotage	Bldg. 5	Laboratory	Day Shift	.8
Bio. Sabotage	Bldg. 5	Laboratory	Day Shift	.8
Indust. Sabotage	Bldg. 1	Fab. Room	Day Shift	.8
Espionage of Classified	Bldg. 5	Office Area	Day Shift	.8
Other Losses	Bldg. 5	Laboratory	Day Shift	.8

SECTION D—SITE SAFEGUARDS AND SECURITY PLAN RESOURCE PLAN

1. OBJECTIVE. The Resource Plan (RP) identifies safeguards and security (S&S) resources necessary to ensure protection of Department assets and identifies changes in resource requirements (i.e., operational requirements, capital equipment, general plant projects (GPPs), and line item construction projects (LICPs) that directly impact risk, indirectly impact risk, or derive from changing S&S policy, directives, guidance or other Department governing statements.

   a. Operational Requirements. Briefly describe operational requirements relating to S&S operations that would require increments or decrements to operational accounts (e.g., program direction, operational support, etc.). Operational requirements must include, but are not limited to, material consolidation, facility mission changes, changes in the design basis threat (DBT) impacting site operations, protective force (PF) redeployments, maintenance and testing changes, PF manning levels, procuring technical expertise and support personnel, and additional training requirements. Summarize the pertinent information in a table as outlined in Table D-1, Operational Requirements. The table and supporting narrative must include the following:

      (1) the title of each operational requirement;

      (2) the basis of the requirement (drivers behind the requirement);

      (3) the funding profile and the impacts if not funded (if possible, state the impact in terms of probability of system effectiveness (P_E) and indicate if this is a new resource requirement); and

      (4) provide a status of operational requirements that were previously authorized but have not yet been completed.

      Provide a separate section for each operational requirement.

Table D-1. Operational Requirements

Requirement (section)	Basis	Funding Request/Profile						Currently in Budget (Y or N)	Type of Expense
		FY xxxx (current year)	FY + 1	FY + 2	FY + 3	FY + 4	FY + 5		

b. Capital Equipment. Briefly describe identified/proposed capital equipment procurements and funding requirements that are not part of a LICP or GPP, and support S&S programs and operations. These procurements could include, but are not limited to, alarm and assessment system components, material control and accountability (MC&A) systems, access control system components, and equipment necessary to complete the S&S mission (e.g., breaching tools, vehicles, PF armaments, additional capabilities necessary to address changes in the DBT). Summarize the pertinent information in a table as outlined in Table D-2, Capital Equipment. The table and supporting narrative must include the following:

(1) a title for each capital equipment procurement;

(2) the basis of the requirement (drivers behind the requirement);

(3) the funding profile and the impacts if not funded (if possible, state the impact in terms P_E, and indicate if this is a new resource requirement); and

(4) a status of capital equipment upgrades that were previously authorized but have not yet been completed.

Provide a separate section for each capital equipment procurement.

Table D-2. Capital Equipment

Capital Equipment (section)	Basis	Funding Request/Profiles						Currently in Budget (Y or N)
		FY xxxx (current year)	FY + 1	FY + 2	FY + 3	FY + 4	FY + 5	

c. GPP. Describe significant identified/proposed GPPs that are not part of a LICP or capital equipment expense but that are necessary to support S&S programs and operations. These GPPs could include, but are not limited to, alarm and assessment systems/components, MC&A systems, access control systems/components, or infrastructure improvements. Summarize the pertinent information in a table as outlined in Table D-3, General Plan Projects. The table and supporting narrative must include:

(1) a title for each GPP;

(2) the basis of the requirement (drivers behind the requirement);

(3) the funding profile and the impacts if not funded (if possible, state the impact in terms P_E, and indicate if this is a new resource requirement); and

(4) a status of general plan project upgrades that were previously authorized but have not yet been completed.

Provide a separate section for each GPP.

Table D-3. General Plant Projects

General Plant Projects (section)	Basis	Funding Request/Profiles						Currently in Budget (Y or N)
		FY xxxx (current year)	FY + 1	FY + 2	FY + 3	FY + 4	FY + 5	

d. LICP. Describe current and proposed LICPs that are not part of a GPP or capital equipment procurement but are necessary to support S&S programs and operations. Summarize the pertinent information in a table as outlined in Table D-4, Line Item Construction Projects. The table and supporting narrative must include:

(1) a title for each LICP;

(2) the basis of the requirement (drivers behind the requirement);

(3) the funding profile and the impacts if not funded (if possible, state the impact in terms P_E, and indicate if this is a new resource requirement);

(4) the status of S&S upgrades that were authorized but have not yet been completed. Discuss any changes to cost estimates [i.e., total estimated cost (TEC) versus total project cost (TPC)] identified in the previous RP.

Provide a separate section for each LICP.

Table D-4. Line Item Construction Projects

LICP Title (section)	Basis	Funding Request/Profiles						Total Costs		Schedule		Currently in Budget (Y or N)
		FY xxxx (current year)	FY + 1	FY + 2	FY + 3	FY + 4	FY + 5	TEC	TPC	Start Date	Finish Date	

Table D-5. Unfunded/Unsupported Requirements

Requirement (section)	Basis	Resource Type	Base FY	Original Funding Request/Profiles						Impact
				FY xxxx	FY + 1	FY + 2	FY + 3	FY + 4	FY + 5	

2. UNFUNDED/UNSUPPORTED REQUIREMENTS. Briefly describe proposed S&S operational requirements, capital equipment procurements, GPPs, or LICPs that had been previously identified and have not been funded supported. Summarize the pertinent information in a table such as Table D-5, Unfunded/Unsupported Requirements. The table and supporting narrative must include:

   a. a title for each unfunded requirement;

   b. the basis for the requirement (drivers behind the requirement);

   c. the type of resource requested (operating expense, capital equipment, GPP, or LICP);

   d. the fiscal year the requirement was originally identified; and

   e. the proposed funding profile and impacts due to lack of funding (if possible, state the impact in terms of P_E).

   Provide a separate section for each unfunded requirement.

3. REFERENCES FOR THE RESOURCE PLAN.

   a. Facility SSSP. Provide a reference to the most recent/current SSSP.

   b. Programmatic Documentation. Provide a reference (include title, date, and responsible organization) for any programmatic policy, directive, or guidance necessitating the allocation of additional resources.

4. HEADINGS AND TERMS FOR TABLES D-1 THROUGH D-5. The following are the types of data to be included in the RP.

   a. Basis.

      (1) Compliance.

      (2) Risk reduction.

      (3) SSSP derived.

      (4) Cost-efficiency.

      (5) Operational efficiency.

      (6) Enhanced operations.

      (7) DBT change.

b. Type of Expense.

(1) Operational = annual recurring cost that will need to be added to the budget baseline.

(2) Single = one time only expense paid from operating dollars.

c. Total Costs.

(1) TEC[20] = Total estimated cost.

(2) TPC = Total project cost.

d. Resource Type.

(1) OE = operational expense.

(2) CE = capital expense.

(3) GPP = general plant project.

(4) LICP = line item construction project.

(5) BASE FY = fiscal year in which the resources were identified and requested.

e. Impact.

(1) Continued risk.

(2) Cost escalation.

(3) Unable to comply with xxxx (list applicable directive).

(4) Programmatic impact.

(5) Operational impact.

(6) Other (list).

[20]As defined in DOE O 413.3, Chg 1, *Project Management for the Acquisition of Capital Assets.*

SECTION E—VULNERABILITY ASSESSMENT PROGRAM

1. OBJECTIVE. The Vulnerability Assessment (VA) Program must consider other programs such as protective force (PF), material control and accountability (MC&A), emergency operations, safety, maintenance, facility operations, personnel security, physical protection, and information security.

2. CONDUCTING VAs. The process of conducting a VA includes gathering data that describe the physical and operational characteristics of a safeguards and security (S&S) system, assigning values such as delay and detection, and analyzing the results to determine the relative effectiveness in conjunction with the adversary's capabilities as identified in the Design Basis Threat (DBT) and the Adversary Capabilities List (ACL). Below is a description of the VA process.

   a. Assumptions. Assumptions and scoping agreements must be defined. All assumptions must be documented in the VA report.

   b. Threat. The person responsible for the conduct of VAs, hereinafter referred to as the analyst (see paragraph 9 of this section), must understand how the DBT relates to VAs. The analyst performing the VA must apply DOE Headquarters (HQ), regional and local threat guidance.

      (1) DOE HQ Threat.

         (a) The DBT must be used to define threat against which VA analysts evaluate the protection system.

         (b) The site's protective systems must be analyzed against the ACL.

      (2) Regional and local threats must be considered during the conduct of VAs.

   c. Targets. All security interests whose loss, theft, compromise, and/or unauthorized use will affect the national security and/or the health and safety of DOE and contractor employees, the public, the environment, or DOE programs are potential targets. The analyst must consider target configurations and conditions, as well as operational conditions and acquisition times.

   d. Modeling. Modeling is used to analyze S&S programs, interests, assets, and the effectiveness of program implementation. Modeling can include computer-based tools and simulations, table-top analyses, and subject matter expert analyses. Section E, Appendix 3, Vulnerability Assessment Modeling Tools, lists those modeling tools approved by DOE. Methods to ensure that the models accurately reflect the facility posture must be part of the final VA results. The modeling process must establish critical pathways. The following must be considered:

Vertical line denotes change.

(1) facility characterization;

(2) system effectiveness models and equations must be used. Section E, Appendix 4, System Performance Effectiveness Equation, delineates the system effectiveness equation;

(3) response force times;

(4) the probability of neutralization (P_N) must be calculated using data available regarding the PF response and their ability to interrupt and neutralize an adversary. The methods used must be documented and retained as part of the evidence file. The calculated number for P_N must be derived from more than one source, one of which must be joint tactical simulation (JTS), joint conflict and tactical simulation (JCATS), or force-on-force (FoF) exercises;

(5) blast effect modeling must consider blast effects on barrier breaching, a force multiplier, and target buildings;

(6) table-top methods used to determine system effectiveness must be documented and a means provided to allow for validation or verification;

(7) radiological sabotage must be fully analyzed against the DBT and ACL. Existing information from safety analyses can be used but must be analyzed to consider deliberate rather than accidental release;

(8) chemical and biological sabotage must be analyzed against the DBT and ACL;

(9) the analysis must use the threshold stated in DOE O 470.3, *Design Basis Threat (DBT) Policy*; and

(10) the use of chemical and biological agents must be analyzed as a force multiplier. Methods of release and mitigation measures must be a part of the analysis.

e. Performance Testing. If conducted, the results of the following tests (including validations) must be considered in determining system effectiveness:

(1) FoF exercises;

(2) limited scope performance tests (LSPTs);

(3) alarm response and assessment performance tests (ARAPTs);

(4) breaching test data;

(5) critical system element tests.

Vertical line denotes change.

f. Results. The results of VAs indicate P_E. The VA results must be used for determining:

(1) protection system effectiveness reporting;

(2) S&S upgrades;

(3) manning/armament levels for the PF;

(4) justifications for waivers of and exceptions to S&S policy.

g. VA Practitioner Training. VA practitioners must successfully complete VA program training within 2 years (24 months) of appointment. This requirement can be met through the National Training Center (NTC).

3. QUALITY ASSURANCE. The analyst must verify the data used for the analyses. These data include:

a. modeling data to include detection, assessment, delay, interruption, neutralization, PF response times, etc.;

b. all facility modeling characterization direct settings, rationales, and documentation;

c. performance test results and documentation; and

d. sensitivity analyses such as single point failure and critical system element analyses.

4. VA DOCUMENTATION. All information used to support or document VAs must be maintained and made available upon request. Examples include:

a. modeling inputs;

b. PF response;

c. adversary capabilities;

d. blast effects;

e. sabotage data;

f. timeline data; and

g. neutralization data.

5. ASSIGNING FIGURES OF MERIT. "Figures of merit" is defined as numerical values and/or qualitative ranges assigned to component systems and personnel associated with the protection system. Collectively the qualitative and/or quantitative measures provide the basis for determining system effectiveness. Approved reference materials must be used to provide initial data and to calculate accurate detection and delay numbers. A list of approved references is provided in DOE M 470.4-7, *Safeguards and Security Program References*. Reference materials are to be used only as a basis for the relative figures of merit. Non-default figures of merit must be documented and based on performance testing or engineering studies.

6. CRITICAL SYSTEM ELEMENTS. Critical system elements are components or subcomponents of an S&S protection system that directly affects the ability of the system to perform a required function. Critical system elements may be equipment, procedures, or personnel. Failure of a critical system element would result in the protection system effectiveness of the target being reduced to levels requiring management action. Critical system elements must be:

   a. identified for every target that requires a VA;

   b. specifically delineated such that specific performance tests can be performed to determine the ability of the protection measures to perform their intended function; and

   c. tested, documented, and the results analyzed to validate element effectiveness.

7. VULNERABILITY ASSESSMENT REPORTS (VARs). VARs document the results of a VA. VARs must include targets analyzed, methodology used, system effectiveness results, parameters and assumptions under which the VA was conducted, and reference to evidence files. VARs published in support of an SSSP should conform to the suggested format given in Section E, Appendix 5, Suggested Vulnerability Assessment Report Format. The approval chain for VARs is below.

   a. The analyst responsible for the VA must sign the report.

   b. Line management responsible for the Facility/Site VA program must approve the report.

   c. DOE line management responsible for the VA program must concur with the report.

   d. The DOE cognizant security authority must concur with the report.

8. SYSTEM EFFECTIVENESS. Only the Secretary of Energy or the Deputy Secretary can accept low protection system effectiveness that results in high risk. Cognizant Under Secretaries can accept marginal protection system effectiveness that results in moderate risk. If the results of a VA, survey, self-assessment, audit, or inspection conducted by the

Vertical line denotes change.

cognizant security authority, Departmental element, Office of Security, or Office of Independent Oversight and Performance Assurance indicate a decreased (low or marginal) protection system effectiveness that is not mitigated by compensatory measures based upon a risk management determination (see Section A, paragraph 2e), the following actions must be initiated.

a. Low Protection System Effectiveness.

(1) Once a low protection system effectiveness condition that results in high risk is identified, that condition must be reported to the responsible Departmental element within 4 hours.

(2) A corrective action plan must be submitted to the responsible Departmental element within 8 hours, with a copy to the Office of Security.

b. Marginal Protection System Effectiveness.

(1) Once a marginal protection system effectiveness condition that results in moderate risk is identified, that condition must be reported to the responsible Departmental element within 2 working days.

(2) A corrective action plan with recommendations must be submitted to the responsible Departmental element within 5 working days with a copy to the Office of Security.

9. TRAINING AND CERTIFICATION.

a. The analyst responsible for the conduct of Vulnerability Assessments must complete the Department approved training program (scheduled to be fully implemented by 2008).

b. The analyst must be certified as outlined in the contractor requirements for *Vulnerability Assessment Certification* Program Manual, which is currently under development.

c. Any person currently conducting VAs may be “grandfathered” until such time as the *Vulnerability Assessment Certification* Program Manual is issued.

SECTION E
APPENDIX 3—VULNERABILITY ASSESSMENT MODELING TOOLS

1. ASSESS – Analytic System and Software for Evaluating Safeguards and Security.

2. ATLAS - Adversary Time Line Analysis System.

3. BATLE - Brief Adversary Threat Loss Estimator.

4. JTS - Joint Tactical Simulation.

5. JCATS - Joint Conflict and Tactical Simulation.

6. AT Planner – Anti-Terrorist Planner.

7. BLAST X – Explosive Effects Analysis Software.

8. BLAST FX – Explosive Effects Analysis Software.

9. ConWEP – Conventional Weapons Effects Program.

10. BEEM - Blast Effects Estimation Model.

11. HOTSPOT – HOTSPOT Health Physics Code provides the capability to calculate the radiation effects associated with the short-term (less than 24 hours) atmospheric release of radioactive materials.

12. RSAC - Radiological Safety Analysis Computer program calculates the consequences of a release of radionuclides to the atmosphere.

13. ACATS – Airborne Chromatograph for Atmospheric Trace Species.

14. ISA – Iterative Site Analysis.

15. VISA – Vulnerability of Integrated Security Analysis.

16. VISA II - Vulnerability of Integrated Security Analysis II.

17. ERAD - Explosive Release Atmospheric Dispersion.

18. ALOHA – Area Locations of Hazardous Atmospheres.

19. ARAC – Atmospheric Release Advisory Capability.

Vertical line denotes change.

20. ACCS 2 - Accident Consequence Code System for the calculation of the health and economic consequences of accidental atmospheric radiological releases.

21. HPAC - Hazard Prediction Analysis Code provides the capability to accurately predict the effects of hazardous material releases into the atmosphere.

SECTION E

APPENDIX 4—SYSTEM PERFORMANCE EFFECTIVENESS EQUATION

The methodology requires the determination of the probability of sensing, probability of assessment, and probability of detection at each layer. These are then combined to determine the contribution to overall system effectiveness represented by each layer. Mathematically, this can be expressed as the equation:

$$P_{EL} = P_{IL} \times P_{NL} = P_{DL} * P_{NL} = P_{AL} * P_{SL} * P_{NL}$$

Where:

P_{EL} is the system effectiveness contribution for layer L;

P_{IL} – Probability of Interruption given first detection at layer L, $P_{IL} = P_{DL}$ if detection on layer L is timely, and is equal to 0 ($P_{IL} = 0$) if detection is not timely;

P_{DL} – Probability of Detection at layer L, $P_{DL} = P_{SL} \times P_{AL}$ on layer L. P_{DL} is the probability of first detection at layer L, given that detection has not occurred at an earlier layer, multiplied by the probability of sensing at an earlier layer, multiplied by the probability of sensing at layer L (P_{SL}) and the probability of assessment at layer L (P_{AL});

P_{SL} – Probability of Sensing on layer L;

P_{AL} – Probability of Assessment on layer L; and

P_{NL} – Probability of Neutralization given first detection at layer L.

L is defined as the number of detection layers in the system before the critical detection point (CDP) in the adversary path(s). Detection after the CDP cannot not be counted.

P_E is defined as the system effectiveness of the layer. The system effectiveness of the layer is the product of the probability of interruption of the layer and the probability of neutralization given that detection occurred at that layer ($P_I \times P_N$). The probability of neutralization is determined discretely for each layer given detection at the layer. The neutralization determination is made if detection (regardless of the extent) takes place at the layer in question. Neutralization will occur sometime past the detection point and would be valid for the probability of neutralization of that specific layer.

P_D of the layer is defined as the product of the probability of sensing and the probability of assessment of the layer ($P_S \times P_A$). Note that detection and assessment will be different between the elements of the layer and between layers.

P_{IL} of the layer is defined as $P_{IL} = P_{DL}$ if detection on layer L is timely, and is equal to 0 ($P_{IL} = 0$) if detection is not timely.

Vertical line denotes change.

The Σ symbol is the summation of terms. The summation symbol is defined as:

$$\sum_{i=1}^{n} k_i \equiv k_1 + k_2 + \ldots + k_n$$

The Π symbol is the product of terms. The product symbol is defined by:

$$\prod_{i=1}^{n} f_i \equiv f_1 \times f_2 \times \ldots \times f_n$$

For those protection systems based on sensing, assessment, detection, interruption, and active neutralization of an adversary, credit can only be taken up to the "point on the pathway" at which the total of the adversary task time, engagement times, and delay times exceeds the protective force response times. This limiting criterion eliminates credit being taken for protection system capabilities that are not engaged prior to the adversary completing their objective. For denial based protection systems, the point on the pathway is the critical detection point. The critical detection point is defined as the point at which the protective force must have timely detection, assessment, and response to initiate a response to have a high probability of success in the neutralization of the adversary or denial of the adversary's task/objective. Therefore, for a facility employing multiple, complementary layers of protection, the representative total protection system effectiveness is calculated up to the point at which the protection systems can still effectively engage an adversary prior to completion of the objective.

The contributions of each layer along the adversary pathway are then combined to determine the overall system effectiveness, where the overall system effectiveness is provided by the sum of the contributions of each layer (only those encountered along the adversary pathway) to the system effectiveness.

An example of the system effectiveness equations for a three-layer system protecting SNM would be as follows:

In extended notation, the Overall System Effectiveness is:

$$P_E = (P_{A1} \times P_{S1} \times P_{N1}) + [(1 - (P_{A1} \times P_{S1})) \times (P_{A2} \times P_{S2} \times P_{N2})] + \{(1 - ((P_{A1} \times P_{S1}) + [(1 - (P_{A1} \times P_{S1})) \times (P_{A2} \times P_{S2})])) \times (P_{A3} \times P_{S3} \times P_{N3})\}$$

Which reduces to:

$$P_E = (P_{D1} \times P_{N1}) + [(1 - P_{D1}) \times (P_{D2} \times P_{N2})] + \{(1 - (P_{D1} + [(1 - P_{D1}) \times P_{D2}])) \times (P_{D3} \times P_{N3})\},$$

and since $P_{IL} = P_{DL}$ when detection is timely,

$$P_E = (P_{I1} \times P_{N1}) + [(1 - P_{I1}) \times (P_{I2} \times P_{N2})] + \{(1 - (P_{I1} + [(1 - P_{I1}) \times P_{I2}])) \times (P_{I3} \times P_{N3})\}$$

$$P_E = P_{E1} + [(1 - P_{I1}) \times P_{E2}] + \{(1 - (P_{I1} + [(1 - P_{I1}) \times P_{I2}])) \times P_{E3})\}$$

SECTION E

APPENDIX 5—SUGGESTED VULNERABILITY ASSESSMENT REPORT (VAR) FORMAT

1.0 Executive Summary

Objective

Purpose and Summary of Protection Effectiveness

2.0 Introduction

Scope

Changes in the VAR

Methodology and Assumptions

3.0 Target Identification and Description

Theft or Diversion

Sabotage (Radiological)

Sabotage (Chemical and/or Biological)

Theft or Espionage of Classified Information or Matter

Other Losses

4.0 Threat Definition

Adversary Type(s)

Adversary Attributes

5.0 S&S Protection Elements

Physical Security Systems

Protective Forces (Response Strategies, Interruption, Neutralization)

Material Control and Accountability

Reliability Program

6.0 Performance Testing

Program Description

Site Protection Elements

Critical Protection Elements

Vertical line denotes change.

