TS

NOT MEASUREMENT SENSITIVE

DOE–STD–1171–2009
May 2009

DOE STANDARD

SAFEGUARDS AND SECURITY FUNCTIONAL AREA QUALIFICATION STANDARD

DOE Defense Nuclear Facilities Technical Personnel

U.S. Department of Energy
Washington, D.C. 20585

AREA TRNG

DISTRIBUTION STATEMENT A. Approved for public release; distribution is unlimited.

This document is available on the

Department of Energy

Technical Standards Program

Web Site at

http://www.hss.energy.gov/nuclearsafety/techstds/

APPROVAL

The Federal Technical Capability Panel consists of senior U.S. Department of Energy (DOE) managers responsible for overseeing the Federal Technical Capability Program. This Panel is responsible for reviewing and approving the qualification standard for Department-wide application. Approval of this qualification standard by the Federal Technical Capability Panel is indicated by signature below.

_____
Karen L. Boardman, Chairperson
Federal Technical Capability Panel

INTENTIONALLY BLANK

TABLE OF CONTENTS

ACKNOWLEDGMENT vii

PURPOSE 1

APPLICABILITY 1

IMPLEMENTATION 2

EVALUATION REQUIREMENTS 3

INITIAL QUALIFICATION AND TRAINING 4

DUTIES AND RESPONSIBILITIES 5

BACKGROUND AND EXPERIENCE 5

REQUIRED TECHNICAL COMPETENCIES 5

A. Safeguards and Security Program Planning and Management (PP&M) 6
B. Physical Security (PS) 15
C. Protective Force Operations (PFO) 20
D. Information Protection (IP) 23
E. Personnel Security (PERS SEC) 28
F. Nuclear Material Control and Accountability (MC&A) 31
G. Cyber Security (CS) 35

APPENDIX A 41

INTENTIONALLY BLANK

ACKNOWLEDGMENT

The Office of Defense Nuclear Security is the sponsor for the Safeguards and Security Functional Qualification Standard (FAQS). The sponsor is responsible for coordinating the development and/or review of the FAQS by subject matter experts to ensure that the technical content of the standard is accurate and adequate for Department-wide application for those involved in the Safeguards and Security program. The sponsor, in coordination with the Federal Technical Capability Panel (FTCP), is also responsible for ensuring that the FAQS is maintained current.

The following subject matter experts participated in the development and/or review of this qualification standard:

McNeilly, Debra K.	NA-70 (Team Leader) (Writer)
Anderson, Thomas	EM-3.1
Cowden, Jack	HS-71
Crossland, Ernie	Raytheon
Faiver, Richard	HS-71
Gallion, Mary	HS-71
Hautala, Laurel	Kansas City Site Office
Holmer, Debarah	HS-71
Hitson, Mary Helen	Y-12 Site Office (Writer)
Jones, Wayne	NA-1 (Writer)
Khanna, Sabeens	HS-71
Kellogg, Del	Pantex Site Office
Kleinrock, Michael	CTAC (Writer)
Kubasek, Randy	Sandia Site Office
Lehman, Winifred	NNSA Service Center
Loftis, Jo	Sandia Site Office
Morgan, William	Pantex Site Office
Moran, Kieran	Livermore Site Office (Writer)
Mozzer, Laura	NE-ID
Piechowski, Carl,	HS-71
Royal, Paul	CTAC (Writer)
Ruhnow, Linda	NS-71
Sager, Eric	NNSA Service Center (Writer)
Showers, Russell	HS-51/NTC
Todd, Jon	NNSA Service Center

INTENTIONALLY BLANK

DOE-STD-1171-2009

U.S. DEPARTMENT OF ENERGY
FUNCTIONAL AREA QUALIFICATION STANDARD

Safeguards and Security

PURPOSE

DOE M 426.1-1A, *Federal Technical Capability Manual*, commits the Department to continuously strive for technical excellence. The Technical Qualification Program (TQP), along with the supporting technical qualification standards, complements the personnel processes that support the Department's drive for technical excellence. In support of this goal, the competency requirements defined in the technical qualification standards should be aligned with and integrated into the recruitment and staffing processes for technical positions. The technical qualification standards should form the primary basis for developing vacancy announcements, qualification requirements, crediting plans, interview questions, and other criteria associated with the recruitment, selection, and internal placement of technical personnel. The U.S. Office of Personnel Management (OPM) minimum qualifications standards will be greatly enhanced by application of appropriate materials from the technical FAQS.

The technical qualification standards are not intended to replace the OPM qualifications standards or other Departmental personnel standards, rules, plans, or processes. The primary purpose of the TQP is to ensure that employees have the requisite technical competency to support the mission of the Department. The TQP forms the basis for the development and assignment of DOE personnel responsible for ensuring the secure and safe operation of defense nuclear facilities.

APPLICABILITY

The Safeguards and Security FAQS establishes common functional area competency requirements for all DOE safeguards and security personnel who provide assistance, direction, guidance, oversight, or evaluation of contractor technical activities that could impact the safeguards and security operations of DOE's defense nuclear facilities. The technical FAQS has been developed as a tool to assist DOE program and field offices in the development and implementation of the TQP in their organization. For ease of transportability of qualifications between DOE elements, program and field offices are expected to use this technical FAQS without modification. Needed additional office-/site-/facility-specific technical competencies should be handled separately. Satisfactory and documented attainment of the competency requirements contained in this technical FAQS (see the Federal Technical Capability Program [FTCP] Directives and Standards page at http://www.hss.energy.gov/deprep/ftcp/directives/directives.asp for an example of the Safeguards and Security FAQS qualification card) ensures that personnel possess the minimum requisite competence to fulfill their functional area duties and responsibilities common to the DOE complex. Additionally, office-/site-/facility-specific qualification standards supplement this technical FAQS and establish unique operational competency requirements at the Headquarters or field element, site, or facility level.