SECTION F—PERFORMANCE ASSURANCE PROGRAM

1. OBJECTIVE. To demonstrate the effectiveness of the protection provided Departmental safeguards and security (S&S) interests by systematically evaluating all protection program essential elements.

2. REQUIREMENTS. Each performance assurance program must be developed to validate the performance of all essential S&S protection elements.

   a. Operability and Effectiveness. Performance assurance programs must provide for operability and effectiveness testing of each protection program essential element or component.

      (1) Operability tests provide measures of integrity and must check the essential elements or total system to confirm operability.

      (2) Performance tests provide comprehensive assurance that protection program elements are performing as designed and provide the required levels of protection.

         (a) Performance tests results are used to validate the effectiveness of all elements of a layered S&S system.

         (b) Performance tests are not substitutes for compliance with requirements.

   b. Continuity. Performance assurance programs must evaluate operational continuity of all S&S essential elements. Limited scope performance tests (LSPTs) and/or force-on-force (FoF) tests may be used as a means of meeting specific performance assurance testing requirements. Performance assurance programs must be evaluated as part of the DOE survey and the facility self-assessment programs as described in Section G of this CRD.

      (1) New protection program essential elements and components must be validated through acceptance testing before operational use.

      (2) Essential elements that have been repaired or undergone maintenance must be validated through testing before use.

      (3) The PF must be performance tested both individually and in small tactical units.

      (4) Performance tests must ensure that approved protection strategies of denial, containment, recapture, recovery, and pursuit can be accomplished by the PF.

Vertical line denotes change.

(5) Essential elements of the protection program security systems and subsystems are performance tested to ensure that system detection, assessment, and response to alarms and adversarial actions meet stated requirements.

c. Reliability. Each essential element whose failure would reduce protection to an unacceptable level must be tested at frequencies that provide high assurance of operability and reliability.

(1) Testing frequencies must reflect site-specific conditions and operational needs.

(2) Testing frequencies must be documented for each essential element.

d. Performance Tests. At least every 365 days, an integrated performance test encompassing all essential protection elements associated with a comprehensive site or facility threat scenario must be conducted to evaluate the overall facility S&S effectiveness.

(1) Those Category I facilities requiring denial protection strategies must conduct integrated performance testing on a quarterly (at least every 3 months) basis.

OR

(2) Those sites with multiple Category I facilities requiring denial protection strategies may rotate quarterly performance testing so that at least one facility is tested on a quarterly basis (at least every 3 months). However, an integrated performance test for all Category I facilities must occur at least once every 365 days.

e. Documentation.

(1) Performance Assurance Program Plan. This plan must be an integral part of the site safeguards and security plan (SSSP)/site security plan (SSP), or material control and accountability (MC&A) plan, as applicable. The performance assurance program plan must describe the program and its administration and implementation by:

(a) identifying protection elements for the protection of Category I and II special nuclear material (SNM) and Top Secret matter;

(b) describing how the performance of these elements is to be ensured, including the manner in which credit is taken for activities performed by external oversight organizations; and

Vertical line denotes change.

(c) addressing how deficiencies identified during performance assurance activities are to be corrected.

(2) Performance Assurance Reports. The results of performance assurance program testing must be documented.

(3) Document Retention. Record keeping systems must provide an audit trail for performance assurance activities and reports.

SECTION G—SURVEY, REVIEW, AND SELF-ASSESSMENT PROGRAMS

1. OBJECTIVES.

   a. Provide assurance to the Secretary of Energy, Departmental elements, and other government agencies (OGAs) that safeguards and security (S&S) interests and activities are protected at the required levels.

   b. Provide a basis for line management to make decisions regarding S&S program implementation activities, including allocation of resources, acceptance of risk, and mitigation of vulnerabilities. The results must provide a compliance- and performance-based documented evaluation of the S&S program.

   c. Identify S&S program strengths and weaknesses, develop and complete a process improvement schedule, and use the results to correct and improve the overall S&S program.

   d. Provide documentation of oversight and assessment activities.

2. REQUIREMENTS. Surveys are conducted by the DOE cognizant security authority. The requirements pertaining to surveys are provided for informational purposes only.

   a. Types and Frequencies of Surveys and Assessments.

      (1) Initial Surveys. Initial surveys must be conducted at facilities where there will be a facility clearance established for a facility with an importance rating of: A, B, C, or PP (see Section I, Chapter II, of this CRD). Survey activities must be comprehensive and result in a satisfactory composite rating prior to a facility clearance (FCL) being granted.

      (2) Periodic Surveys. Periodic surveys are conducted for all facilities and must cover all applicable topics to ensure survey program objectives are met. The periodic survey may be composed of multiple special survey reports providing all the requirements of this section are met. Integration of internal and external reports including quality assurance, property appraisals, performance assurance, and other evaluation reports may be used to augment the requirement for a periodic survey.

         (a) Facilities with importance ratings of A, B, or C must be surveyed once every 12 months [with the exception of Category IV SNM only facilities—see (c) below].

         (b) Facilities with an importance rating of PP must be surveyed once every 24 months.

(c) For facilities with Category IV special nuclear material (SNM) and nuclear material, including source material, the nuclear material control and accountability (NMC&A) topical area must be surveyed at least every 24 months.

(d) Facilities with importance ratings of D, NP, or E do not require surveys but do require periodic reviews [see paragraph 2a(5) below].

(3) Special Surveys. Special surveys may be conducted at facilities for specific limited purposes. Examples include extended survey activities, technical security activities, "for cause" reviews, line management direction, shipment of nuclear and/or classified information or matter, or a change in the contractor operating a Government-owned facility.

(4) Termination Surveys. Termination surveys must be conducted to verify the termination of Departmental activities and 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, property, security badge retrieval, debriefings, and verification of the termination or transfer of Department of Energy (DOE) access authorizations.

(a) Onsite termination surveys must be conducted at facilities possessing Top Secret matter, sensitive compartmented information (SCI)/special access program (SAP) information or matter, or SNM.

(b) Onsite or correspondence termination surveys must be accomplished for all other possessing facilities.

(5) Periodic Reviews. A documented review of entities (D, NP, and E facilities) such as subcontractors, consultants, and common carriers must be performed by the DOE cognizant security authority at least every 5 years.

(6) Self-Assessments. Contractors must conduct self-assessments between periodic surveys conducted by the cognizant security authority and include all applicable facility S&S program elements. The self-assessment must ensure the S&S objectives are met (see paragraph 1 above). NOTE: NP facilities are not required to conduct self-assessments. However, sponsoring organizations (Federal or contractor) must include in their self-assessments a thorough review of their registration program for NP facilities which may result in a program review of identified subcontractors.

(7) Reviews or Inspections by Other DOE Elements or OGAs. Reviews/inspections conducted by other DOE elements (including site quality assurance programs) or OGAs may be used to meet survey requirements. When using reviews/inspections conducted by other organizations to meet the requirements of the survey, these guidelines must be followed.

(a) The review/inspection must have been conducted within the survey period.

(b) Applicable portions of the review/inspection must be attached to the survey report.

(c) Portions of topical and subtopical areas not covered by the review/inspection must be surveyed.

(d) If ratings were not assigned during the review/inspection, the surveying office must analyze the impact of any deficiencies and assign ratings.

(8) Extension of Frequency. The results of previous surveys may affect the frequency of future surveys. Contractors may request that the interval between periodic surveys be increased up to 24 months by the DOE cognizant security authority. Documentation of the justification for increases in the interval of periodic surveys must be maintained by the DOE cognizant security authority.

(a) The following conditions must be met for extensions:

1 the facility was rated satisfactory during the most recent survey activity;

2 the facility has no unmitigated deficiencies that impact the security posture of the facility, and all applicable topical area ratings are satisfactory from the previous survey; and

3 all applicable topical area ratings from the most recent self-assessment are satisfactory, and the DOE cognizant security authority concurs with the ratings.

(b) Increasing the interval between surveys for a facility possessing Category I SNM or credible roll-up to Category I SNM must be approved, in writing, by the Associate Administrator for Defense Nuclear Security or the Under Secretary for Energy, Science, and Environment.

(c) All modifications to survey frequency requirements must be documented in the Safeguards and Security Information Management System (SSIMS).

b. Scope and Methodologies. Surveys and self-assessments must provide an integrated evaluation of all topical and subtopical areas to determine the overall status of the S&S program and ensure the objectives of this section are met (see paragraph 1 above). The integrated evaluation is a comprehensive synergistic approach using multiple S&S program elements that ensures total system effectiveness and, if properly implemented, will meet the objectives identified in paragraph 1 above. The scope of these activities and the methods used must include those listed below.

(1) Compliance. Compliance reflects the status of the S&S program as measured against implementation of applicable Federal statutes, regulations, policies approved site safeguards and security plans (SSSPs)/site security plans (SSPs), and other approved security plans.

(2) Performance. Performance indicates the degree to which the elements of the S&S program meet protection objectives based on the operational testing of program elements.

(3) Comprehensiveness. Comprehensiveness identifies the breadth of protection afforded all activities and interests within a facility. This is accomplished by an evaluation of the adequacy and effectiveness of programs and a thorough examination of the implementation of policies, practices, and procedures to ensure compliance and performance. All applicable topical areas identified on DOE Form (F) 470.8, "Survey/Inspection Report" Form, must be evaluated.

(4) Other. The scope of special and termination surveys is determined by the DOE cognizant security authority in coordination with the surveying office. Determinations of survey scope are predicated on the nature or status of operations at the facility, activity, or element being surveyed. These surveys may not cover all topical areas identified on DOE F 470.8.

3. CONDUCT. Local survey and self-assessment procedures implementing this section must be developed, documented, and approved by the cognizant security authority. Procedures must ensure completion of the objectives contained in paragraph 1 above and must include the requirements listed below.

a. Team Composition. Contractor line management must determine that contractor survey and self-assessment team members possess qualifications, experience, and training sufficient to review and inspect the topical/subtopical areas of the

survey/self-assessment. The National Training Center (NTC) provides training courses for survey/self-assessment team leaders and team members.

b. Planning, Scheduling, and Integration. Surveys and self-assessments must be planned, scheduled, and conducted in an integrated manner to achieve the objectives identified in paragraph 1 above. If topical and subtopical area evaluations are performed separately, the surveying office must document and integrate the results of each into a single (periodic) survey report that includes a composite facility rating. The frequency between topical and subtopical areas cannot exceed the frequency for the single (periodic) survey.

c. Validation. Results must be validated by methods including, but not limited to, document review, performance testing, and interview analyses and observations.

d. Exit Briefing. An exit briefing must be conducted with the surveyed or assessed organization to include the minimum facts:

(1) program strengths and weaknesses, including all findings;

(2) corrective action reporting requirements for all open findings, regardless of source; and

(3) topical and composite ratings. For less than satisfactory ratings, the communication of the composite rating initiates the actions required in paragraph 8 of this section.

4. FINDINGS.

a. Identification and Documentation. Findings are any validated program deficiency (failure to meet a performance or compliance requirement) regardless of source. Findings may be reflected in documents resulting from internal and external reviews, audits, appraisals, and other sources [e.g., Office of Independent Assessment and Performance Assurance (OA), the General Accountability Office (GAO), Office of the Inspector General (IG), previous surveys, self-assessments, etc.].

All open findings must be reviewed during the survey or self-assessment to validate the status of corrective action and to evaluate the impact on the existing S&S program.

Findings identified during the current survey or self-assessment must be reported immediately to the Departmental element and contractor line management if a vulnerability to national security, classified information or matter, nuclear materials, or Department property results, or may result, in a programmatic impact to the Department. Findings identified during a survey or self-assessment,

even if closed during the survey or self-assessment activity must be documented in the associated report.

b. Tracking. Findings and deficiencies, regardless of source, and corrective action plans (milestones and estimated completion dates) must be entered into SSIMS in accordance with SSIMS guidelines and tracked until closed. Quarterly status reports must be entered into SSIMS by January 15, April 15, July 15, and October 15 of each year. Self-assessment deficiencies are not required to be entered into SSIMS; however, a local mechanism/system must be used to track these deficiencies and corrective action until closed.

c. Trending. Trending evaluations must be considered in the resolution of findings in the subtopical area of program management to determine if systemic and systematic causal factors exist within the S&S program. Results of this evaluation that indicate negative trends must be analyzed to ensure corrective action plans, address root causes, and the need to ensure continuous improvement of the S&S program.

5. RATINGS.

a. Types. Ratings must be based on the effectiveness and adequacy of the program at a facility and reflect a balance of performance and compliance results as well as the impact of the deficiency(ies) (e.g., findings, IG recommendations, etc.) and mitigating factors. The ratings listed below must be used for all surveys (except termination), reviews, and self-assessments. Does not apply (DNA) and Not Rated (NR) may also be used in applicable situations.

(1) Types of Ratings.

(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.

(d) Inspection Ratings. “Effective Performance,” “Needs Improvement,” and “Significant Weaknesses” are indicators of a management system performance level as outlined in DOE O 470.2B, *Independent Oversight and Assurance Program*.

(2) Rating Determinations.

(a) Existing Conditions. Ratings must be based on existing conditions at the end of the survey and not future or planned corrective actions or conditions.

(b) Impact. Ratings must be based on the impact of all open deficiencies, regardless of source.

(c) Marginal or Unsatisfactory Ratings. Less than satisfactory ratings in any topical area must be based on validated weaknesses in the S&S system or deficiencies in performance.

(d) Topical Area Ratings. A topical area rating must not be marginal for consecutive survey periods and must be assigned an unsatisfactory rating unless one of the following conditions applies.

1 The current survey of the topical area results in a satisfactory rating.

2 The previous survey that resulted in a marginal rating identified different deficiencies and reasons for the rating.

3 The deficiencies and reasons that were the basis for the previous marginal rating were related to the completion of a line item construction project (LICP) or upgrade program. In that case, acceptable interim measures must have been implemented, physically validated pending completion of the project, and documented in the survey report.

(e) Subtopical Ratings. The decision whether or not to use all subtopical ratings must be documented in local procedures.[21] Regardless of the rating method used, the report must include the evaluation of all required subtopical areas which must be used as part of the appropriate topical area rating justification and rationale.

(f) Justification and Rationale. All ratings must be supported and documented to include the rating justification and rationale.

[21] A minimum of one subtopical area rating must be used to effect the rating for the topical area in SSIMS.

6. REPORT CONTENT.

a. Initial/Periodic Survey Reports and Self-Assessment Reports. Reports (to include self-assessment reports) must contain the following items.

(1) A completed DOE F 470.8 or equivalent for self-assessments.

(2) An executive summary containing:

(a) the scope, methodology, period of coverage, duration, date of the exit briefing to management;

(b) a brief overview of the facility, function, scope of operations, and contractual information (e.g., contract number, award and expiration dates, contract type, identification of security clauses, identification of the security and overall scores assigned to the most recent contract appraisal);

(c) a brief synopsis of major strengths and weaknesses that impact the effectiveness of the facility's overall S&S program, including identification of any topical areas rated less than satisfactory;

(d) the overall composite facility rating with supporting rationale;

(e) a reference to a list of findings identified during the survey or self-assessment.

(3) An introduction containing:

(a) the scope, methodology, period of coverage, duration, date of the exit briefing to management; and

(b) a description of the facility, its function and scope of operations, security interests, and contractual information (e.g., contract number, award and expiration dates, contract type, identification of security clauses, identification of the security and overall scores assigned to the most recent contract appraisal).

(4) Narrative for all rated topical and subtopical areas that includes:

(a) a description of the site's implementation of the program element;

(b) the scope of the evaluation;

(c) a description of activities conducted;

(d) the evaluation results and associated issues (including other Department elements or OGA review or inspection results related to this topic/subtopic that were included);

(e) the identification of all findings, including new and previously identified open findings, regardless of source (e.g., OA, IG, GAO), and their current corrective action status; and

(f) an analysis that provides a justification and rationale of the factors responsible for the rating.

(5) Attachments, including:

(a) a copy of the current DOE F 470.2, "Facility Data and Approval Record" (FDAR);

(b) a listing of all active DOE F 470.1, "Contract Security Classification Specification" (CSCS), (or DD F 254, "Contract Security Classification Specification");

(c) a listing of all new findings resulting from the survey/self-assessment;

(d) a listing of all previous findings that are open to include the current status of corrective action;

(e) a listing of team members, including names, employer, and their assigned area(s) of evaluation; and

(f) a listing of all source documentation used to support the survey/self-assessment conduct and results (e.g., GAO, IG, OA, and similar assessment documents).

b. Special Survey Reports. Special survey reports must follow the format and content for initial and periodic survey/self-assessment reports except that an executive summary is not required. Attachments must be included as appropriate to the scope of the special survey.

c. Reports for NP Facilities. Reports for non-possessing facilities must include:

(1) a completed DOE F 470.8;

(2) a copy of the DOE F 470.2, FDAR;

(3) a list of each active DOE F 470.1, CSCS, or DD F 254;

(4) an evaluation of the foreign ownership, control, or influence (FOCI) status;

(5) a determination that employees and subcontractors possess appropriate access authorizations;

(6) a review to ensure that individuals no longer employed under the contract have had their access authorizations terminated and security badges have been accounted for; and

(7) other topical/subtopical areas identified on DOE F 470.8 as required by the DOE cognizant security authority.

d. Termination Survey Reports. Termination survey reports must include:

(1) verification of non-possession of classified information or matter, SNM, hazardous material presenting a potential sabotage threat, or Government property;

(2) verification that all DOE access authorizations have been terminated or transferred and that termination statements have been completed and security badges have been accounted for;

(3) validation that all findings have been closed in SSIMS;

(4) verification of termination of all S&S activities;

(5) a copy of the terminating DOE F 470.2, FDAR; and

(6) a completed certificate of non-possession.

e. Memorandum Report Content. Memorandum reports for DOE programmatic entities and OGAs are generated when it is inappropriate to transmit a copy of the survey report due to need-to-know issues. Reports must contain:

(1) a notification of inclusion of their activity in the survey;

(2) the date of the survey;

(3) ratings and rationale for the ratings associated with the activity; and

(4) all findings applicable to that activity.

7. DISTRIBUTION.

a. The surveying office must send a copy of the survey report to the appropriate Departmental elements and support offices including, the Office of Security.

b. The surveying office must send any memorandum report to applicable DOE program offices and OGAs.

c. Survey/memorandum reports must be distributed within 60 working days of the exit briefing.

d. Self-assessment reports must be distributed to the applicable senior managers and to other personnel responsible for corrective action and other personnel, as deemed appropriate.

8. NOTIFICATIONS AND ACTIONS FOR LESS THAN SATISFACTORY SURVEY COMPOSITE RATINGS. When the survey composite ratings are less than satisfactory the following notifications and actions must occur.

a. Marginal Ratings. Within 15 working days of the determination of a marginal composite rating, the DOE cognizant security authority must ensure SSIMS is updated and provide the applicable Departmental elements and OGAs with the following:

(1) a statement identifying the vulnerabilities and the rationale for the rating;

(2) description of the corrective action/compensatory measures taken to date; and

(3) a statement acknowledging physical validation of the adequacy of items listed in 8a(2), above.

b. Unsatisfactory Ratings. Within 24 hours of determination of an overall composite rating of Unsatisfactory, the DOE cognizant security authority must coordinate with the Departmental element to take the following actions.

(1) Suspend the activity and/or the Facility Clearance (FCL) pending remedial action.

OR

(2) Provide the justification for continuing this critical operation to the Office of Security, the Departmental element, and as directed, other applicable Department elements. In addition to providing the rationale, the DOE cognizant security authority must identify and evaluate those immediate interim corrective actions being undertaken to mitigate identified risks or vulnerabilities.

9. NOTIFICATION AND ACTION FOR LESS THAN SATISFACTORY SELF-ASSESSMENT COMPOSITE RATINGS. Actions required in response to less than satisfactory self-assessment composite ratings are listed below:

   a. Marginal Ratings. Within 15 working days of the determination of a marginal composite rating, notification must be made to line management that includes:

      (1) a statement identifying the vulnerability and rationale for the rating;

      (2) a description of the corrective action/compensatory measures taken to date; and

      (3) a statement acknowledging physical validation of the adequacy of items listed in paragraph 9a(2) above.

   b. Unsatisfactory Ratings. Within 24 hours of determination of an overall composite rating of unsatisfactory, the cognizant security authority must coordinate with the DOE cognizant security authority, which in turn must coordinate with the Departmental element to take the following actions:

      (1) suspend the activity and/or recommend suspension of the FCL pending remedial action;

      (2) provide justification for continuing operations to the DOE cognizant security authority. In addition to providing the rationale, the cognizant security authority must evaluate those immediate interim corrective actions being undertaken to mitigate identified risks or vulnerabilities; and

      (3) if the results of a self-assessment identify an incident of security concern; it must be reported in accordance with Section N of this CRD.

10. CORRECTIVE ACTIONS. Corrective action plans must be developed for all open survey and self-assessment findings. Corrective action plans for survey and self-assessments must be submitted and reported within 30 working days after the date of the exit briefing. If a finding is corrected during the survey, it must be identified in the survey report with a description of the closure/validation performed by the survey/self-assessment team. Quarterly reports of the status of corrective actions for each finding must be provided to the DOE cognizant security authority. All survey and self-assessment corrective actions must:

   a. be based on documented root cause analyses, risk assessments, and cost-benefit analyses to ensure the survey/self-assessment program objectives are met (see paragraph 1 above) and

b. be reported, entered, tracked, and updated until completed, validated, and closed in SSIMS, where applicable (see paragraph 4b above).

11. UPGRADE OF COMPOSITE RATINGS. When line management determines that the composite rating should be upgraded, the survey/self-assessment team must physically verify the completion and adequacy of corrective actions and make notification of the rating upgrade in accordance with approved local procedures.

12. RECORDS RETENTION. Documentation associated with the conduct of survey and self-assessment conduct must be retained in accordance with approved procedures and appropriate records inventory disposition schedules.

13. CONTINUOUS IMPROVEMENT PROCESS. The cognizant security authority must conduct an annual evaluation of their survey or self-assessment processes. This evaluation must ensure any identified process improvements (i.e., lessons learned) are incorporated in the S&S survey/self-assessment process.

PART 2—SAFEGUARDS AND SECURITY MANAGEMENT

SECTION H—FOREIGN OWNERSHIP, CONTROL, OR INFLUENCE (FOCI) PROGRAM

1. APPLICABILITY.

   a. The entities[22] listed below are required to obtain FOCI determinations.

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

      (2) All tier parents located in the United States, Puerto Rico, or a U.S. possession or trust territory.

   b. A FOCI determination is not required for an individual performing work under a consulting agreement (e.g., an individual awarded a contract)[23]. This does not include individuals contracting as a business.

   c. Personnel responsible for the FOCI program can successfully meet FOCI competencies through training courses offered at the DOE National Training Center (NTC).

2. GENERAL REQUIREMENTS.

   a. When the contract involves access to SNM, DOE must render the FOCI determination.

   b. No further FOCI review is required for an applicant holding an equal or higher U.S. Government FCL, based upon a favorable FOCI determination.

   c. Contractors with existing U.S. Government Facility Clearances (FCLs) are identified in the DOE's SSIMS, and the Department of Defense (DoD) Defense Security Service/Central Verification Activity System (DSS/CVA).

   d. Information submitted with a FOCI package is used for the sole purpose of evaluating FOCI and must be treated by DOE contractors, to the extent permitted by law, as business/financial information submitted in confidence. The information must be protected as Official Use Only (OUO).

[22]The entities listed are referred to as "applicants" throughout this section.
[23]The self-employed consulting firm's foreign involvement is determined through the background investigation conducted to determine the individual's eligibility for an access authorization.

e. The Department of Energy Acquisition Regulation (DEAR) prohibits the award of a classified contract until an FCL has been granted. When an existing contract that does not require access authorization is modified to require access authorizations, the contract modification cannot take effect until an FCL is granted. Contract award/modification cannot be made until: (i) all relevant aspects of FOCI have been resolved and, if necessary, are favorably adjudicated; (ii) the signed DOE F 470.1, "Contract Security Classification Specification," (CSCS) is accepted by the cognizant security authority; and (iii) the appropriate DEAR security clauses have been incorporated in the contract.

f. In lieu of hard-copy FOCI submissions, applicants may use the Department's electronic 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.td.anl.gov. To ensure confidentiality of the information submitted and stored on the system, the site is protected with 128-bit encryption. 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 be submitted to the DOE cognizant security authority.

3. DETERMINING THE SECURITY REQUIREMENTS OF THE CLASSIFIED CONTRACT/AGREEMENT.

a. The procurement request originator (or other individual, as designated by the contractor line management) must identify and document on the appropriate procurement form the security requirements of the classified contract. If the procurement request requires an access authorization, FOCI requirements are not applicable. If the procurement request requires access authorizations, a DOE F 470.1 CSCS[24] must be completed by the procurement request originator.

b. The procurement request originator submits the appropriate procurement form and DOE F 470.1 CSCS to the contracting officer. Upon receipt of these forms, the contracting officer must incorporate the appropriate security clauses in the solicitation. When the applicant is included in the competitive range, they must be required to complete the SF 328.

4. DETERMINING THE FCL STATUS OF THE APPLICANT. The contracting officer must identify the FCL status of all applicants within the competitive range and preliminary selection criteria for the pending contract. The contracting officer must then verify whether the applicant's FCL meets the appropriate safeguarding level of the pending contract. Verification of existing FCLs must be obtained from the DOE cognizant security authority through DOE SSIMS or DoD DSS/CVA.

[24]If a DD Form 254 has been used by the agency sponsoring the activity, it can be submitted instead of the DOE F 470.1 CSCS provided it is annotated with the DOE facility code.

5. CONTRACTS REQUIRING ACCESS.

a. When the contracting officer determines that the applicant possesses an existing FCL the same level that the pending contract requires, the contracting officer must send a DOE F 470.1 CSCS to the DOE cognizant security authority for review and approval. Contract award cannot be made until the DOE F 470.1 CSCS is signed by the DOE cognizant security authority and returned to the contracting officer.

b. When the contracting officer determines that the applicant possesses an existing FCL but the pending contract requirements exceed the level of the current FCL, the contracting officer must send a DOE F 470.1 CSCS to the DOE cognizant security authority for review and approval. Contract award cannot be made until the contracting officer has received the signed DOE F 470.1 CSCS from the DOE cognizant security authority.

c. When the contracting officer determines that the applicant does not possess an FCL based on a FOCI determination, the contracting officer must obtain a complete FOCI package. Appendix 6, FOCI Matrix, summarizes the documents and forms required to be completed and submitted by the applicant.

(1) When the applicant is owned by a parent organization(s), a separate FOCI package must be submitted for the applicant and each tier parent located in the United States, Puerto Rico, or a U.S. possession or territory. Foreign tier parents do not need to submit a comprehensive FOCI package, but a key management personnel (KMP) listing must be submitted for each foreign tier parent. Additionally, each foreign tier parent must be identified in the FOCI submission(s) from the U.S. companies, and details provided as to whether the foreign parent(s) is controlled by any foreign government or any entity that is controlled by a foreign government.

(2) When the applicant is a division or branch of a legal entity (i.e., part of but not a separate legal entity), the division/branch only needs to submit a listing of its KMP; and if applicable, representative of foreign interest statement(s), and authorizing resolutions[25] for the division/branch's KMP. The legal entity and, if applicable, its tier parents must submit a complete FOCI package.

d. After obtaining the packages from the applicant, the contracting officer must review the submission(s) to ensure the package(s) is complete. When the package(s) is incomplete, the contracting officer must notify the applicant that the package cannot be submitted for a FOCI determination and must request a complete package. After obtaining the required FOCI documentation, the

[25] Resolutions (adopted by the governing body) that list the express authority (i.e., duties and responsibilities) of the organization's KMP.

Vertical line denotes change.

contracting officer forwards the FOCI package to the DOE cognizant security authority for processing.

e. Contracting officers must provide written notice to the DOE cognizant security authority when:

(1) a notice of change has been submitted by the applicant on a FOCI package submitted for FOCI review;

(2) a requested FOCI review is no longer needed;

(3) a FOCI determination was rendered on an applicant that was not awarded the contract; and

(4) within 30 days of the termination or completion of all work on a contract requiring access authorizations. This notification must also be made when access authorizations are no longer required in performance of the contract. (Notification can be accomplished by using DOE F 470.1 CSCS.)

f. 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.

g. A final FOCI determination can only be requested for the successful applicant. Procurement requesters must allow sufficient lead-time for the processing of the FOCI determination and FCL prior to award of the contract.

6. REPORTING REQUIREMENTS.[26, 27]

a. FOCI Changes That Occur Following Submission of A 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 to the contracting officer.

[26]Reports and submissions required by this chapter must be submitted as follows: Each contractor granted a facility clearance by DOE (including excluded tier parents, if applicable) must provide the reports/information listed in this Section to its DOE cognizant security authority.

[27]Failure of the cleared U.S. organization to report changes in accordance with the requirements of this chapter or to ensure compliance with the terms of its applicable security arrangement may result in suspension or termination of the organization's DOE-approved facility clearance if foreign ownership, control, or influence factors are at a level inconsistent with national security interests.

b. Updates. Contractors holding an FCL based upon a favorable FOCI determination must submit written reports of changed conditions and anticipated changes. Additionally, contractors are required to submit a new FOCI package at least once every 5 years (60 months).

c. Significant Changes. When changes have occurred in the extent and nature of FOCI that affect the information in an applicant's most recent DOE FOCI submission(s), the applicant must provide written notification and supporting documentation relevant to the changes to the DOE cognizant security authority. Significant changes that warrant a new FOCI determination include the following:

(1) a new threshold or factor exists that did not exist when the previous determination was made (e.g., a "no" answer changes to "yes"), and any additional factors associated with the questions on the SF 328;

(2) a previously reported threshold or factor that was favorably adjudicated by the DOE cognizant security authority has increased to a level requiring a determination by the Office of Security;

(3) 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 or end user (i.e., for revenue and/or net income) or lenders (i.e., indebtedness);

(4) 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

(5) any changes in ownership or control. 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). Notification of these changes must be made to the cognizant security authority no later than 5 working days after the event or action necessitating the notice.

d. Anticipated Changes. Anticipated changes are events that arise when the contractor or any of its tier parents enters into formal negotiations toward agreement, and in any event 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 authority with written notification of anticipated actions including those listed below.

(1) An action to terminate business or operations of the contractor or any of its parents for any reason; e.g., 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 its business or assets; 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(s).

e. Other Reportable Changes.

(1) Any change of operating name or address of the company or any of its cleared locations. The cognizant security authority must be notified at least 5 working days prior to the effective date of an address change.

(2) Any change to the information previously submitted for KMP, including, as 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 authority.

(a) Date and place of birth, social security number, citizenship, and, if appropriate, personnel security clearance level and issuing agency.

(b) Whether they have been excluded from access to classified information or matter, or SNM.

(c) Whether they have been temporarily excluded from access to classified information or matter, or SNM pending the granting of their DOE access authorization.

A new complete listing of KMP need only be submitted at the discretion of the contractor and/or when requested in writing by the DOE cognizant security authority.

f. Submission of a New FOCI Package. A new FOCI package must be completed by the contractor or tier parent and submitted to the DOE cognizant security authority at least every 5 years or at the request of the cognizant security authority.

g. Annual Certification.

(1) Each contractor holding an FCL, based upon a favorable FOCI determination, must provide written annual (at least every 12 months) certification to the DOE cognizant security authority acknowledging that:

(a) no significant change has occurred in the extent and nature of FOCI that would affect the organization's answers to the questions provided in its SF 328;

(b) no changes have occurred in the organization's ownership or legal entity name;

(c) no changes have occurred in the organization's KMP. In addition, when the contractor's governing body has invoked resolutions to process KMP for access authorizations and to exclude from the personnel clearance requirement certain members of its governing body and other officers and executive personnel, the contractor's certification must include statements as to whether:

1 each of the organization's KMP required to obtain and retain an access authorization continues to hold the required access authorization;

2 any changes have occurred in the positions held by any of the organizations uncleared KMP whereby the duties of such position(s) require the KMP, to be identified by name, to have access to classified information or matter, or SNM or to be involved in the protection of classified information or matter, or SNM;

3 the invoked resolutions remain in full force and effect; or

4 there were any acts of noncompliance with these security measures, whether inadvertent or intentional, with a description of steps that were taken to prevent such acts from recurring.

(2) Any contractor controlled by a parent organization(s) that has/have been excluded (by formal resolution) must provide written certification on an annual (at least every 12 months) basis to the DOE cognizant security authority acknowledging the continued effectiveness of the resolution. Additionally, the contractor must obtain and provide to its DOE cognizant security authority written certification executed by an authorized official from each such excluded parent that:

(a) no significant changes have occurred in the extent and nature of FOCI that would affect the organization's answers to the questions provided in its SF 328;

(b) no changes have occurred in the organization's ownership or legal entity name;

(c) no changes have occurred in the organization's KMP; and

(d) the exclusionary resolution invoked by the contractor's tier parent's governing body remains in full force and effect.

(3) Any contractor that has executed a Board Resolution to reduce FOCI in noncontrolling foreign ownership situations must provide written certification on an annual (at least every 12 months) basis to its DOE cognizant security authority acknowledging the continued effectiveness of the resolution.

(4) At the end of each year of operation, the trustees, proxy holders, or outside directors, as appropriate, of those organizations operating under a DOE-approved Voting Trust Agreement, Proxy Agreement, Special Security Agreement, or Security Control Agreement[28] must submit to the DOE cognizant security authority an annual (at least every 12 months) implementation and compliance report. The annual implementation and compliance report must include:

(a) a detailed description of the manner in which the company is carrying out its obligations under the arrangement;

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

(c) 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;

(d) any changes or impending changes of senior management officials or key governing body members, including the reasons;

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

[28] A contractor operating under one of these foreign ownership, control, or influence mitigation plans must also submit the applicable annual certifications mentioned in paragraphs 7g(1), (2), and (3).

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

7. METHODS TO MITIGATE UNACCEPTABLE FOCI. The affected U.S. organization or its legal representatives may propose a plan to negate or reduce unacceptable FOCI; however, DOE reserves the right and has the obligation to impose any security method, safeguard, or restriction it believes necessary to ensure that unauthorized access to classified information or matter or SNM is precluded. A plan may consist of one or more of the mitigation measures identified in DOE M 470.4-1, *Safeguards and Security Program Planning and Management,* Part 2, Section H, Chapter IV, "FOCI Mitigation Action Plans."

Vertical line denotes change.

SECTION H

APPENDIX 6—FOCI MATRIX CHART

Sole Proprietorship	Privately Owned Corporation	Publicly Traded Corporation	**Partnership** **1. General** **2. Limited** **3. Limited Liability**	Limited Liability Company	College/University
Completed SF 328, Certificate Pertaining to Foreign Interests Form must be dated and signed by a person legally authorized to represent the business.	Completed SF 328, Certificate Pertaining to Foreign Interests Form must be executed under the corporate seal, dated and signed by a person legally authorized to represent the business.	Completed SF 328, Certificate Pertaining to Foreign Interests Form must be executed under corporation's seal, dated and signed by a person legally authorized to represent the business.	Completed SF 328, Certificate Pertaining to Foreign Interests Form must be dated and signed by a person legally authorized to represent the partnership.	Completed SF 328, Certificate Pertaining to Foreign Interests Form must be dated and signed by a person legally authorized to represent the business.	Completed SF 328, Certificate Pertaining to Foreign Interests Form must be dated and signed by a person legally authorized to represent the college/university.
Summary FOCI Data Sheet	Summary FOCI Data Sheet	Summary FOCI Data Sheet	Summary FOCI Data Sheet	Summary FOCI Data Sheet	Summary FOCI Data Sheet
Representative of Foreign Interest Statement [**when applicable**]	Representative of Foreign Interest Statement [**when applicable**]	Representative of Foreign Interest Statement [**when applicable**]	Representative of Foreign Interest Statement [**when applicable**]	Representative of Foreign Interest Statement [**when applicable**]	Representative of Foreign Interest Statement [**when applicable**]
List of key management personnel[29] In community property States, spousal information is also required on the key management personnel list. If single, so state.	List of key management personnel[11] Stock ownership form (shareholder's form). If there is a Shareholders Agreement, a copy MUST be provided.	List of key management personnel[11] Any authorizing resolutions of governing body that spell out authorities of the key management personnel.	List of key management personnel[11] Stock ownership form (shareholders' form) MUST be provided if partnership has public stock.	List of key management personnel[11] Any authorizing resolutions of the governing body that spell out the authorities of the key management personnel.	List of key management personnel[11] Any authorizing resolutions of the governing body that spell out the authorities of the key management personnel.

[29] Formerly known as the Owners, Officers, Directors, and Executive Personnel (OODEP) List.

Sole Proprietorship	Privately Owned Corporation	Publicly Traded Corporation	**Partnership** **1. General** **2. Limited** **3. Limited Liability**	Limited Liability Company	College/University
State Registration to do business/Tax ID Number.	Certificate of Incorporation (also known as Corporate Charter). Articles of Incorporation (with all amendments).	Certificate of Incorporation (also known as Corporate Charter). Articles of incorporation (with all amendments).	1. **General** – Similar to a sole proprietorship; may only be able to provide Certificate of Fictitious Business Name. 2. **Limited** – Certificate of Limited Partnership. 3. **Limited Liability Partnership** - Certificate of Limited Liability Partnership.	Articles of Organization	College/university charter (similar to articles of incorporation).
	Bylaws (attested copy with all amendments).	Bylaws (attested copy with all amendments).	Partnership Agreement.	Operating agreement.	Charter (or similar document to company's bylaws).
Latest financial report or a copy of the 1040 for the previous year (including Schedule C). NOTE: The most recent IRS tax return may ONLY be submitted if the tax return includes the information required being included on a balance sheet and income statement, and the tax return is a copy of the entire return.	Consolidated financial information, including notes, for the most recently closed accounting year. (If audited report is not available, entity must certify to the unavailability of audited information.) If company stock is not publicly traded but the company has publicly-traded debt, submit the Form 10-K filed with the Securities and Exchange Commission (SEC) for the company's most recently closed accounting year.	Consolidated annual report to shareholders for the most recently closed accounting year. Form 10-K report, and all Form 10-Q reports for financial quarters filed (with the SEC) since the last annual report (Form 10-K).	If publicly traded, submit consolidated annual report to shareholders for most recently closed accounting year; also Form 10-K and Form 10-Q reports for financial quarters filed (with SEC) since the last annual report (Form 10-K). If not publicly traded, submit latest consolidated annual report or audited financial information, including notes, for most recently closed accounting year. (If audited report is not available, entity must certify to the unavailability of audited information).	Consolidated financial information, including notes, for the most recently closed accounting year. (If audited report is not available, entity must certify to the unavailability of audited information).	Consolidated financial information, including notes, for the most recently closed accounting year. (If audited report is not available, entity must certify to the unavailability of audited information).

Sole Proprietorship	Privately Owned Corporation	Publicly Traded Corporation	**Partnership** **1. General** **2. Limited** **3. Limited Liability**	Limited Liability Company	College/University
	Most recent annual stockholders and board meeting minutes that identify directors and officers of corporation and company's voting list. Include any authorizing resolutions of governing body that spell out authorities of the key management personnel.		If required by the partnership agreement: The most recent Annual Stockholders and Board meeting minutes identifying directors and officers and company's voting list.		Most recent annual board meeting minutes identifying governing body and officers of the entity, and entity's voting list.

* FOCI determination is not required of self-employed individuals performing work under a consulting agreement.

** If applicable, each tier parent of the bidder must submit a complete package (i.e., information shown above for the applicable form of business).

*** A publicly-traded entity is not required to provide all identifying information on its owners as required on the key management personnel list unless those individuals are key management personnel of the U.S. organization. Instead, submit: (i) most recent Proxy Statement for annual meeting of Shareholders; and (ii) most recent copies of Schedules 13D's and/or 13G's received from any beneficial owner (foreign or domestic) who holds 5 percent or more of the U.S. organization securities.

SECTION I—FACILITY CLEARANCES AND REGISTRATION OF SAFEGUARDS AND SECURITY ACTIVITIES

1. OBJECTIVE. To ensure that safeguards and security (S&S) activities are afforded proper levels of protection consistent with Departmental standards to prevent unacceptable impact to national security, the environment, or the health and safety of the public or employees.

CHAPTER I. FACILITY CLEARANCE (FCL) PROGRAM

1. GENERAL. The FCL program regulates Department approval of a 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 Department of Energy (DOE) property worth more than $5 million, exclusive of facilities and land values (hereinafter referred to as security activities). The following delineates the primary requirements of the FCL program.

   a. Eligibility Requirements.

      (1) 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 the uncleared contractor. A contractor cannot sponsor themselves for an FCL.

      (2) The contractor or prospective contractor must meet the following eligibility requirements prior to being processed for an FCL. The contractor or prospective contractor must:

         (a) need an FCL in connection with a legitimate U.S. Government or foreign requirement;

         (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 (KMP) on the contract;

         (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 common defense and national security. This requirement only applies when the contract awarded or to be awarded requires access authorizations;

b. An FCL must be granted before any nuclear or other hazardous materials presenting a potential radiological, chemical, or biological sabotage threat; classified information or matter; or property protection interests are placed on premises occupied by the Department or its contractors.

c. The cognizant security authority must establish and maintain FCLs by registering, updating, suspending, reinstating, and terminating security activities under their cognizance. Each registered FCL must identify the highest security activity approved for that facility.

d. The FCL for a prime contractor must include those instances where classified access will include contractors.

e. The Safeguards and Security Information Management System (SSIMS) must be used by all Departmental elements to register FCL information over which they have cognizant security authority, survey cognizance, or registered security activities.

(1) DOE F 470.1, CSCS, is used to register information in SSIMS concerning contract vehicles [contracts, subcontracts, solicitations, purchase orders, Work for Others (WFO), leases, Cooperative Research and Development Agreements (CRADA), etc.] that require access authorizations (personnel security clearances). If a DD Form 254 has been used by the agency sponsoring the activity, it can be submitted instead of the DOE F 470.1 CSCS provided it is annotated with the DOE facility code. The DOE F 470.1 CSCS and DD Form 254 document specifics concerning each awarded contract (e.g., statement of work, classification, information pertaining to supplies, service, and other matters) to be furnished by the contractor to the government or by the government to the contractor.

(2) DOE F 470.2, "Facility Data and Approval Record" (FDAR), is used to record approvals, changes, and deletions of DOE contractor security facility information.

(3) The cognizant security authority and surveying offices, as identified by DOE line management, must ensure that SSIMS reflects established facilities and security activities under their jurisdictions by submission of an accurate DOE F 470.1 CSCS and DOE F 470.2 FDAR.

(4) 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 authority. This responsibility may be delegated, by mutual agreement, to another Department element.

(5) Any change in the responsible DOE cognizant security authority must include a written transfer of appropriate documentation (e.g., S&S plans; construction project status; FOCI files).

f. Certain company officials must be granted access authorizations in order for a company to qualify for an FCL involving classified information or matter, or special nuclear material (SNM). These company officials include the owners, officers, directors, partners, regents, trustees, or executive personnel (i.e., those considered KMP).

g. A contractor that will not possess classified information or matter, or SNM at the contractor's place of business and will only access such security activities at other cleared facilities must be cleared as a "non-possessing facility." A non-possessing contractor must adhere to the security plans of the facilities where the contractor is afforded access to classified information or matter, or SNM. In addition, a separate security plan must be executed to cover the non-possessing contractor's security responsibilities.

h. A self-employed individual or consultant who will not retain classified information or matter at his/her place of business does not require FCL. For security administration activities, to include the processing for an access authorization, the consultant will be considered an employee of the facility where he/she is afforded access to classified information or matter. The consultant and the cognizant security authority must jointly execute a security plan that sets forth their respective security responsibilities.

A self-employed individual or consultant who will retain classified information or matter at his/her place of business must be processed and granted an FCL that applies to the premises where the individual or consultant will store, handle, or process classified information or matter.

i. A contractor granted an FCL by an OGA may be granted a DOE FCL for processing, using, or storing classified information or matter, based on reciprocity.

j. Verification of the clearance and security capability of an OGA must be based on written assurance from that agency. No classified information or matter may be given to the OGA until the OGA has submitted the required verification of its clearance and security capability and the DOE cognizant security authority has approved and registered an FCL for the OGA in SSIMS.

2. EXCEPTIONS TO REGISTRATION IN SSIMS. Foreign intelligence information, sensitive compartmented information (SCI), special access programs (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. Exceptions to the registration requirements are identified below.

a. SAPs. SAPs are not registered in SSIMS. SAPs are registered under the contract requirements in DOE M 470.4-4, *Information Security*.

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 FDAR.

c. Cover Operations. Classified activities designated as "cover operations" (i.e., activities conducted in secrecy or concealment) are not registered in SSIMS as security activities (i.e., DOE F 470.1, CSCSs). The cognizant security authority must notify the appropriate Departmental element before granting the FCL.

CHAPTER II. IMPORTANCE RATINGS

1. FACILITY IMPORTANCE RATINGS. Importance ratings are used to identify the protection importance of facilities. Each facility's assigned importance rating must be recorded on DOE F 470.2 FDAR. Importance rating criteria are as follows.

   a. "A" Importance Ratings. Ratings 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 Departmental element;

      (2) authorized to possess Top Secret matter, 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. Ratings 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. Ratings 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. Ratings 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. Ratings assigned to a corporate tier parent (of a contractor organization) that has been barred from participation in the activities related to a contract with DOE.

f. "PP" (Property Protection) Importance Ratings. Ratings assigned to those facilities for which a special standard of protection must be applied. Basic considerations that include physical protection to prevent or deter acts of arson, civil disorder, riots, sabotage, terrorism, vandalism, and the threat or destruction of DOE property and facilities. These special standards are applied when a facility has:

(1) government property of a significant monetary value (more than $5 million, exclusive of facilities and land values);

(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. Ratings assigned to those facilities that have authorized access to classified information or matter, or SNM at other approved locations. Non-possessing facilities do not themselves possess any classified information or matter, or SNM.

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 authority functions. Changes to the facility importance rating must be registered in SSIMS by the submission of DOE F 470.2 FDAR.

CHAPTER III. ORGANIZATIONAL STRUCTURES AND FCLs

1. FCL FOR SINGLE LEGAL ENTITIES.

   a. Single FCL Registration. Only one FCL registration is required if the company and its classified security activities meet the following criteria.

      (1) 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).

      (2) The distance between the security activities is such that the contractor is able to maintain daily supervision of its operations, including day-to-day observations of the security program.

   b. Multiple-Facility Registrations for Multiple-Facility Organizations (MFOs).

      (1) When a company is composed of two or more facilities existing as a single legal entity, the home office facility must have an FCL at the same or higher level of any cleared facility within an MFO.

      (2) When branches, divisions, etc. of an MFO are cleared, the corporate headquarters must be registered in SSIMS as the home office.

      (3) Each separate branch, division, etc., of an MFO performing a security activity requiring access authorizations must be processed for an FCL and registered in SSIMS. This FCL registration must reflect the branch or division location and reference the home office.[30]

      (4) Because branches, divisions, offices, etc., of an MFO are not legally accountable in their own right, only the home office facility can execute an agreement/contract with the Government.

      (5) A FOCI determination is not required of the subordinate facility of an MFO. However, a subordinate facility of an MFO must submit a list of its (not its home office's) KMP, and the subordinate facility's KMP must be cleared (and excluded, if applicable) as required by Chapter V of this section.

[30] A multiple-facility organization may implement a consolidated security plan applicable throughout the organization, but the security plan must then be adapted as necessary to adequately address the requirements of each operating site.

2. PARENT–SUBSIDIARY RELATIONSHIP.

a. In a corporate tier parent-subsidiary relationship, the parent and each of its subsidiaries are separate legal entities and must be processed separately for FCL.

(1) 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.

(2) Because a subsidiary is legally accountable in its own right, the U.S. Government can permit the parent to remain uncleared or a subsidiary to hold an FCL of a higher level than the parent's.

(3) The DOE cognizant security authority is responsible for determining the necessity for the parent to be cleared:

(a) at the same level as the subsidiary;

OR

(b) at a lower level than the subsidiary;

OR

(c) excluded from access to all classified information or matter available to the subsidiary.

(4) The decision to clear or exclude must be based on:

(a) the parent's requirement for access authorizations to perform tasks or services essential to the fulfillment of a classified contract; and

(b) the parent's eligibility for an FCL, including its FOCI status. Information regarding FOCI negation action plans can be found in Section H of this CRD.

b. When, pursuant to paragraph 2a(4), above, it is determined that the FOCI for a parent is acceptable, the parent can be either excluded altogether from the requirement for an FCL or excluded from higher-level access by virtue of possessing an FCL at a level below that of the subsidiary. This exclusion must be based on formal action by the governing bodies of the parent and each intervening subsidiary level. Compliance with one or both of the exclusion actions listed below, as applicable, is mandatory before issuance to a subsidiary of an FCL requiring access authorizations.

(1) Parent Organizations.

(a) The parent organization's board of directors (or similar governing body) must adopt a resolution, which cannot be amended or repealed without notification to DOE, that excludes the parent organization, the members of its board of directors, and its officers, employees, representatives, and agents, as such, from access to all classified information or matter, or nuclear and other hazardous material presenting a potential radiological, chemical, or biological sabotage threat or to a higher category of classified (specifically identified in the resolution) entrusted to or held by the cleared subsidiary.[31]

1 This action must be made a matter of record in the minutes of the board of directors (or similar executive body).

2 A copy of the resolution, dated and identified by the name and address of the organization, must be furnished to the DOE cognizant security authority.

(2) Subsidiaries. The board of directors of a subsidiary whose parent organization (all shareholder firms in the chain of ownership) has executed exclusion resolutions (paragraph 2b above) must adopt a resolution, which cannot be amended or repealed without notification to DOE, that excludes the parent organization(s) from access to classified information or matter, or nuclear and other hazardous material presenting a potential radiological, chemical, or biological sabotage threat, as applicable, and acknowledges (i.e., notes) the exclusion resolution adopted by the parent's board of directors (or similar governing body).

(a) This action must be made a matter of record in the minutes of the board of directors (or similar executive body), and must be furnished to the DOE cognizant security authority.

(b) A copy of the resolution, dated and identified by the name and address of the facility, must be furnished to the DOE cognizant security authority.

[31]The applicable board resolution must be completed by all shareholder firms in the chain of ownership.

CHAPTER IV. INTERIM AND LIMITED FCLs

1. INTERIM FCL. National policy permits the granting of an interim FCL to an eligible contractor. Interim FCLs are granted on a temporary basis pending completion of full investigative requirements (i.e., final access authorization) for those individuals required to be cleared in connection with the FCL (e.g., KMP). Interim FCLs may be granted only:

   a. to avoid unacceptable delays in pre-contract negotiation or in performance on a contract; and

   b. after DOE has granted interim access authorizations to facility personnel requiring interim clearance.

   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.

   Foreign owned or controlled companies and non-U.S. citizens are not eligible for interim FCL.

2. LIMITED FCL. See Section H of this CRD for eligibility criteria, etc., for a limited FCL.

   A limited FCL must be restricted to one security activity involving classified information or matter, or SNM. Award of another security activity involving classified information or matter, or SNM requires separate FCL registration (i.e., under an FCL without restrictions or another limited FCL provided the eligibility criteria set forth in Section H for such FCL are met).

   Issuance of a limited FCL requires that strict access restrictions must be imposed to limit access to the scope of the contract. Such access restrictions must be reflected on the badges issued to the contractor's employees and also reflected in any central registration (local or Departmental) of issued DOE access authorizations.

   The clearance and exclusion requirements of KMP covered in Chapter V of this section apply to all FCLs, including a limited FCL.

CHAPTER V. ACCESS AUTHORIZATIONS AND EXCLUSION PROCEDURES REQUIRED IN CONNECTION WITH FCLs

1. ACCESS AUTHORIZATIONS REQUIRED IN CONNECTION WITH THE FCL. Certain officials [typically the owners, officers, directors, partners, regents, trustees, and/or executive personnel (KMP)] must always be cleared to the level of the FCL. The KMP who must always be cleared commensurate with the FCL and are listed below by type of organization. Based on their need for access, as determined by the DOE cognizant security authority, all other KMP must be cleared commensurate with the FCL level, cleared at a lower level, or excluded from being cleared. KMP exclusion determinations must be made prior to the granting of the FCL.

   a. Sole Proprietorships. The sole proprietor and the facility security officer (FSO) must be cleared commensurate with the FCL. Any KMP designated to succeed the sole proprietor or the FSO during permanent or temporary absence must be cleared commensurate with the FCL.

   b. Corporations, Nonprofit Organizations. The senior management official [i.e., president or chief executive officer (CEO)]; chairman of the board or, if meetings of the board of directors are chaired by a pro tem or rotating chairman, any board members who could serve as board chairman; and the FSO must be cleared commensurate with the FCL. Any KMP designated to succeed the senior management official, board chairman, or FSO during permanent or temporary absence must be cleared commensurate with the FCL.

   c. Partnerships. The managing partner and the FSO must be cleared commensurate with the FCL. Any partner designated to succeed the managing partner or the FSO during permanent or temporary absence must be cleared commensurate with the FCL.

   d. Colleges and Universities. The CEO, chairman of the board, or (if meetings of the board of regents, trustees, or directors are chaired by a pro tem or rotating chairman), any board members who could serve as board chairman, and the FSO must be cleared commensurate with the FCL. Any official or officer designated to succeed the CEO, board chairman, or FSO during permanent or temporary absence must be cleared commensurate with the FCL.

2. MULTIPLE FACILITY ORGANIZATIONS. Any of the business structures mentioned above may be configured as an MFO. Each subordinate facility's KMP must be cleared or excluded as required by paragraph 1 above. Subordinate facilities of an MFO must not be granted higher FCL or access authorizations than held by the home office of the MFO.

3. ACCESS AUTHORIZATIONS 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 access authorizations concurrent with the FCL. The granting of an FCL is not dependent on the access authorization of such employees.

4. EXCLUSION PROCEDURES. Other officials, as determined by the DOE cognizant security authority, must be cleared commensurate with the FCL level, cleared at a lower level, or excluded from being cleared. When other 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. When formal exclusion action is required, the organization's governing body must affirm the following items.

   a. Such officers, directors, partners, regents, or trustees (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; can be denied access to higher level classified information or matter (specified by level) 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.

      (1) This action must be made a matter of record in the minutes of the governing body.

      (2) A copy of the resolution, dated and identified by the name and address of the facility, must be furnished to the DOE cognizant security authority.

CHAPTER VI. FACILITY CLEARANCE

1. REQUIREMENTS. As part of the DOE Facility Clearance (FCL) Program, facilities are evaluated against a set of requirements to determine their ability to meet Departmental protection standards.[32] Approval of an FCL by DOE is based on a favorable evaluation of all of the following requirements.

   a. DOE F 470.2 FDAR. Completion and registration in SSIMS of DOE F 470.2 FDAR.

   b. DOE F 470.1 CSCS. Completion and registration in SSIMS of DOE F 470.1 CSCS or similar form (e.g., DD F 254) for contractor/subcontractor facilities performing contracts, subcontractors, and other contractor solicitations that require access authorizations.

   c. Security Plan. Approval of a security plan by the DOE cognizant security authority that describes the controls necessary within the facility to appropriately protect the security activities being performed. Such plans would include, but are not limited to, at least one of the following:

      (1) a site safeguards and security plan (SSSP) as required by Section A of this CRD; or

      (2) a site security plan (SSP) as required by Section A of this CRD.

   d. Survey.

      (1) For facilities with importance ratings of A, B, C, or PP, a comprehensive initial survey must be completed in accordance with Section G of this CRD. The survey must result in a composite facility rating of "satisfactory" and be conducted no more than 6 months before granting the FCL.

      (2) Completion of an initial review for non-possessing facilities.

   e. FSO. The FSO must be an employee of the company. The FSO must be appointed in writing. As covered in Chapter V of this section, the FSO must be cleared commensurate with the FCL and concurrent with the issuance of the FCL. The FSO and others performing security duties must complete security training in accordance with Section J of this CRD.

[32] Requirements for non-possessing facilities are covered in Chapter I, paragraph 1g of this section. Requirements for self-employed individuals or consultants who will not possess classified information or matter at their places of business are covered in Chapter I, paragraph 1h of this section.

f. FOCI. A favorable FOCI determination must be rendered in accordance with Section H of this CRD. A counterintelligence (CI) threat assessment and technology transfer risk assessment must be obtained and considered prior to a final decision to grant an FCL to an applicant company under FOCI or to restore an FCL previously suspended because the contractor was determined to be under FOCI.

g. Nuclear Materials Management and Safeguards System (NMMSS). A reporting identification symbol code for NMMSS must be established for facilities authorized to possess SNM and a nuclear materials representative must be appointed with the contractor requirements in DOE M 470.4-6, *Nuclear Material Control and Accountability*.

h. Access Authorizations. Granting access authorizations for personnel in connection with the FCL (i.e., KMP) and, as appropriate, company employees requiring access to perform tasks or services related to the fulfillment of a classified contract.

i. Exclusions. Exclusion procedures must be invoked in accordance with Chapters III and V of this section.

2. ISSUANCE OF FCLs. After all requirements (as mentioned above) have been satisfactorily met, the DOE cognizant security authority must notify the contractor in writing of the level of FCL granted. See Chapter IV of this section for requirements on the issuance of an interim FCL.

3. CHANGED CONDITIONS AFFECTING THE FCL. Contractors must report events that will or may have an impact on the status of the FCL (see Section H, paragraphs 7b-7f, for reportable changed conditions and anticipated changes). It is the contractor's responsibility to ensure that any change that might affect the validity of the FCL is reported to the DOE cognizant security authority.

4. INTERFACE WITH FOCI REQUIREMENTS. Procedures must be in place to ensure that coordination is accomplished between the FCL and FOCI programs. This includes notification of FOCI determinations rendered for the company and its tier parents, updating of determination dates, suspension of FCLs, etc. (see Section H of this CRD for a detailed discussion of the FOCI Program).

CHAPTER VII. PROCESS FOR FCL AND SECURITY ACTIVITY REGISTRATION

1. ACCEPTING OGA FCLs.

a. Contractor. A contractor with an equal or higher FCL granted by OGAs 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 agreement before acceptance of the FCL (i.e., the requirements identified below must be documented in a letter or MOA between the DOE cognizant security authority and the cognizant OGA).

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

(a) A limited FCL granted by an OGA cannot be accepted.

(b) An interim FCL at the Secret or Confidential level granted by an OGA cannot be accepted.

(c) An interim Top Secret FCL granted by an OGA may be accepted once the following have been completed:

1 the DOE cognizant security authority has analyzed the conditions of the interim FCL and the scope for the DOE work and determined that the interim FCL status is acceptable.

2 an interim FCL may be withdrawn if the interim personnel security clearance for an individual (KMP) is withdrawn. When an interim personnel clearance is withdrawn, the interim FCL must also be withdrawn unless action is taken to remove the individual from the position requiring access.

3 until a final FCL has been granted, a contractor with an interim FCL may not be eligible for certain categories of classified information such as weapon data [RD/Formerly Restricted Data (FRD)], COMSEC, SCI, SAP, or North Atlantic Treaty Organization (NATO). The names of each individual granted temporary access authorization under the interim FCL are obtained from the OGA and submitted to the Director, Office of Security.

(d) For DOE contracts involving proscribed information, the following requirements, as appropriate, must be met before accepting an FCL cleared in conjunction with a special security agreement.

1 When the company is controlled by a foreign government:

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

b a waiver must be granted by the cognizant Secretary (i.e., the Secretary of Energy and/or the Secretary of Defense). This waiver is based on 10 U.S.C. 2536(a) (i.e., Defense Authorization Act, which prohibits contract award involving proscribed information to foreign government-controlled companies); and

c the proposed Secretarial waiver must be prepared by the cognizant contracting officer, sponsored by the head of the contracting activity and appropriate Departmental element, and then forwarded through appropriate Department channels for approval and/or coordination with all affected agencies.

2 When a company is not controlled by a foreign government, the following activities must be completed prior to contract award:

a a National Interest Determination (NID) for the specific program/project/contract must be approved by the cognizant DOE Departmental Element and/or OGA official(s);

b a proposed NID must be prepared by the cognizant contracting officer, sponsored by the head of the contracting activity and Departmental element, and then forwarded through appropriate Department channels for approval and/or coordination with all affected agencies.

3 For contracts involving RD/FRD, the additional requirements set forth below in paragraphs 1a(6)(a)–(d) have been met or addressed, as appropriate.

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

(3) Protective Measures. Confirmation is 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 is confirmed by the OGA, and assurance is 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 authority following each scheduled survey.

(5) Access Authorizations. Each employee to be granted access to DOE classified information or matter must have appropriate DOE access authorization or, at a minimum, a Federal personnel security clearance equivalent to the required DOE access authorization. Discrepancies must be reconciled through interagency coordination on a case-by-case basis.

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

(a) An assurance is 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 classified at the Secret level or above, an assurance is obtained from the OGA that the facility's protective measures and procedures meet the requirements of the supplement to the National Industrial Security Program Operating Manual (NISPOM).

(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 will be accepting an FCL based on a DoD-approved Voting Trust Agreement, Proxy Agreement, Special Security Agreement, or Security Control Agreement, an assurance is obtained from the OGA that it will invite or 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 FCL holds an FCL granted by another Federal agency, the tier parent(s) does not need to provide DOE with a FOCI package provided the following reciprocity is accomplished with the OGA. Reciprocity between the DOE cognizant security authority and the OGA must be documented in a written agreement prior to DOE granting the subsidiary FCL. The written agreement must contain the requirements listed below.

(1) Classification Level/Category.

(a) When the FCL granted to a tier parent by an OGA is equal to the level of FCL required by the subsidiary, an assurance is obtained from the OGA that the DOE cognizant security authority will be notified prior to any reduction or increase to the level of the OGA-issued FCL that would require parent/subsidiary exclusion resolutions be invoked.

(b) If the FCL granted to a tier parent by an OGA is as an excluded parent or is lower or higher than the FCL required by the subsidiary, DOE must have the subsidiary and its tier parent(s) invoke the required exclusion resolutions.

(2) Validation of the Subsidiary's SF 328. The DOE cognizant security authority must provide the cognizant OGA with a copy of the subsidiary's executed SF 328, and the subsidiary's listing of KMP positions and personnel.

(a) Confirmation must be obtained from the OGA as to whether the agency determined if the tier parent's FOCI package(s) disclosed any FOCI issue(s) applicable to the subsidiary to be cleared by DOE.

(b) An assurance is obtained from the OGA that the DOE cognizant security authority will be notified if any FOCI issue(s) are subsequently reported to or identified by the OGA that will or might affect the DOE-granted subsidiary FCL.

(3) Transfer of Security Cognizance. An assurance must be obtained from the OGA that security cognizance will be transferred to DOE for any tier parent no longer requiring OGA FCL.

2. REGISTRATION OF OGA CONTRACTORS IN SSIMS. Classified mail channels must be registered in SSIMS for an OGA contractor organization where the Department does not have a contractual interest. 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 cognizant security authority and by the authorizing government official for the OGA contractor.

   Once the form is completed, the information must be entered into SSIMS. This process may only be used when the contractor facility has been approved by another Government agency and registered in SSIMS. Note: such an FCL cannot be used as a basis for registering additional security activities.

3. REGISTERING WORK FOR OTHERS (WFO) ACTIVITIES. The contractor requirements of DOE O 481.1C, *Work for Others (Non-Department of Energy Funded Work)*, dated 1-24-05, or successor documents, must be met before a WFO project or any "out of scope" modifications to existing WFO agreements are accepted.

   a. WFOs Performed at DOE-Owned or DOE-Operated Facilities.

      (1) OGA's WFO activities must be based on a determination that the S&S measures to be provided are consistent with DOE policy.

         (a) Before acceptance of WFO activities, the Department and the requesting agency must exchange classification and protection information, including the DD F 254 (or form similar in content).

         (b) 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.

         (c) These activities must be registered in SSIMS.

      (2) When subcontracting is required in connection with WFO, the subcontractor can be registered based on DOE F 470.2 FDAR and verification of the FCL. In this instance, a security cognizance agreement is not required.

         (a) If the subcontractor has a DOE FCL at the appropriate level, the WFO activity must be registered.

         (b) If the subcontractor has an FCL issued by an OGA.

         (c) If the subcontractor has no FCL or the FCL is at a lower level than required, see the requirements in paragraph 6 of this chapter.

b. WFOs 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. The WFO activity must be registered in SSIMS. Before the activity can be registered, the applicable contractor requirements in DOE O 481.1C, *Work for Others (Non-Department of Energy Funded Work)*, must be met and made part of the contract. Additionally, the following actions must be completed and documented.

(1) Verification that the FCL for the location where the work is to be performed meets or exceeds the level of clearance required for the WFO activity.

(2) Review and certification that the sponsoring organization has either provided the classification guidance or has stated in writing that the non-DOE-funded work will not entail classified activities as required by DOE M 475.1-1A, *Identifying Classified Information*, dated 2-26-01.

(3) Verification that classified security activities [i.e., those requiring access authorizations (personnel security clearances)] have been recorded as security interests on a DD F 254 (or a form similar in content).

(4) Execution of an agreement between DOE and the other agency with respect to reimbursement for any additional S&S costs incurred by DOE.

(5) The activity must be registered in SSIMS.

4. REGISTRATION OF SECURITY ACTIVITIES. Security activities are specific, unrelated tasks or contract elements involving security interests at a facility. Security activities must be registered in association with a specific FCL. The DOE cognizant security authority must ensure that each security activity is recorded on DOE F 470.1 CSCS and registered in SSIMS. If a DD F 254 has been used by the OGA sponsoring the activity, it will be annotated with the DOE facility code, if applicable and submitted instead of the DOE F 470.1.

a. Security Activities for Existing FCLs. The DOE cognizant security authority must perform the following actions.

(1) Determine and validate the security requirements, including access authorizations, for the proposed security activity.

(2) Determine the FCL status through SSIMS or the Defense Security Service (DSS)/Central Verification Activity System (CVAS).

(3) Compare the security requirements for the activity to the approved FCL in the following situations.

(a) When the contractor FCL is granted by an OGA, the requirements of paragraph 1 of this chapter must be met.

(b) When the contractor FCL is granted by DOE, the requirements listed below must be met.

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 applicable cognizant security agency (i.e., DOE cognizant security authority and/or OGA) in the manner set forth in paragraph 1b of this chapter for any tier parent(s) of the contractor holding a DOE or OGA FCL (i.e., FCL granted by the agency that rendered the FOCI determination).[33]

b. Registering New Security Activities.

(1) The procurement request originator must prepare a DOE F 470.1 CSCS or submit a DD F 254 to the contracting official. The contracting official must forward the completed DOE F 470.1 CSCS or DD F 254 to the DOE cognizant security authority. The cognizant security authority must ensure that each security activity is recorded on DOE F 470.1 CSCS and registered in SSIMS.

(2) When a new activity will exceed the current FCL or an FCL does not exist, the actions required to upgrade the current level or obtain an FCL must be completed as appropriate (these actions are detailed in paragraph 6 of this chapter). Upgrading an FCL may also require transfer of DOE cognizant security authority functions.

[33]Coordination is required in order to ensure compliance with national requirements (e.g., fulfill the Government's responsibility to validate and verify the company's foreign ownership, control, or influence to determine its initial and continuing eligibility for a facility clearance (FCL), ensure that exclusion resolutions are invoked when the parent organization either holds no FCL or holds a FCL at a lower level than the subsidiary).

c. Changing Security Activity Information. The DOE cognizant security authority who established the security activity is responsible for updating and changing security activity information. Changes must be registered in SSIMS through submission of an updated DOE F 470.1 or DD F 254.

d. Terminating Security Activities. When a registered security activity is terminated, the organization that established the security activity must ensure that all affected access authorizations are terminated and all DOE property, classified information or matter, or nuclear and other hazardous material presenting a potential radiological, chemical, or biological sabotage threat 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 facility and maintained by the DOE office that established the security activity. SSIMS must then be updated to reflect the change in status.

SECTION J—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. The Department of Energy (DOE) National Training Center (NTC) provides assistance and resources for the development and instructional needs for security and safety.

2. S&S TRAINING PROGRAM REQUIREMENTS.

   a. Key Program Elements. The S&S Training Program must encompass the following key S&S program elements:

      (1) Program Planning and Management,

      (2) Personnel Security,

      (3) Physical Protection,

      (4) Protective Force (PF),

      (5) Nuclear Material Control and Accountability,

      (6) Information Security.

   b. Job Analysis. A job analysis must identify, describe, and document major tasks and skill requirements.

   c. Testing. Knowledge- and/or performance-based testing must be used to measure the knowledge and/or skills acquired from training programs.

   d. Training Content. 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. Performance testing of individual and small unit tactics must be performed as part of initial, refresher, and on-the-job training for the PF.

   e. Training Course Development. A systematic approach must be used to produce training products that ensure the individual acquires the knowledge and skills necessary for the individual to perform their assigned duties. The approach used must have the following phases: analysis, design, development, implementation, and evaluation.

      (1) Analyses. Analyses must be conducted to ensure that training courses reflect the requirements of the job competencies. Training requirements

Vertical line denotes change.

must be determined by analyzing needs, the job or function, or performance deficiencies

(a) Needs analyses must be conducted in response to identified performance problems to validate the need for training.

(b) Job analyses must identify critical tasks. Job analyses will determine the frequency and method of training.

(c) Analysis must include determination of delivery methods to ensure the most effective training outcome (i.e. Web-based training, interactive television, classroom-based, or a combination of delivery methodologies).

(2) Design. Instructional objectives must be developed based upon the skills and knowledge associated with a task and must form the basis for the development of all training materials, tests, and strategies.

(3) Development.

(a) Lesson plans must reflect instructional objectives to ensure consistent achievement of those objectives each time the course is taught.

(b) Course design documents and training materials used to support instructional objectives must be technically accurate and current.

(4) Implementation.

(a) Training will be conducted using certified instructors who have appropriate experience and/or training to ensure the accomplishment of instructional objectives. Instructor certification will be obtained through the NTC. Instructors will be recertified at least once every 2 years (at least every 24 months) to maintain technical proficiency.

(b) Qualified personnel whose past experience in training is such that they may be exempted from training may be allowed to do so on a case-by-case basis through testing or equivalency. When testing is used for this purpose, it will consist of the same or equivalent examinations based on instructional objectives as stated for the required training course.

(c) Completion of testing or granting of equivalency will be documented in the training records system.

(5) Evaluations. Evaluations of training must be performed to ensure that instructional objectives are met and to determine the overall effectiveness.

f. Training Approval Program (TAP). A TAP is a process to ensure that established objectives, standards, and criteria are met by validating, through the Office of Security, contractor security training programs conducted by organizations other than the NTC.

(1) Upon the request of the Departmental element the NTC will certify site implementation of NTC-developed courses.

(2) Site programs must be examined by representatives of the NTC at least every 5 years (at least every 60 months) to verify adherence to Department objectives and standards and to provide program approval recommendations to the Director, Office of Security.

(3) Initial and recurring reviews for training approval must cover all aspects of local training programs including program management and structure, course content, training facilities, observation of course presentations for effectiveness, and evaluation of students.

(4) Training approvals will remain valid for a period of 5 years.

(5) TAPs must be re-evaluated and resubmitted for approval based upon significant changes in operational missions or conditions.

g. Training Records Management.

(1) Training records must be maintained.

(2) Training records must contain dates of course attendance, course title, and scores/grades achieved, where applicable.

(3) Training records may be retained in electronic or hardcopy form.

(a) Training provided at the NTC must be recorded by the NTC and the organization sponsoring the individual.

(b) Records of training provided at other facilities, including contractor or other Government facilities, must be provided to, and retained by, the organizations sponsoring the individual.

h. Training Plans. Training plans that project training derived from a valid needs analysis for the forthcoming year must be developed annually (at least every 12 months) for each program element. Annual training plans must be approved by the DOE cognizant security authority and must address:

(1) training needs analysis,

(2) critical needs, or those immediate training needs which when met will be effective at improving organizational and workforce performance,

(3) training goals and objectives,

(4) major training delivery programs, projects, and other significant activities,

(5) mandatory training and qualifications for compliance with DOE requirements and any additional requirements directed by DOE line management.

SECTION K—SAFEGUARDS AND SECURITY AWARENESS PROGRAMS

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

2. REQUIREMENTS.

   a. Briefings. S&S awareness programs must include:

      (1) an initial briefing for all contractor employees;

      (2) comprehensive, refresher, and termination briefings for all contractor employees and personnel granted Department of Energy (DOE) access authorizations.

      (3) appropriate awareness briefings for any non-DOE personnel granted unescorted access to Departmental security areas (e.g., regarding information on prohibited articles).

   b. Classified Information Nondisclosure Agreement (SF 312). An individual granted a DOE access authorization must execute a "Classified Information Nondisclosure Agreement" (SF 312) or otherwise comply with 32 CFR, Chapter XX, before being granted access to classified information or matter.

   c. Supplementary Awareness Activities. S&S awareness programs must include supplementary activities to keep individuals aware of their responsibilities.

3. PROGRAM DESIGN AND DEVELOPMENT.

   a. Program Design. S&S awareness programs must include objectives designed to meet site-specific needs and Federal requirements, and ensure cleared and uncleared personnel are continuously aware of their S&S responsibilities.

   b. Program Development. Procedures must be developed to ensure implementation of all S&S awareness program requirements.

   c. Program Assessment. S&S awareness programs must be assessed in accordance with Section G of this CRD.

4. BRIEFINGS. S&S awareness briefings for cleared personnel must address site-specific needs, S&S interests, and potential threats to the facility/organization. Contents must be updated as necessary. Records must be maintained in a manner that provides an audit trail that verifies an individual's receipt of the briefings.

a. Initial Briefing. Personnel who receive a DOE security badge must receive an initial briefing before they are given unescorted access.

(1) Content.

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

(b) overview of facility/organization's major S&S program and their 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 unclassified controlled information;

(h) procedures for reporting incidents of security concern (e.g., attempts to gain unauthorized access 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 an access authorization 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) Classification and declassification requirements and procedures:

1 definition of classified information and matter;

2 purpose of DOE classification and declassification program;

3 levels and categories of classified information or matter;

4 damage criteria associated with each classification level;

5 authority for classification and declassification; and

6 procedures for challenging the classification status of information.

(b) Classified information protection elements:

1 procedures for protecting classified information or 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 unclassified controlled information, including telecommunications and electronic transmissions;

8 information pertaining to security badges, access authorization 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.

(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 an access authorization is extended or transferred to another DOE facility/organization. Initial and comprehensive briefings may, at the discretion of line management, be combined only if the access authorization has been extended. 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 may be used to document this briefing.

c. Refresher Briefing. Cleared individuals must receive annual (at least every 12 months) 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.

(1) Content. Refresher briefings must selectively reinforce the information provided in the comprehensive briefing. Refresher briefings must also address current facility-/organization-specific S&S issues and counterintelligence (CI) awareness. The CI awareness component should use material on this topic prepared annually (at least every 12 months) by the NTC or developed in coordination with the local CI office.

(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 briefings. Documentation may be in electronic or hardcopy 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 an access authorization has been or will be terminated. Termination briefings must reiterate to the individual the continuing responsibility not to disclose classified information 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 authority or to the DOE.

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

(a) information contained in items 1 through 6 of DOE F 5631.29, "Security Termination Statement;"

(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 of 1954, and 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 an access authorization, 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) 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.

5. CLASSIFIED INFORMATION NONDISCLOSURE AGREEMENT.

a. Administration.

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

(2) Any individual who refuses to execute an agreement must be denied access to classified information or matter and reported to the cognizant security authority.

(3) Any DOE employee can witness a DOE or contractor employee's agreement but only an authorized DOE employee may accept a contractor employee's agreement, or a contractor representative may be authorized in writing by the DOE cognizant security authority to witness and to accept an agreement from a contractor employee on behalf of the U.S. Government.

b. Retention. The original SF 312 or legally enforceable facsimile of the SF 312 may be retained by the contractor for the duration of the individual's employment or it may be sent to the servicing personnel security offices. In any event, the

agreement must be with DOE for retention after the termination of employment, and the cognizant security authority must ensure SF 312s retained by contractors are sent to DOE upon the termination of employment of contractor employees.

c. Storage. The original or legally enforceable facsimile of the SF 312 must be stored in a file system, such as personnel files, from which they can be expeditiously retrieved if the U.S. Government seeks enforcement or subsequent employers require confirmation of execution.

6. SUPPLEMENTARY AWARENESS ACTIVITIES.

a. Purpose. Supplementary S&S awareness activities must be provided between annual (at least every 12 months) and refresher briefings to ensure that individuals are aware of their S&S responsibilities.

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

SECTION L—CONTROL OF CLASSIFIED VISITS PROGRAM

1. OBJECTIVE. To ensure that only persons with the appropriate access authorizations and need to know receive access to classified information or matter, in connection with visits involving the release or exchange of classified information or matter.

2. REQUIREMENTS.

   a. Procedures. Line management must establish local procedures for the control of classified visits. Procedures must ensure the following actions.

      (1) Verification of the visitor's identity, programmatic need-to-know, and that the visitor's clearance or access authorization is at least equal to the classification of the information to which access is being requested.

      (2) Identification of limitations and enforcement of controls for access to classified information or matter or facilities and submission of appropriate forms, requests, etc., to the cognizant security authority and programmatic line management within the timeframes below.

         (a) Visit requests must be submitted at least 15 working days before the date of a one-time visit or the first day of a recurring visit.

            1 Department of Energy (DOE) and DOE Contractor Employees. DOE Form (F) 5631.20, Request for Visit or Access Approval, must be used by DOE Federal and contractor employees to obtain programmatic approval for Sigma access. This form does not need to be submitted to visit Department facilities. A DOE security badge will serve as evidence of DOE access authorization.

            2 Other Government Agency (OGA) and OGA Contractor Employees. DOE F 5631.20 (or form similar in content) must be used by employees of OGAs to obtain access approval for visits to DOE facilities.

         (b) Exceptions to required processing times will be allowed only for emergency visits (i.e., visits that must take place as a matter of urgency and importance and the processing lead time cannot be met). Emergency visits will only be approved as one-time visits.

         (c) Requests for visits/access to weapons programs, nuclear materials production facilities, or sensitive nuclear materials production information must be referred to the Associated Administrator for Defense Nuclear Security.

(d) Requests for visits/access to uranium enrichment plants or facilities engaged in uranium enrichment technology development, including advanced isotope separation technology, must be referred to the Office of Nuclear Energy, Science, and Technology.

(e) Requests for access to Naval Nuclear Propulsion facilities must be referred to the Deputy Administrator for Naval Reactors.

(3) Continuing visitor access approval is necessary for individuals who frequently visit DOE facilities. However, the access approval cannot exceed a period of 1 year or the final day of a contract for contractors, whichever is less. The approval may be renewed annually.

(4) Operational approval of visits.

(5) Maintenance of documentation associated with all classified visits/access.

(a) Records of classified visits by employees and contractors of OGAs must be maintained.

(b) Records of classified visits by DOE Federal and contractor employees that entailed Sigma access must be maintained.

(c) Records of requests for classified visits by DOE contractor employees to OGAs must be maintained.

(6) Referral of any nonroutine, written, or visual material resulting from classified visits and proposed for public release to the Director, Public Affairs.

(7) Limiting the sending and receiving of a classified visit request to the security office of OGAs.

b. Classified Visits by Departmental Employees, Contractors, and Subcontractors.

(1) Visitors are responsible for making administrative arrangements and obtaining approval from the Department element, as appropriate. (The authority granting such approval is responsible for informing the facility to be visited.)

(2) Contractors or subcontractors with mutual program interests may be authorized, subject to the limitations in paragraph 2b(3), below, to arrange for visits without obtaining Department approval if such authorization will be advantageous to the Department.

(3) Visitors who require access to weapon data (classified Secret or Top Secret), Top Secret information (non-weapon data), 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.

(a) Facility Visits. When the classified visit is under the auspices of a Departmental element, the programmatic approval for the visit must be obtained from the Departmental element exercising jurisdiction over the facility.

(b) Headquarters Visits. When the classified visit is under the auspices of line management, the programmatic approval for the visit must be obtained from both the responsible line management and the Departmental element being visited.

c. Visits to DoD and NASA Facilities. Both agencies accept DOE access authorizations for Restricted Data (RD) and other classified information or matter under their jurisdictions on the same basis as the Department if access authorization and need to know are properly certified.

(1) DOE Top Secret approvals must be specifically certified in the event access to Top Secret information is required.

(2) A DOE F 5631.20 must be forwarded directly to the military or civilian official with jurisdiction over the information to which access is being requested.

(3) Any exchange of RD occurring during the course of a visit must be accomplished as stated in paragraph 2e below.

d. RD Visits by NRC Employees.

(1) Visits to DOE facilities 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 Department classified weapon or production facility must:

(a) be arranged through the Departmental element coordinating the visit;

(b) have prior approval of the Associate Administrator for Defense Nuclear Security if visiting classified weapon or production facilities;

(c) have necessary clearance verification and certification by the NRC Director of Security that access to the information requested is required in performance of official duties.

(2) Visits involving access to RD not requiring prior approval from the Departmental element exercising jurisdiction over the facility or the office to be visited may be arranged directly by NRC with the Departmental element provided this procedure does not conflict with the existing visitor control procedures of the cognizant security authority. (NOTE: A DOE F 5631.20 or equivalent NRC visit request form is required.)

(3) The NRC identification badge must not be used as authority for visits in lieu of the aforementioned specific visit approval arrangements.

e. RD Visits by DoD and NASA Employees.

(1) Access to RD is contingent upon submission of a DOE F 5631.20; NASA Form 405, Request for Access Approval; or a memorandum or electronic message signed by or in the name of the certifying official. The request must be forwarded for approval or other action to the Departmental element with jurisdiction over the information to which access is requested.

(2) Requests for access must include the following:

(a) names, citizenship, dates of birth, and social security numbers of persons requesting access and organizations represented (if not Armed Services, relationship to DoD or NASA);

(b) facility and information to which access is requested (access to critical nuclear weapon design information must be specified as requested);

(c) security clearance or access authorization status of each person, including clearance date;

(d) purpose of visit and certification that the person needs the access in the performance of duty;

(e) anticipated date of visit and names of persons to be visited (if a conference is involved, the date, place, and sponsor of the conference must be specified); and

(f) a certification that the matter to which access is requested relates to aeronautical and space activities, for requests from NASA.

(3) The approving official must have the authority to approve such access.

(4) Control of access to RD in the custody of another Federal agency by members of the Armed Services or by DoD or NASA personnel or contractors is the responsibility of the appropriate official or his/her designee (see Appendix 7, Access to Restricted Data in Possession of Other Federal Agencies, for a listing of those officials).

f. Other Classified Visits by DoD and NASA Employees.

(1) Requests for such visits to DOE, contractor, and subcontractor facilities are approved by line management, or in the case of HQ elements, by the cognizant Departmental element after ensuring that each visitor has the appropriate military or NASA security clearance and requires the information in the performance of their duties.

(2) Certification of security clearances may be made by memorandum, electronic message, DOE F 5631.20, or NASA Form 405.

g. Classified Visits by Employees of OGAs.

(1) Requests for visits to DOE facilities by employees, contractors, or subcontractors of Federal agencies other than DoD, NASA, or NRC are approved by the cognizant security authority.

(2) RD may not be exchanged with persons in this category unless they have appropriate DOE access authorization.

(3) Classified information or matter other than RD may be exchanged provided the individual has the appropriate Q or L access authorization or a security clearance granted under the provisions of Executive Order 12968, *Access to Classified Information*, and need for such access has been verified.

(4) Certification of security clearances or RD access must be made on DOE F 5631.20.

Vertical line denotes change.

h. Congressional and State Classified Visits. Requests for visits to DOE, contractor, or subcontractor facilities by members or employees of Congress or congressional committees and by governors or their staffs must be approved by the Departmental element with jurisdiction over the facilities to be visited, provided the following are verified:

(1) visitor's identity;

(2) access authorization or security clearance; and

(3) need to know.

i. Emergency Visits to Classified Areas and Facilities.

(1) In an emergency, requests for visit approval may be made by telephone or electronic message.

(2) Telephonic requests must be confirmed by memorandum or electronic message.

j. Classified Visits to Department of Energy Facilities by Non-U.S. Citizens. The exchange of classified information or matter with non-U.S. citizens, whether through visits to DOE or contractor facilities or foreign travel by DOE employees or contractors, is covered in the contractor requirements document for DOE O 142.1, *Classified Visits Involving Foreign Nationals,* dated 1-13-04.

SECTION L

APPENDIX 7—ACCESS TO RESTRICTED DATA IN POSSESSION OF OTHER FEDERAL AGENCIES

The following Federal officials are authorized to permit their Federal and contractor employees with DOE access authorizations to grant access to restricted data (RD) in their possession to members of the Armed Forces and Department of Defense (DoD) and National Aeronautics and Space Administration (NASA) employees and their contractors, in accordance with Title 42 U.S.C. Section 2163 and 2455(b).

- The Assistant to the President
- Director, Office of Management and Budget
- Executive Secretary, National Security Council
- Director, Central Intelligence Agency
- Director, Federal Emergency Management Agency
- Secretary, Department of Homeland Security
- Secretary of State
- Secretary of the Treasury
- Attorney General of the United States
- Secretary of the Interior
- Secretary of Agriculture
- Secretary of Commerce
- Secretary of Labor
- Secretary of Health and Human Services
- Secretary of Transportation
- Secretary of Education
- Chairman, Federal Communications Commission
- Administrator, Agency for International Development
- President, National Academy of Sciences and National Research Council
- Director, National Science Foundation
- Chairman, Tennessee Valley Authority
- Director, United States Information Agency
- Comptroller General of the United States

Vertical line denotes change.

SECTION M—DEVIATIONS

1. OBJECTIVE. To establish procedures, coordination, and approval levels that must apply to all deviations from Department of Energy (DOE) safeguards and security (S&S) program directive requirements.

2. REQUIREMENTS. There are 3 categories of deviations: variations; waivers; and exceptions. Deviations from S&S program directive requirements require approval before implementation. Table M-1, Deviation Approval Process, depicts the approval level required for the various types of deviations.

   a. Deviations. Deviations from S&S program directive requirements require approval before implementation. Table M-1, Deviation Approval Process, depicts the approval level required for the various types of deviations. Coordination, approval, and duration limits are as follows.

Table M-1. Deviation Approval Process

Deviation	Approval Level			
	Related to Protection of Category I and II Quantities of SNM	Related to Other S&S Program Directive Requirements (exclude Exceptions to SECON, see Part 1, Section B)		
		Field	NNSA HQ	Non-NNSA HQ
Variance: Approved conditions that technically vary from S&S directives' requirement, but afford equivalent levels of protection **without compensatory measures**.	**Departmental element** cc: SO	**DOE cognizant security authority** cc: SO, Departmental element, and Associate Administrator for Defense Nuclear Security for NNSA	**Cognizant Deputy Administrator** Concurrence of Associate Administrator for Defense Nuclear Security cc: SO	**Departmental element** SO Concurrence
Waiver: Deviation from S&S directive that **requires compensatory measures** to preclude potential or real vulnerability.	**Under Secretary for Nuclear Security** (for NNSA sites) **Under Secretary for Energy, Science, and Environment** (for non-NNSA sites) cc: SO	**DOE cognizant security authority** With 30-day advance notice to SO and, for NNSA facilities, Associate Administrator for Defense Nuclear Security	**Cognizant Deputy Administrator** With 30-day advance notice to and of concurrence of Associate Administrator for Defense Nuclear Security	**Departmental element** SO Concurrence
Exception: Deviation creating vulnerability for which there are no adequate compensatory measures.	**Secretary of Energy** or **Deputy Secretary of Energy** cc: SO	**Under Secretary for Nuclear Security** (for NNSA Sites) **Under Secretary for Energy, Science, and Environment** (for non-NNSA sites) with concurrence of Departmental element cc: SO	**Deputy Secretary** SO Concurrence	**Deputy Secretary** SO Concurrence

(1) Variances. Variances are approved conditions that technically vary from an Office of Security directive requirement but afford equivalent levels of protection without compensatory measures.

(a) Approval Process for Variances.

1 Variances Related to Protection of Category I and II Quantities of Special Nuclear Material (SNM).

a The cognizant security authority for the contractor must submit the request for a variance through the contractor line management to the DOE cognizant security authority for approval.

b The contractor line management must not implement any variance related to protection of Category I and II quantities of SNM without Departmental element approval.

2 Variances Related to Other S&S Program Contractor Requirements.

a The cognizant security authority for the contractor must submit the request for a variance through the contractor line management to the DOE cognizant security authority for approval.

b The contractor line management must not implement the variance without DOE approval.

c The Director, Office of Security must concur on variances to national policy requirements, such as the National Industrial Security Program (NISP) or the Personnel Security Program.

(b) Duration of Variances. There is no restriction on the length of time for which a variance can be approved.

(2) Waivers. Waivers are approved nonstandard conditions that deviate from a contract requirement that if uncompensated would create a potential or real S&S vulnerability. Waivers, therefore, require implementation of compensatory measures (e.g., additional resources to implement enhanced protection measures) for the duration of the waiver.

(a) Approval Process for Waivers.

1 Waivers Related to Protection of Category I and II Quantities of SNM.

a The cognizant security authority for the contractor must submit the request for a waiver through the contractor line management to the DOE cognizant security authority for approval. The cognizant security authority approval is contingent upon:

i. the presence of adequate compensatory measures in place before waiver implementation; and

ii. the documentation of any appropriate performance testing/vulnerability assessments (VAs).

b The contractor line management must not implement any waiver related to protection of Category I and II quantities of SNM without the approval of the Under Secretary for Nuclear Security for NNSA sites or the Under Secretary for Energy, Science, and Environment (ESE) for ESE sites.

c If the Office of Security disagrees with the waiver, written notification will be made to either the Under Secretary for Nuclear Security or the Under Secretary for Energy, Science, and Environment and the Deputy Secretary of the basis for the disagreement.

2 Waivers Related to Other S&S Program Contractor Requirements.

a The cognizant security authority for the contractor must submit the request for a waiver through the contractor line management to the DOE cognizant security authority for approval. Cognizant security authority approval is contingent upon:

i. comments provided by HQ elements are formally reconciled before waiver implementation;

ii. adequate compensatory measures are in place before waiver implementation; and

iii. documented performance testing/VAs, if appropriate, are accomplished prior to waiver implementation.

b The contractor line management must not implement the waiver without DOE approval.

c The Director, Office of Security must concur on waivers to national policy requirements, such as the NISP or the Personnel Security Program.

(b) Duration of Waivers. Waivers must not be approved for periods exceeding 2 years.

(3) Exceptions. Exceptions are approved deviations from a contract requirement that can create an S&S vulnerability. Exceptions must be approved only when correction of the condition is not feasible and compensatory measures are inadequate to preclude the acceptance of risk.

(a) Approval Process for Exceptions.

1 Exceptions Related to Security Conditions.

a For other non-NNSA operations, a request for an exception must be sent to the Under Secretary for Energy, Science, and Environment for review and approval.

b For NNSA operations, a request for an exception must be sent to the Under Secretary for Nuclear Security for review and approval.

2 Exceptions Related to Protection of Category I and II Quantities of SNM.

a The cognizant security authority for the contractor must submit the request for an exception through the contractor line management to the DOE cognizant security authority for approval.

b The contractor line management must not implement any exception related to protection of Category I and II quantities of SNM without the

approval of the Secretary of Energy or the Deputy Secretary of Energy.

c If the Office of Security disagrees with the exception, written notification will be made to either the Under Secretary for Nuclear Security or the Under Secretary for Energy, Science, and Environment and the Deputy Secretary of the basis for the disagreement.

3 Exceptions Related to All Other S&S Program Directive Requirements.

a The cognizant security authority for the contractor must submit the request for an exception through the contractor line management to the DOE cognizant security authority for approval.

b The contractor line management must not implement the exception without DOE approval.

i. comments provided by HQ elements are formally reconciled before exception implementation;

ii. adequate compensatory measures are in place before exception implementation; and

iii. documented performance testing/VAs, if appropriate, are accomplished prior to exception implementation.

c Exceptions to national policy requirements, such as the NISP or the Personnel Security Program, must have the concurrence of the Director, Office of Security and the approval of either the Deputy Secretary or Secretary prior to implementation.

(b) Compensatory Measures. Compensatory measures implemented as the basis for an exception request must be subject to formal VAs. Compensatory measure implementation must be tested and validated.

(c) Duration of Exceptions. Exceptions must not be approved for periods exceeding 3 years (36 months).

(d) Annual Validation. The need for an exception must be validated annually (at least every 12 months) and documentation submitted through the DOE cognizant security authority to the Office of Security and cognizant Departmental element.

b. Documentation.

(1) Deviation Request Format. Specific information requirements for deviations are provided in Appendix 8, Format for Deviation Requests.

(2) Assessments and Performance Testing. The results of VAs and tests must be documented in the deviation request and in the site safeguards and security plan (SSSP)/site security plan (SSP), as appropriate.

(3) Security Plans. Approved deviations must be documented in the SSSP/SSP and site procedures as appropriate. A deviation request approved out of cycle with the S&S plan formulation and approval process must be documented as an attachment to the applicable plan until the next annual update.

c. Extensions. Any extension to the approved period of time for deviations requires reapplication of the deviation process.

Vertical line denotes change.

SECTION M

APPENDIX 8—FORMAT FOR DEVIATION REQUESTS

1. Date. Date the request is signed by the requesting official.

2. Request Number. Alphanumeric identifier beginning with "SO" followed by the routing symbol used in the DOE National Telephone Directory, followed by the last two digits of the year of the request, followed by the three-digit number that is next in the sequence of requests from that cognizant security authority in that calendar year. For example, the third request from Headquarters during 2005 would be SO-HQ-05-003.

3. Deviation Title. Short, concise description of the specific deviation (e.g., Request for waiver of the vault-type-room requirements for building Z3999, Room 101; Request for variance for limited area barrier boundary).

4. CRD Citation. Title and date of the contractor requirements document from which a deviation is being requested with a citation (paragraph or other provision) and summary of the contractor requirements document requirements.

5. Impacted Entity. Identification of the specific facility (by SSIMS facility code number), process, procedure, system, etc.

6. Deviation Justification. Specific description of the deviation and the associated reason or rationale for the deviation request. A description of the relationship of the requested deviation to other S&S interests must be included if they are significantly affected.

7. Protection Measures. Description of the current measures used for protection and an evaluation of the effectiveness of such measures; description of alternate/compensatory measures or levels of protection to be provided as an alternative to contractor requirements document.

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

   NOTE: Waivers cannot be for more than 2 years (24 months); exceptions cannot be in place for more than 3 years (36 months).

9. Risks. Evaluation of the risks associated with the deviation, if approved. Results of vulnerability analyses and performance tests conducted on proposed alternatives must be included.

10. Signature. Requesting official's signature.

Vertical line denotes change.

SECTION N—INCIDENTS OF SECURITY CONCERN

1. OBJECTIVES. To set forth requirements for the Department of Energy (DOE) Incidents of Security Concern Program, including timely identification and notification of, response to, inquiry into, reporting of, and closure actions for incidents of security concern.

2. REQUIREMENTS. The broad-based requirements for implementing this section are listed below with elaboration provided in associated chapters. Additionally, there may be instances where security incidents are required to be reported through other department reporting systems (e.g., Computer Incident Advisory Capability, Occurrence Reporting and Processing System).

   a. Any person who observes, finds, or has knowledge or information about a potential incident of security concern must immediately report this information to the Facility Security Officer (FSO) or designee of the facility where the incident occurred. The FSO or designee must make notifications as specified in Chapter I, paragraph 3, of this section.

   b. Any person discovering a potential incident of security concern, including one that involves classified information or matter; special nuclear material (SNM), including material protected, controlled, and accounted for as SNM; or other security interests at risk (e.g., interests not properly controlled), must make reasonable efforts to safeguard the security interests in an appropriate manner. The individual must also ensure evidence associated with the incident is not tampered with or destroyed.

   c. Any person discovering actual or suspected fraud, waste, or abuse of Government resources must ensure such incidents are reported to the Office of the Inspector General in accordance with DOE O 221.1, *Reporting Fraud, Waste, and Abuse to the Office of Inspector General*, dated 3-22-01.

   d. Locally developed procedures must be established, documented, approved by the Departmental element, and disseminated to ensure the identification, reporting, root cause analysis, and resolution of incidents of security concern. These procedures must also identify guidelines for corrective actions and documentation of time and funds expended on incidents.

   e. Inquiries must be conducted to establish the facts and circumstances surrounding an incident of security concern.

   f. Appropriate Federal (to include the Office of Security), State, and local organizations must be contacted when a violation of law is suspected or discovered.

g. Appropriate corrective actions must be taken for each incident of security concern to reduce the likelihood of recurrence of the incident, including review and/or revision of applicable safeguards and security (S&S) plans and procedures.

h. The party or parties responsible for an incident of security concern must be subject to appropriate administrative actions, including disciplinary measures, retraining, counseling, or other directed actions necessary to reduce the likelihood of recurrence of the incident.

CHAPTER I. IDENTIFICATION AND REPORTING REQUIREMENTS

1. GENERAL.

   a. A system of controls and procedures must be developed, approved, implemented, enforced, and maintained:

      (1) to deter, detect, and prevent recurrence of incidents of security concern and

      (2) for the timely identification and notification of, inquiry into, analysis of, and reporting of incidents of security concern.

   b. Inquiries are used to determine the root causes of and individuals responsible for incidents of security concern.

   c. All discussions and documents associated with an incident of security concern must be classified or controlled according to current classification or control guidance and follow procedures contained in contractor requirements.

2. INCIDENT IDENTIFICATION AND CATEGORIZATION. DOE uses a graded approach for identification and categorization of incidents of security concern. 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 section based on the severity of security incidents. The following paragraphs provide the basis for identification and categorization of incidents of security concern.

   a. Incident Identification. Incidents of security concern are actions, inactions, or events that have occurred at a site that:

      (1) pose threats to national security interests and/or critical DOE assets;

      (2) create potentially serious or dangerous security situations;

      (3) potentially endanger the health and safety of the workforce or public (excluding safety related items);

      (4) degrade the effectiveness of the S&S program; or

      (5) adversely impact the ability of organizations to protect DOE S&S interests.

b. Incident Categorization. Incidents of security concern must be categorized in accordance with their potential to cause serious damage or place S&S interests and activities at risk. Four categories of security incidents have been established based on the relative severity of the incident. Each of the four categories is identified by an impact measurement index (IMI) number as follows (from most severe to least severe): IMI-1, IMI-2, IMI-3, and IMI-4. Each of the four categories is further subdivided into specific subcategories based on the security topical areas of physical protection, protective force (PF), information security, personnel security, and nuclear material control and accountability (MC&A). The categorization of specific security incidents occurs at the time the security incident is discovered. The categorization of specific security incidents can change based on information developed during the inquiry into the incident.

c. IMI. The IMI number is used to identify, trend, and evaluate each security incident or combination of incidents. (Specific information to be used to categorize incidents of security concern is contained in Table 1 through Table 4; however, the IMI subcategories contained in these tables are not all inclusive and if they overlap, the more stringent reporting category will apply.) The basis for each IMI category is provided below.

(1) IMI-1. Actions, inactions, or events that pose the most serious threats to national security interests and/or critical DOE assets, create serious security situations, or could result in deaths in the workforce or general public. See Table 1, Reportable Categories of Incidents of Security Concern, Impact Measurement Index 1 (IMI-1).

(2) IMI-2. Actions, inactions, or events that pose threats to national security interests and/or critical DOE assets or that potentially create dangerous situations. See Table 2, Reportable Categories of Incidents of Security Concern, Impact Measurement Index 2 (IMI-2).

(3) IMI-3. Actions, inactions, or events that pose threats to DOE security interests or that potentially degrade the overall effectiveness of the Department's S&S protection program. See Table 3, Reportable Categories of Incidents of Security Concern, Impact Measurement Index 3 (IMI-3).

(4) IMI-4. Actions, inactions, or events that could pose threats to DOE by adversely impacting the ability of organizations to protect DOE S&S interests. See Table 4, Reportable Categories of Incidents of Security Concern, Impact Measurement Index 4 (IMI-4).

Table 1. Reportable Categories of Incidents of Security Concern, Impact Measurement Index 1 (IMI-1)

IMI-1 Actions, inactions, or events that pose the most serious threats to national security interests and/or critical DOE assets, create serious security situations, or could result in deaths in the workforce or general public.

Contract requirements relating to DOE O 151.1B, *Comprehensive Emergency Management System*, dated 10-29-03, and facility emergency management plans may require more stringent reporting times for IMI-1 type incidents than listed here. Shorter reporting times should be determined on an individual incident basis and applied accordingly and incorporated into the contract.

Incident Type	Report within 1 hour	Report within 8 hours	Report monthly
1. Confirmed or suspected loss, theft, or diversion of a nuclear device or components.	X		
2. Confirmed or suspected loss, theft, diversion, or unauthorized disclosure of weapon data.	X		
3. Confirmed or suspected loss, theft, or diversion of Category I or II quantities of special nuclear material (SNM).	X		
4. A shipper-receiver difference involving a loss in the number of items which total a Category I or II quantity of SNM.	X		
5. Confirmed or suspected loss, theft, diversion, unauthorized disclosure of Top Secret information, Special Access Program (SAP) information, or Sensitive Compartmented Information (SCI), regardless of the medium, method, or action resulting in the incident.	X		
6. Confirmed or suspected intrusions, hacking, or breakins into DOE computer systems containing TS information, SAP information, or SCI.	X		
7. Confirmed or suspected physical intrusion attempts or attacks against DOE facilities containing nuclear devices and/or materials, classified information, or other national security related assets.	X		
8. Confirmed or suspected attacks against DOE Federal and contractor employees that adversely impact a facility's or site's security posture.	X		
9. Confirmed or suspected acts or attempts of terrorist-type actions.	X		
10. Confirmed reports of DOE or DOE contractor employees making threats against Departmental facilities, employees, or the U.S. Government.	X		
11. Confirmed threats that immediately endanger personnel health or safety and may require immediate protective force/law enforcement intervention.	X		
12. Dangerous weapons and firearms-related incidents where an individual is killed, wounded, or an intentional discharge occurs.	X		
13. Confirmed or suspected acts of sabotage, at any DOE facility, that places the safety or security of personnel, facilities, or the public at risk.	X		
14. Confirmed compromise of root/administrator privileges in DOE unclassified computer systems that have a significant possibility of being contaminated with TS information, SAP information, or SCI.	X		
15. Confirmed compromise of root/administrator privileges in DOE computer systems containing Secret or Confidential information.	X		
16. Confirmed intrusions into information systems containing classified information.	X		
17. Instances of malicious code that cause disruption, degradation, or compromise of information systems for an entire site/facility.	X		
18. Instances of malicious code that allow unauthorized or undetected access to information systems containing classified information (Top Secret, Secret, Confidential, SAP information, or SCI).	X		

Table 2. Reportable Categories of Incidents of Security Concern, Impact Measurement Index 2 (IMI-2)

IMI-2 Actions, inactions, or events that pose threats to national security interests and/or critical DOE assets or that potentially create dangerous situations.

Incident Type	Report within 1 hour	Report within 8 hours	Report monthly
1. Suspected loss, theft, or diversion of any radioactive material not categorized as special nuclear materials (SNM), or dangerous materials that could pose a health threat or endanger security.		X	
2. Confirmed or suspected intrusions, hacking, or breakins into DOE computer systems containing Secret or Confidential classified information.		X	
3. Any amount of SNM found in an exceptionally dangerous/hazardous unapproved storage environment, or unapproved mode of transportation/transfer.		X	
4. Alarms or other loss detection indicators for security areas containing a Category I or II quantity of SNM that cannot be proven false within 24 hours.		X	
5. Inventory differences exceeding alarm limits in Category I and II SNM material balance areas, where there is no indication or reason to believe the difference is created by loss, theft or diversion.		X	
6. Confirmed or suspected unauthorized disclosure, loss, or potential loss of Secret matter regardless of the medium, method, or action resulting in the incident.		X	
7. Actual or suspected technical interceptions of any level of classified information.		X	
8. Actions, by electronic or physical means, that interfere with any DOE safeguards and security practices.		X	
9. Notifications, by any media or source, of validated threats that do not appear to immediately threaten personal safety or health.		X	
10. Loss of classified information that must be reported to other Government agencies or foreign organizations.		X	
11. Unsecured classified repositories of any type, including safes, doors, or other protective encasements, that contain Top Secret information, Special Access Program information, or Sensitive Compartmented Information.		X	
12. The loss of any DOE classified interest that requires State or local government or other Federal agency notification.		X	
13. Confirmed compromise of root/administrator privileges in DOE unclassified computer systems.		X	
14. Confirmed compromise of root/administrator privileges in DOE unclassified computer systems that have a significant possibility of being contaminated with Secret or Confidential information.		X	
15. Potential compromise of root/administrator privileges in DOE computer systems containing classified information.		X	
16. Instances of malicious code that cause disruption/degradation or compromise of information systems dedicated to safety, security, or critical operations.		X	
17. Detection of activities involving individuals who have been confirmed as physically watching/casing/surveilling a site in an effort to gather information to aid in the conduct of a terrorist-type attack.		X	

Table 3. Reportable Categories of Incidents of Security Concern, Impact Measurement Index 3 (IMI-3)

IMI-3 Actions, inactions, or events that pose threats to DOE security interests or that potentially degrade the overall effectiveness of the Department's safeguards and security protection program.			
Incident Type	Report within 1 hour	Report within 8 hours	Report monthly
1. A shipper-receiver difference or inventory difference involving a gain in the number of items for which the additional items total a Category I or II quantity of special nuclear material (SNM).		X	
2. Bomb-related incidents at any DOE facility, including location of a suspected device.		X	
3. Confirmed or suspected unauthorized disclosure, loss, or potential loss of Confidential matter by any medium, method, or action.		X	
4. Confirmed or alleged noncompliance with laws or DOE directives/standards that jeopardizes protection of the facility or site security interests.		X	
5. Demonstrators or protestors that cause site and facility damage.		X	
6. Labor strikes that could degrade or impede the required protection of the facility or site.		X	
7. Physical violence or threat of retaliation against facility security personnel.		X	
8. Dangerous weapons and firearms-related incidents involving protective force operations/personnel where an unauthorized weapon discharge occurs.		X	
9. Loss or theft of DOE firearms or ammunition, per DOE M 470.4-3, *Protective Force*.		X	
10. Unplanned/unscheduled power outages that cause a disruption/degradation of physical security systems and that would allow unauthorized or undetected entry to access controlled/protected areas.		X	
11. Incidents involving the attempted or actual introduction of controlled and prohibited items into Limited, Exclusion, Protected, or Material Access Areas, excluding unauthorized cellular phones or personal digital assistants where there is no potential for compromise of classified or unclassified controlled information.		X	
12. Confirmed or suspected malicious activities, including but not limited to stealing badges or vehicle licenses.		X	
13. Discovery of malicious activities, disorderly conduct, or vandalism that disrupts facility activities or causes damage between $10K and $100K.		X	
14. Circumvention of established access control procedures into a security area (excluding Property Protection Area).		X	
15. Inventory differences exceeding alarm limits in Category III SNM material balance areas or inventory differences greater than 50 g of Tritium, where there is no indication or reason to believe the difference is created by loss, theft, or diversion.		X	
16. A shipper-receiver difference involving a loss in the number of items which total a Category III or IV quantity of SNM.		X	
17. Confirmed or suspected loss, theft, or diversion of Category III or IV quantities of SNM.		X	
18. Intrusion attempts into information systems containing classified information.		X	
19. Confirmed intrusions into unclassified information systems that are not publicly available (e.g., behind a firewall).		X	

Table 3. continued

Incident Type	Report within 1 hour	Report within 8 hours	Report monthly
20. Confirmed instances of "denial of service" attacks on information systems that result in disruption of site/facility ability to access the Internet, disruption of site/facility information systems operations, or disruption of site/facility information system protection measures (e.g., firewall).		X	
21. Unauthorized network scans/probes on information systems possessing classified information.		X	
22. Incidents of apparent surveillance of facilities or operations (studying, photographing, low over-flights, outsiders questioning employees or protective force, unusual calls for information, etc.).		X	

Table 4. Reportable Categories of Incidents of Security Concern, Impact Measurement Index 4 (IMI-4)

IMI-4 Actions, inactions, or events that could pose threats to DOE by adversely impacting the ability of organizations to protect DOE safeguards and security interests.

Incident Type	Report within 1 hour	Report within 8 hours	Report monthly
1. Identified special nuclear materials (SNM) inventory differences beyond alarm limits in a Category IV SNM material balance area where there is no indication or reason to believe the difference is created by loss, theft, or diversion.			X
2. Significant shipper-receiver differences that exceed 200g of fissile material and the combined limit of error for the shipment.			X
3. Alarms or other loss detection indicators, excluding inventory differences and shipper-receiver differences, for a security area containing a Category III or IV quantity of SNM.			X
4. A shipper-receiver difference or inventory difference involving a gain in the number of items for which the additional items total to a Category III or IV quantity of SNM.			X
5. Confirmed or suspected unauthorized disclosure of Unclassified Controlled Nuclear Information, Export Control information, and unclassified Naval Nuclear Propulsion Information by any medium, method, or action.			X
6. Non-credible bomb threats at any DOE nuclear or non-nuclear facility.			X
7. Unsecured classified repositories of any type including safes, doors, or other protective encasements in which no likely classified disclosure occurred. If the repository contains Top Secret information, Special Access Program information, or Sensitive Compartmented Information, report under the IMI-1, IMI-2, or IMI-3 category, as appropriate.			X
8. Peaceful demonstrations or protests that do not threaten facility or site security interests or activities.			X
9. Failure to adhere to established procedures contributing to the misuse or misprocessing of or failure to maintain security badges and passes.			X
10. Loss of security badges in excess of 5 percent of total issued during 1 calendar year.			X
11. Failure to adhere to established procedures contributing to the mismanagement or faulty application of the DOE Human Reliability Program.			X
12. Failure to adhere to established administrative procedures contributing to problems with foreign visitors.			X
13. Classified information sent by e-mail that is contained within the firewall. All parties involved are cleared to the level of information transmitted, and the affected systems are identified, taken offline, and appropriately stored in approved areas pending sanitization. If more than 8 hours are required to isolate the affected systems, then such incidents will be handled as suspected compromises in accordance with their classification levels and categories.			X
14. Unauthorized cellular phones and personal electronic devices (e.g., PDAs) introduced into a Limited Area, Protected Area, or Material Access Area, where there is no potential for compromise of classified or unclassified controlled information.			X
15. Circumvent established access control procedures into a Property Protection Area.			X
16. High rate/amount of loss (excluding natural disasters) or theft of Government property.			X

3. REPORTING REQUIREMENTS.

a. 24-hour Determination/Categorization Period. When an incident is suspected to have occurred, the cognizant security authority at the site/facility where the incident occurred has 24 hours to examine and document all pertinent facts and circumstances to determine whether an incident has occurred (see Figure 1, Incidents of Security Concern). During this period, the suspected incident must be categorized by an IMI number. If it is determined that an incident of security concern did not occur, no further action is required.

b. Initial Incident Reporting. Incidents of security concern initial reports for IMI-1, IMI-2, and IMI-3 (as well as those for IMI-4 involving non-U.S. citizens, per paragraph 3d below) must be sent to the DOE Headquarters (HQ) Operations Center (OC) using DOE Form (F) 471.1, "Security Incident Notification Report," in accordance with locally developed procedures approved by line management. Initial security incident reports must be forwarded based on the following criteria.

(1) Within 1 hour following categorization for security incidents determined to be IMI-1 (see Table 1), the cognizant security authority at the originating site/facility must transmit a DOE F 471.1 to the DOE HQ OC. If a verbal notification of the incident is made to the DOE HQ OC, a follow-up transmission of the DOE F 471.1 to the DOE HQ OC must still be made.

(2) Within 8 hours following categorization of security incidents determined to be IMI-2/IMI-3 (see Tables 2 and 3), the cognizant security authority at the originating site/facility must transmit a DOE F 471.1 to the DOE HQ OC. If a verbal notification of the incident is made to the DOE HQ OC, a follow-up transmission of the DOE F 471.1 to the DOE HQ OC must still be made.

c. Reporting Incidents Receiving Media Attention. In addition to the IMI reporting time frames, the Office of Security must be notified within 8 hours of any security incidents that have been or will be reported in the media. The initial DOE F 471.1 and any subsequent updates must clearly identify the fact of media reporting.

d. Reporting Incidents Associated with Non-U.S. Citizens. Security incidents having any association with non-U.S. citizens must be clearly identified and reported on the initial DOE F 471.1 and subsequently in any related update or follow-on activity pertaining to the incident, including incidents categorized as IMI-4. For security incidents involving any credible information that a non-U.S. citizen or an agent of a foreign power is involved, the geographically closest element of the Office of Counterintelligence (OCI)/Office of Defense Nuclear Counterintelligence (ODNCI) must be notified.

e. Numbering Incidents and Changing Categories. When the initial notification incident report (i.e., DOE F 471.1) is transmitted, it must include a local incident tracking number. All subsequent reports pertaining to a security incident (e.g., inquiry and other related activities) must be transmitted to the Office of Security. Changes in IMI categorizations require resubmission of a DOE F 471.1 (or form similar in content) to the Office of Security.

f. Reporting Incidents Associated with Sensitive Programs. Only the initial DOE F 471.1 is required for incidents involving activities associated with sensitive programs. These programs include the sensitive compartmented information (SCI) Program, special access program (SAPs), the Technical Surveillance Countermeasures (TSCM) Program, the Counterintelligence (CI) Program, or other programs identified by the Office of Security. All subsequent reporting must be handled "within channels" until such time as the inquiry report has been distributed. The date of the inquiry report must be transmitted to the Office of Security for entry into the Incident Tracking Analysis Capability (ITAC) database.

g. Closing Inquiries.

(1) IMI-1 and IMI-2 incidents are considered closed upon completion of the inquiry report. The inquiry report must be completed within 60 working days of the incident categorization or a status report must be provided in accordance with paragraph 3j(1), below.

(2) IMI-3 incidents are considered closed upon completion of DOE F 5639.3, "Report of Security Incident/Infraction," (except for completing the section on assignment and acceptance of the security infractions), and transmission of the completed DOE F 5639.3 to the Office of Security. The completion of the section on assignment and acceptance of security infractions (Part II, DOE F 5639.3) must be completed as required in local procedures.

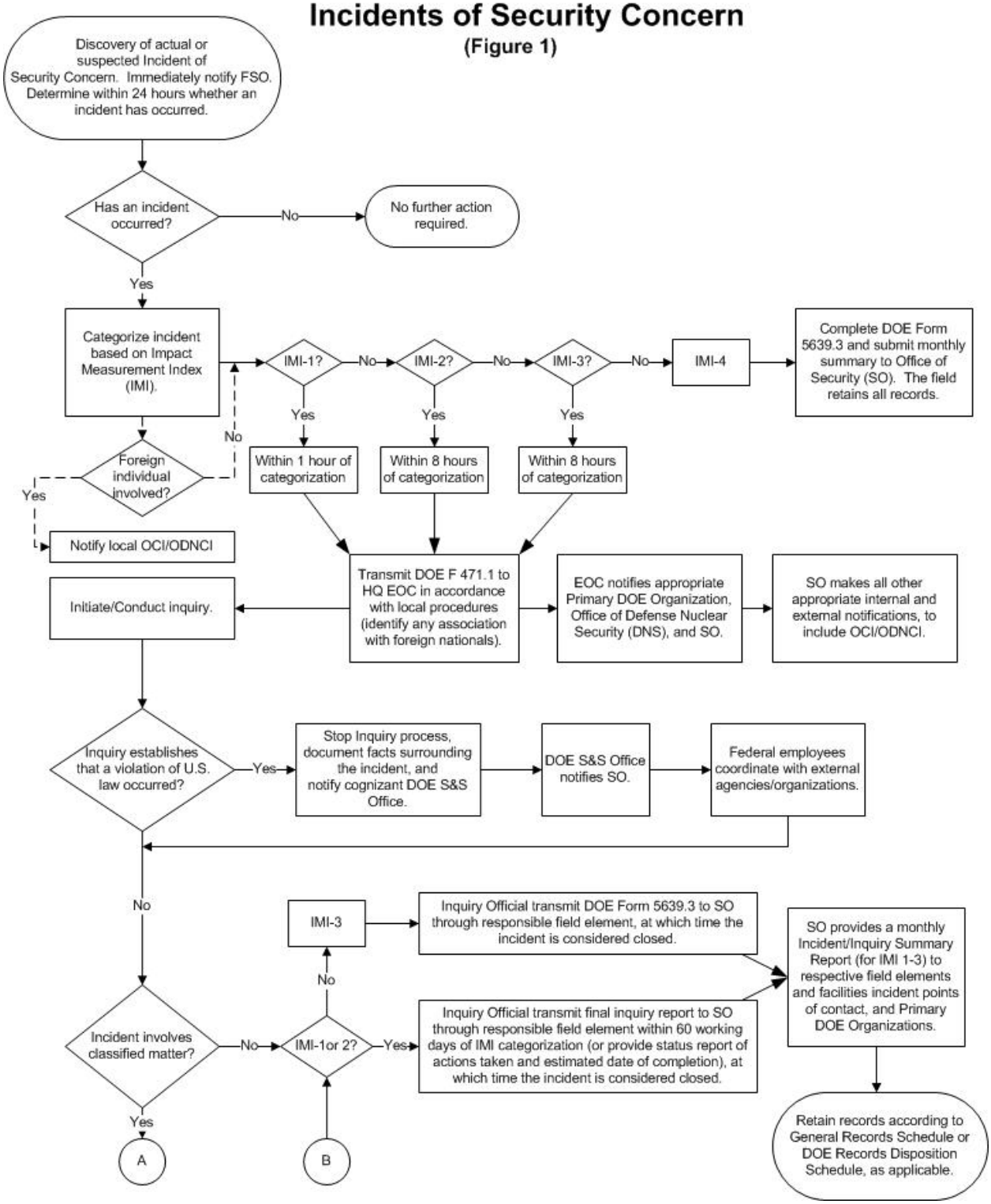
(3) IMI-4 incidents are considered closed upon completion of the DOE F 5639.3 in accordance with associated local procedures.

(4) A sanitized (unclassified) copy of the DOE F 5639.3 must be provided to the responsible personnel security office for placement in the appropriate personnel security file.

h. Final Inquiry Reports. Inquiry officials must forward final inquiry reports in accordance with local procedures to line management for action and to the Office of Security for all IMI-1s, IMI-2s, and IMI-3s.

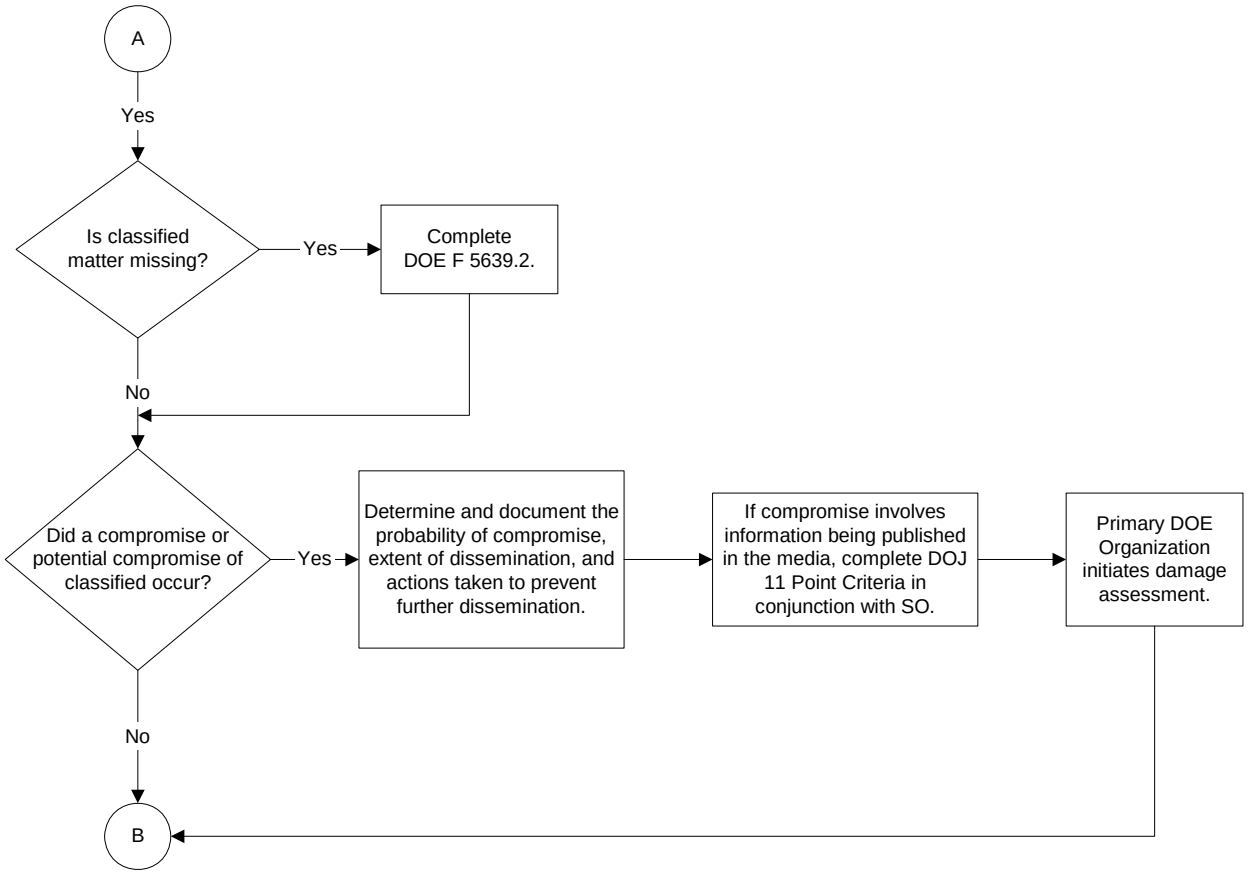
Incidents of Security Concern

(Figure 1)



Incidents of Security Concern

(Figure 1 continued)



i. Status/Summary Reports.

(1) IMI-1 and IMI-2. A monthly status report must be provided to the Office of Security and the Departmental element for IMI-1 and IMI-2 incidents that have not been closed within 60 working days of notification of the incident.

(a) Status reports must include as a minimum, the local tracking number (if applicable), date of incident categorization (not discovery), completed and planned actions, identification of issues precluding closure, and estimated date of closure. A copy of the original DOE F 471.1 (or form similar in content) may be included also.

(b) Status reports are due by the fifth working day of each month.

(2) IMI-3. Status reports are not required for IMI-3 incidents.

(3) IMI-4. The cognizant security authority at each facility must maintain a compilation of IMI-4 incidents by month. These monthly summaries, which must contain the number of open and closed security incidents by IMI-4 subtopic, the total initiated for the calendar month, and a running total of open and closed incidents for the calendar year, must be provided to the Office of Security. If no reportable incidents occurred during the calendar month, a summary stating "no reportable incidents" must be forwarded to the Office of Security by the fifth working day of each month.

j. Separate but Related Reporting.

(1) Occurrence Reporting Processing System. To eliminate reporting redundancy and centralize the reporting of security-related occurrences, all occurrences previously reported within the "Group 5—Safeguards and Security" category once contained in contractor requirements relating to canceled DOE M 231.1-2, *Occurrence Reporting and Processing of Operations Information,* dated 8-19-03, are incorporated into this section. Because an event meets the criteria for reporting as an incident of security concern does not negate the responsibility to report it as an occurrence under contractor requirements relating to DOE O 231.1A, chg 1, *Environment, Safety, and Health Reporting,* dated 6-3-04 (i.e., event affects both safety and security) incorporated into the contract.

(2) DOE O 151.1B, *Comprehensive Emergency Management System*, dated 10-29-03. Incidents that are reportable under the contract provisions of DOE O 151.1B incorporated into the contract and must continue to be reported in accordance with that Order and this section.

(3) Flash Reporting. National Nuclear Security Administration (NNSA) "Flash Reporting" procedures are not affected by the requirements in this section.

(4) Special Reporting Situations. Under certain circumstances, related incidents of security concern, that are anticipated to recur over a long period of time, may be consolidated into single monthly reports. This situation will be handled on a case-by-case basis between the cognizant security authority, the Departmental element, and the Office of Security. Specific plans for this reporting process must be developed by the cognizant security authority and submitted through the Departmental element to the Office of Security.

k. Documenting Corrective Actions. Corrective actions identified in response to an incident of security concern must be documented. For incidents categorized as IMI-1, IMI-2, or IMI-3, a copy of the documentation must be forwarded to the Office of Security if this information is not included in the inquiry report. Documentation on corrective actions for IMI-4 incidents does not have to be forwarded to the Office of Security.

4. INQUIRY OFFICIALS.

a. Inquiry officials must conduct inquiries to establish the pertinent facts and circumstances surrounding incidents of security concern.

b. Inquiry officials may be either Federal or contractor employees but must have previous investigative experience or Department inquiry training and must be knowledgeable of appropriate laws, executive orders, Departmental directives, and/or regulatory requirements.

(1) Contractors may conduct inquiries into incidents of security concern; however, if a violation of law is determined or suspected or the inquiry establishes information that a foreign power or an agent of a foreign power is involved, the contractor must stop further inquiry actions and notify the DOE cognizant security authority, which will assume further notification and reporting responsibilities, to include coordination with OCI/ODNCI. In such instances, the contractor must document the known circumstances surrounding the incident of security concern and submit all accumulated data to the DOE cognizant security authority.

(2) In all instances where the DOE cognizant security authority disagrees with the contractor report, the DOE cognizant security authority must assume supplemental inquiry responsibilities.

(3) When the inquiry into an incident of security concern necessitates communication with agencies/organizations external to the Department (e.g., the U.S. Postal Service, the FBI, or other Federal agencies), a Federal employee must be responsible for performing all such communication.

(4) Contact with Federal, State, and local law enforcement officials may be made by contractors with the written concurrence of the DOE cognizant security authority and DOE line management.

c. Inquiry officials are not authorized to detain individuals for interviews or obtain sworn statements; however, they may conduct consensual interviews and obtain signed statements.

d. Inquiry officials must be appointed in writing by the DOE line management, the head of the Office of Headquarters Security Operations, or the Office of Security.

e. Inquiry officials are responsible for conducting the inquiry and maintaining records and documentation associated with the inquiry (e.g., logs of events, notes, recordings, and statements).

f. When inquiry officials discover suspected or confirmed violations of law, they must immediately notify the Office of Security.

5. FEDERAL, STATE, OR LOCAL LAW ENFORCEMENT PERSONNEL.

a. If a violation of law has occurred and the preservation of evidence requires the immediate notification of Federal, State, or local law enforcement agencies (e.g., theft of SNM, homicide, assault, location or detonation of an explosive device), the DOE cognizant security authority must perform all necessary referrals and notifications, including notification to the Office of Security. The Office of Security will notify the HQ elements of all referrals to other Federal law enforcement agencies, including the FBI.

b. Federal, State, or local law enforcement agency personnel requiring access to limited areas or higher for investigative actions must be escorted, have a current access authorization passed to DOE, or possess an active DOE access authorization. Such personnel will be approved for access to classified information or matter only if they possess the appropriate access authorization, the matter directly pertains to the investigation, and appropriate programmatic approvals have been granted if such approvals are required. Access to restricted data (RD) and formerly restricted data (FRD) requires a DOE Q or L or appropriate personnel security clearance.

c. When authorized and approved Federal, State, or local law enforcement personnel are given access to classified information, they must be immediately advised of the classification level and category. They must also be informed of the protection and control requirements associated with the classified information they possess.

d. When an inquiry establishes information that a foreign power or an agent of a foreign power is involved, the Office of Security must immediately notify OCI/ODNCI, which in turn will notify the FBI in accordance with 50 U.S.C. 402a.

e. When an inquiry surrounding an incident of security concern establishes information indicating that fraud, waste, or abuse has occurred, the Office of the Inspector General must be notified for information and/or action.

f. The DOE cognizant security authority must make arrangements for the issuance of standard DOE security badges, the granting of access to classified information, and any other necessary agreements or items requested or required by Federal, State, or local law enforcement agencies involved in investigations.

6. CONDUCT OF INQUIRIES.

a. If an incident affects more than one site/facility, the following criteria must be used in determining the lead organization responsible for conducting the inquiry.

(1) If the sites/facilities fall under the purview of a single DOE cognizant security authority, that DOE cognizant security authority must assign responsibility to a lead organization.

(2) If the sites/facilities fall under the purview of multiple DOE cognizant security authorities, those DOE cognizant security authorities must, by mutual agreement, decide on a lead organization with responsibility for the inquiry.

b. The following actions must be taken when conducting inquiries into incidents of security concern and be reflected in the inquiry report (see Chapter II for additional requirements).

(1) Data Collection.

(a) Collect all data/information relevant to the incident, such as operations logs, inventory reports, requisitions, receipts, photographs, signed statements, etc.

(b) Conduct interviews to obtain additional information regarding the incident.

(c) Collect physical evidence associated with the inquiry, if available. (Examples of physical evidence include, but are not limited to, recorder charts, computer hard drives, defective/failed equipment, procedures, and readouts from monitoring equipment, etc.)

(d) Ensure physical evidence is protected and controlled and a chain-of-custody is maintained. (See Figure 2 for an example of a Chain-of-Custody Form.)

(2) Incident Reconstruction.

(a) Reconstruct the incident of security concern to the greatest extent possible using collected information and other evidence.

(b) Develop a chronological sequence of events that describes the actions preceding and following the incident.

(c) Identify persons associated with the incident.

(3) Incident Analysis and Evaluation. This analysis determines which systems/functions performed correctly or failed to perform as designed. It provides the basis for determining the cause of the incident and subsequent corrective actions. Inquiry officials must:

(a) analyze the information collected during the inquiry to determine whether it describes the incident completely and accurately;

(b) collect additional data and reconstruct the incident if more information is required;

(c) identify any collateral impact with other programs or security interests.

Figure 2. Example Chain-of-Custody Form

EVIDENCE/PROPERTY CUSTODY DOCUMENT **For use of this form see ISC-301 Conduct of Inquiries Course Manual.** **Proponent is the DOE Computer Forensics Laboratory.**	DOE TRACKING NUMBER: CFL CASE NUMBER

RECEIVING ACTIVITY	LOCATION	
NAME, GRADE AND TITLE OF PERSON FROM WHOM RECEIVED ☐ OWNER ☐ OTHER	ADDRESS *(Including Zip Code)*	
LOCATION FROM WHERE OBTAINED	REASON OBTAINED	DATE/TIME OBTAINED

ITEM NO.	QUANTITY	DESCRIPTION OF ARTICLES *(Include model, serial number, condition and unusual marks or scratches)*

CHAIN OF CUSTODY

ITEM NO.	DATE	RELEASED BY	RECEIVED BY	PURPOSE OF CHANGE OF CUSTODY
		SIGNATURE	SIGNATURE	
		NAME, GRADE OR TITLE	NAME, GRADE OR TITLE	
		SIGNATURE	SIGNATURE	
		NAME, GRADE OR TITLE	NAME, GRADE OR TITLE	
		SIGNATURE	SIGNATURE	
		NAME, GRADE OR TITLE	NAME, GRADE OR TITLE	
		SIGNATURE	SIGNATURE	
		NAME, GRADE OR TITLE	NAME, GRADE OR TITLE	
		SIGNATURE	SIGNATURE	
		NAME, GRADE OR TITLE	NAME, GRADE OR TITLE	

Figure 2. Example Chain-of-Custody (continued)

		CHAIN OF CUSTODY *(CONTINUED)*		
ITEM NO.	DATE	RELEASED BY	RECEIVED BY	PURPOSE OF CHANGE OF CUSTODY
		SIGNATURE	SIGNATURE	
		NAME, GRADE OR TITLE	NAME, GRADE OR TITLE	
		SIGNATURE	SIGNATURE	
		NAME, GRADE OR TITLE	NAME, GRADE OR TITLE	
		SIGNATURE	SIGNATURE	
		NAME, GRADE OR TITLE	NAME, GRADE OR TITLE	
		SIGNATURE	SIGNATURE	
		NAME, GRADE OR TITLE	NAME, GRADE OR TITLE	
		SIGNATURE	SIGNATURE	
		NAME, GRADE OR TITLE	NAME, GRADE OR TITLE	
		SIGNATURE	SIGNATURE	
		NAME, GRADE OR TITLE	NAME, GRADE OR TITLE	
		SIGNATURE	SIGNATURE	
		NAME, GRADE OR TITLE	NAME, GRADE OR TITLE	

FINAL DISPOSAL ACTION

RELEASE TO OWNER OR OTHER (Name/Organization) _____

DESTROY _____

OTHER (Specify)

FINAL DISPOSAL AUTHORITY

ITEM(S)_____ON THIS DOCUMENT, PERTAINING TO THE INQUIRY/INVESTIGATION INVOLVING:

_____(IS)(ARE) NO LONGER
(Grade) *(Name)* *(Organization)*

REQUIRED AS EVIDENCE AND MAY BE DISPOSED OF AS INDICATED ABOVE. *(If articles must be retained do not sign, but explain in separate correspondence.)*

_____
(Typed/Printed Name, Grade, Title) *(Signature)* *(Date)*

WITNESS TO DESTRUCTION OF EVIDENCE

THE ARTICLE(S) LISTED AT ITEM NUMBER(S)_____(WAS) (WERE) DESTROYED BY THE EVIDENCE CUSTODIAN IN MY PRESENCE, ON THE DATE INDICATED ABOVE.

_____
(Typed/Printed Name, Grade, Title, Organization) *(Signature)* *(Date)*

7. INQUIRY REPORT CONTENT/CLOSURE CONSIDERATIONS.[34] Inquiry reports must describe the conduct and results of the inquiry and include the following information for the incident to be closed.

a. An executive summary.

b. A narrative, which must include the following items.

(1) The date and time of incident discovery, any notifications, the incident inquiry, and other time-related actions pertaining to the incident (WHEN).

(2) All data pertinent to the location of an incident, including the facility name and facility code (as registered in SSIMS), building/room numbers, and other identifying information as appropriate. Such information is required for all facilities affected by the incident (WHERE).

(3) A complete discussion of the facts and circumstances surrounding the incident, including a description of all supporting information (WHAT), such as the following:

(a) detailed description of the incident of security concern;

(b) identification of all personnel involved in the incident and when they were notified, including those associated with the inquiry process (i.e., inquiry officials and assisting personnel);

(c) identification of the causes for the incident (direct and contributing factors) and descriptions of the mitigating or aggravating factors that may reduce or increase the impact of the incident;

(d) descriptions of the actions that precipitated the incident;

(e) descriptions of all physical evidence, including all records/documents reviewed (e.g., training records, policies/procedures);

(f) results of any interviews performed;

(g) descriptions of actions taken to minimize vulnerabilities created by the incident and prevent further loss/compromise of the security interest; and

[34] A fully completed Incident Tracking Analysis Capability report form may be used in lieu of a standard narrative report.

(h) if the incident involves classified information or matter, the following must also be included:

1 a description of the potentially compromised classified information or matter, including but not limited to classification level, category, caveats (if any), and form of information (e.g., document title, date, and description). A copy of the evidence (or photograph) must be retained and provided to the Office of Security if requested;

2 the classification guide and topic or source document, including date, of guide or source document;

3 known recipients of potentially compromised matter; and

4 owner of the classified information or matter (e.g., program office or OGA).

(4) An inquiry official's conclusion and the basis/facts that support the conclusion are essential.

(a) Given the facts determined through the inquiry, the conclusion of the final report must address the potential risk to the security interest based upon a subjective analysis of the facts and circumstances surrounding the incident of security concern.

(b) The final report must also identify the line management responsible for corrective actions and disciplinary actions.

c. The following must be included as attachments to the report of inquiry:

(1) a copy of the documentation appointing the inquiry official;

(2) a copy of any signed statements of involved individuals;

(3) a description of the compromised or potentially compromised information (as appropriate);

(4) a copy of the DOE F 471.1 and other documents obtained during the data collection phase of the inquiry;

(5) a copy of any DOE F 5639.3, or a form comparable in content, issued as a result of the inquiry; and

(6) a copy of any DOE F 5639.2, "Reporting Unaccounted for Documents," or a form comparable in content, if applicable.

8. ADMINISTRATIVE ACTIONS.

a. Whenever possible, the responsibility for an incident of security concern must be assigned to an individual rather than to a position or office.

(1) When individual responsibility cannot be established and the facts show that a responsible official allowed conditions to exist that led to an incident of security concern, responsibility must be assigned to that official.

(2) Security infractions are issued to document the assignment of responsibility for an incident of security concern. Individuals who do not possess an access authorization may be issued a security infraction.

b. Corrective actions taken in response to incidents of security concern must be documented, and for incidents categorized as IMI-1, IMI-2, or IMI-3, a copy of the documentation must be forwarded to the Office of Security. Documentation on corrective actions for IMI-4 incidents does not have to be forwarded to the Office of Security.

c. A copy of Part 1 of DOE F 5639.3 or similar form must be placed in the employee's DOE personnel security file. If an employee does not have an access authorization, it must be placed in his/her personnel file.

9. RECORDS RETENTION.

a. Records pertaining to incidents of security concern must not be sent to Federal Records Centers.

b. Records must be dispositioned in accordance with an applicable general records schedule (GRS), published by the National Archives and Record Administration (NARA), or in accordance with a DOE Records Disposition Schedule approved by NARA, whichever is applicable.

c. The site records manager or similarly titled person should be routinely consulted regarding the maintenance and disposition of records.

CHAPTER II. INCIDENTS OF SECURITY CONCERN INVOLVING COMPROMISE OR POTENTIAL COMPROMISE OF CLASSIFIED INFORMATION

1. INQUIRIES INTO COMPROMISE OF, POTENTIAL COMPROMISE OF, OR MISSING CLASSIFIED INFORMATION. The following requirements are in addition to those contained in Chapter I of this section. Inquiry officials must perform the following actions.

   a. Interview custodians and others having knowledge of the incident. When necessary, records must be audited for evidence of destruction, transmission, or other disposition.

   b. Ensure a DOE F 5639.2, "Reporting Unaccounted for Documents," or a form comparable in content, is completed if classified information or matter is missing.

   c. Determine which Departmental element has programmatic responsibility for the information or whether the information was originated by another Government agency or foreign government.

   d. Determine whether a compromise or potential compromise occurred. If there was a potential compromise, seek to determine the probability of compromise. Document the basis for such findings (i.e., potential compromise is defined as an incident of security concern where circumstances exist that cannot rule out the compromise of classified information).

   e. If an inquiry determines that a compromise or potential compromise has occurred, document the extent of the dissemination of the classified information and the actions taken to prevent further dissemination.

   f. When an inquiry establishes that classified information has been compromised by being published in the media, the questions contained in the Department of Justice (DOJ) Eleven-Point Criteria, which are listed below, must be answered and coordinated with the Office of Security. When completing the questions, provide all documentation and appropriate information to support affirmative responses. Each question must be answered affirmatively before the DOJ will initiate a formal investigation into the compromise; however, failure to affirmatively answer all the DOJ criteria does not preclude the DOJ from pursuing administrative or criminal action.

      (1) Could the date and identity of the article or articles disclosing the classified information be provided?

      (2) Could specific statements in the article that are considered classified be identified? Was the data properly classified?

(3) Is the classified data that was disclosed accurate? If so, provide the name of the person competent to testify concerning the accuracy.

(4) Did the data come from a specific document, and, if so, what is the origin of the document and the name of the individual(s) responsible for the security of the classified data disclosed?

(5) Could the extent and official dissemination of the data be determined?

(6) Has it been determined that the data has not been officially released in the past?

(7) Has it been determined that prior clearance for publication or release of the information was not granted by proper authorities?

(8) Does review reveal that educated speculation on the matter cannot be made from material, background data, or portions thereof which have been published officially or have previously appeared in the press?

(9) Could the data be made available for the purpose of prosecution? If so, include the name of the person competent to testify concerning the classification.

(10) Has it been determined that declassification had not been accomplished prior to the publication or release of the data?

(11) Will disclosure of the classified data have an adverse impact on the national defense?

2. DAMAGE ASSESSMENTS. Damage assessments determine potential damage to national security when classified information has been compromised or potentially compromised. Damage assessments are performed to evaluate and document possible countermeasures and conduct actions to limit potential damage. Additionally, damage assessments are used by appropriate authorities when criminal prosecution is sought. Classification guidance must be evaluated and updated, as appropriate, based on damage assessments. Damage assessments must be conducted when:

a. inquiries disclose evidence that classified information, including Weapon Data (Sigmas 1, 2, 14, and 15), SCI, or SAP data have been compromised or potentially compromised;

b. analysis reveals similar information has been compromised frequently or when the information has been compromised to a wide audience (e.g., public media, international conference, Internet);

c. a violation of laws appears to have occurred and criminal prosecution is contemplated; or

d. the Departmental element determines one is necessary.

3. CONDUCT OF DAMAGE ASSESSMENTS. Damage assessments are conducted by the Departmental element with programmatic responsibility for the compromised or potentially compromised classified information.

The originator of the compromised information must provide the DOE cognizant security authority with a copy of the compromised or potentially compromised information, if available. If no other copy exists, the originator must provide a detailed description of the compromised information.

The originator must coordinate with a derivative classifier to confirm the classification level and category of the compromised information according to current classification guidance and policy. The derivative classifier provides the basis from the classification determination (i.e., classification guide used).

4. COMBINING SIMILAR INCIDENTS. Damage assessments may be completed for a group of similar incidents when such grouping is a logical method of meeting this requirement. A logical grouping includes a situation where multiple matters requiring a damage assessment are related to a programmatic area and would result in the same or similar damage to national security or advantage to foreign governments and/or hostile organizations.

5. CASES INVOLVING OTHER GOVERNMENT AGENCY INFORMATION. Whenever a compromise or potential compromise involves the classified information of another Government agency (OGA), the contractor cognizant security authority through the DOE cognizant security authority responsible for the inquiry must provide the facts and circumstances that affect the OGA's information or interests to the Director, Office of Security.

6. CASES INVOLVING FOREIGN GOVERNMENT INFORMATION. Whenever a compromise or potential compromise involves the information of a foreign government that requires protection [e.g., Confidential Foreign Government Information Modified Handling (C/FGI-Mod)], the contractor cognizant security authority through the DOE cognizant security authority responsible for the inquiry must provide the facts and circumstances that affect the foreign government's information or interests to the Director, Office of Security. The foreign government, however, will not normally be advised of any Departmental security system vulnerabilities that allowed or contributed to the compromise or potential compromise.

SECTION O—RESTRICTIONS ON THE TRANSFER OF SECURITY-FUNDED TECHNOLOGIES OUTSIDE THE DEPARTMENT AND ITS OPERATIONAL FACILITIES

1. OBJECTIVE. To establish Technology Development Program (TDP) procedures and criteria for disseminating classified and/or unclassified controlled Office of Security and Safety Performance Assurance (SSA)-funded technology, other TDP-related information, and/or protection practices/expertise to any recipients who are not Department of Energy (DOE) Federal or contractor employees.

2. REQUIREMENTS.

   a. General. In all cases, the dissemination in any form of SSA-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) verification that the intended recipient has a strict need-to–know; a security clearance, and 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 set forth in this CRD and Export Control Laws and Regulations.

   b. Types of Technology/Information. The types of technology, information, and protection practices/expertise that are subject to the requirements include S&S technology development programs.

   c. Risk Assessment.

      (1) A risk assessment of the unauthorized use/transfer of classified technology, information, or practices must be conducted before release of the technology/information and used as the basis for approving or denying proposed transfers.

      (2) The risk assessment must be used to determine whether an applicant is eligible to receive a specific type of information/technology.

(3) Proposed release must be handled on a case-by-case basis because eligibility criteria are determined by both the type of information/ technology and the intended recipient. Additionally, the risk assessment must address the following factors.

(a) No person is entitled solely by virtue of rank, position, or access authorization (security clearance) to have access to classified or unclassified controlled SSA-funded technology, information, or protection practices/expertise.

(b) Relevance of the subject information to the protection of Departmental facilities and assets.

(c) Ability of the intended recipient to protect the information/technology in a manner equivalent to minimum security standards required by the Department.

d. Review and Approval Process. Coordination and approval must include the Departmental element and the Director, Office of Security.

e. Centralized Reporting. Written reports of each approval or denial of a request for technology subject to the requirements of this section must be sent to the Office of Security within 30 days of the decision.

f. Documentation.[35] The records listed below must be completed to document each receipt of a request for transfer of technology subject to the requirements of this chapter and to document the Department's transfer decision.

(1) Technology Transfer Approval Requests. The information in Appendix 9, Technology Transfer Approval Requests, must be included in all technology transfer approval requests.

(2) Basis for Approving or Denying a Transfer. A record of the concurrences, nonconcurrences, reviewer comments, executed Nondisclosure Agreement (if applicable), risk assessment (see paragraph 2c above), and approval or denial of the transfer must be created and maintained.

g. Records Retention. Each element requesting, reviewing, approving, and/or denying technology transfer requests must maintain a documented audit trail of requests initiated or handled by that office. Records, including the documentation cited in paragraph 2f above, must be retained for a minimum of 5 years.

[35] A nondisclosure agreement form will be provided upon request.

Vertical line denotes change.

SECTION O
APPENDIX 9—TECHNOLOGY TRANSFER APPROVAL REQUESTS

1. Name of Individual Requesting the Transfer:						**Date:**__/__/
2. Proposed Technology for Transfer:						
3. Proposed Recipient and Address:						
4. Type of Technology or Information:						
DOE Proprietary Protection Capability	Vulnerability Fix Information	Vulnerability Information	Best-In-Class Protection Capability & Technical Advances	Risk Analysis & System Modeling Information	Performance Information	Fundamental Protection Capability
5. Method of Transferring the Technology or Information:						
Briefing	Written Report	Design Documents	Source Code	License	Course	Hardware
6. Type of Recipient:						
Domestic	DOE Employee or Contractor	Federal Employee	Domestic Users & Academia	Manufacturer	Other (specify) _____	Public Fora
Foreign	Foreign Government Official	Non-Government User	Foreign Manufacturer	Other (specify) _____	Export License Required? Yes/No Basis for determination__ _____	
7. Level of Classification or Control	Unclassified	OUO	UCNI*	Confidential*	Secret*	Top Secret*
8. Type of Agreement Proposed:		Written Instructions	License	Nondisclosure	Sales Limitation	None
9. Estimated U.S. Taxpayer Investment to Develop this Technology: $ _____						
10. Has This Technology Been Previously Transferred to this Recipient? YES ☐ NO ☐						

*Also requires a documented need to know**.**
Abbreviations: OUO=Official Use Only; UCNI=Unclassified Controlled Nuclear Information.

Vertical line denotes change.

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

PAGE CHANGE

DOE M 470.4-1 Chg 1

Approved: 8-26-05
Chg 1: 3-7-06

SUBJECT: SAFEGUARDS AND SECURITY PROGRAM PLANNING AND MANAGEMENT

1. PURPOSE. To transmit revised pages to DOE M 470.4-1, *Safeguards and Security Program Planning and Management*, dated 3-7-06.

2. EXPLANATION OF CHANGES. To establish the new requirements necessary to support raising the Department's protective forces to the elite level as first outlined by Secretary Abraham in May of 2004.

3. LOCATION OF CHANGES.

Pages	Paragraphs
1	Change 1
iv	e.
vii	Appendix 2
x	Appendix 3, 4, & 5
xii	Appendix 5
xiv	Appendix 7
xv	Appendix 8
xvi	Appendix 9
A-1	2.a.
A-2	(3)(b) & (3)(c)
A-3	f.(2)
2-1 – 2-10	Appendix 2, Part 1, Section A
C-9	d.(1)
C-10	e.(1) & (2)
C-14	j.

E-1	2.d.
E-2	(2)
E-4	7.
3-1	Appendix 3, Part 1, Section E, Title
4-1	Appendix 4, Part 1, Section E, Title
5-1	Appendix 5, Part 1, Section E, Title
F-1	2.b.
II-2	Part 2, Section H, Chapter II, c.
6-1 – 6-3	Part 2, Section H, Appendix 6, Title
J-1	Part 2, Section J, 2.
L-5	Part 2, Section L, (4)
7-1	Part 2, Section L, Appendix 7, Title
M-1	Part 2, Section M, 2.a.
M-7	Part 2, Section M, b.(1)
8-1	Appendix 8, Title
O-2	e.
9-1	Appendix 9, Title
Page 1	Attachment 1
A-1	Attachment 2, 2.a.
A-2	(3)(b)&(c)
A-4	(2)
2-1 – 2-10	Section A, Appendix 2
C-8	d. (1)
C-11	e. (1) & (2)
C-15	j.

E-1	d.
E-2	(2)
E-4	7.
3-1	Section E, Appendix 3, Title
4-1	Section E, Appendix 4, Title
5-1	Section E, Appendix 5, Title
F-1	b.
F-2	(5)
H-3	c.
6-1	Section H, Appendix 6, Title
J-1	2.a. & d.
L-5	(4)
7-1	Section L, Appendix 7, Title
M-6	b.(1)
8-1	Section M, Appendix 8, Title
O-2	(1)
9-1	Section O, Appendix 9, Title

After filing the attached pages, this transmittal may be discarded.

CLAY SELL
Deputy Secretary