It should be noted that the competencies of management and leadership, general technical knowledge, regulations, administrative capability, and assessment and oversight are all

embodied in the competencies listed in this standard. All of these factors have a bearing on safeguards and security. Although the focus of this standard is technical competence, competencies such as good communication, recognized credibility, ability to listen and process information, and the ability to guide an effort to get it right the first time are recognized as important aspects of safeguards and security.

IMPLEMENTATION

This FAQS identifies the minimum technical competency requirements for DOE personnel. Although there are other competency requirements associated with the positions held by DOE personnel, this FAQS is limited to identifying the specific, common technical safeguards and security competencies required throughout DOE. The competency requirements define the expected knowledge and/or skill that an individual must meet. Each of the competency requirements is further described by a listing of supporting knowledge and/or skill statements. The supporting knowledge and/or skill statements for each competency requirement are provided to challenge the employee in the breath and depth of his/her understanding of the subject matter. In selected competencies, expected knowledge and/or skills have been designated as "mandatory performance activities." In these competencies, the actions are not optional.

The term "must" denotes mandatory requirements, "should" denotes a recommended practice that is not required, and "may" denotes an option in this standard.

The competencies identify a familiarity level, a working level, or an expert level of knowledge; or they require the individual to demonstrate the ability to perform a task or activity. These levels are defined as follows:

> **Familiarity level** is defined as basic knowledge of or exposure to the subject or process adequate to discuss the subject or process with individuals of greater knowledge.
>
> **Working level** is defined as the knowledge required to monitor and assess operations/activities, to apply standards of acceptable performance, and to recognize the need to seek and obtain appropriate expert advice (e.g., technical, legal, security, safety) or consult appropriate reference materials required to ensure the safety and security of DOE activities.
>
> **Expert level** is defined as a comprehensive, intensive knowledge of the subject or process sufficient to provide advice in the absence of procedural guidance.
>
> **Demonstrate the ability** is defined as the actual performance of a task or activity in accordance with policy, procedures, guidelines, and/or accepted industry or DOE practices.

Headquarters and field elements must establish a program and process to ensure that DOE personnel possess the competencies required by their position, including the competencies identified in this technical FAQS. Documentation of the completion of the requirements of this standard must be included in the employees' training and qualification records. Satisfactory attainment of the competency requirements contained in this technical FAQS may be documented using the example Safeguards and Security FAQS qualification card that can be

obtained from the Federal Technical Capability Program Directives and Standards page at http://www.hss.energy.gov/deprep/ftcp/directives/directives.asp.

Equivalencies should be used sparingly and with the utmost rigor and scrutiny to maintain the spirit and intent of the TQP. Equivalencies may be granted for individual competencies based on objective evidence of previous education, training, certification, or experience. Objective evidence includes a combination of transcripts, certifications, and in some cases, a knowledge sampling obtained through written and/or oral examinations. Equivalencies must be granted in accordance with the TQP plan of the site/office/Headquarters organization qualifying the individual. The supporting knowledge and/or skill statements and mandatory performance activities should be considered before granting an equivalency for a competency.

Training must be provided to employees in the TQP who do not meet the competencies contained in this technical FAQS. Training may include, but is not limited to, formal classroom and computer-based courses, self-study, mentoring, on-the-job training, and special assignments. Departmental training must be based on appropriate supporting knowledge and/or skill statements similar to the ones listed for each of the competency requirements. Headquarters and field elements should use the supporting knowledge and/or skill statements as a basis for evaluating the content of any training used to provide individuals with the requisite knowledge and/or skill required to meet the technical FAQS competency requirements.

EVALUATION REQUIREMENTS

Attainment of the competencies listed in this technical FAQS must be documented in accordance with the TQP plan or policy of the site/office/Headquarters organization qualifying the individual and the requirements in DOE M 360.1-1B, *Federal Employee Training Manual*, and DOE M 426.1-1A, *Federal Technical Capabilities Manual*.

The qualifying official or immediate supervisor should ensure that the candidate meets the background and experience requirements of this FAQS. Unless stated otherwise within the program or site TQP plan, attainment of the competencies listed in the Safeguards and Security FAQS should be evaluated and documented by either a qualifying official or immediate supervisor (note: If the immediate supervisor is not a Safeguards and Security qualifying official, it is expected the supervisor consult with a qualified Safeguards and Security qualifying official to assist in qualifying a safeguards and security TQP candidate.) using one or a combination of the following methods:

- Satisfactory completion of a written examination
- Satisfactory completion of an oral examination
- Satisfactory accomplishment of an observed task or activity directly related to a competency
- Documented evaluation of equivalencies (such as applicable experience in the field) without a written examination.

Field element managers/Headquarters program managers shall qualify candidates as possessing the basic technical knowledge, technical discipline competency, and position-specific knowledge, skills, and abilities required for their positions. Final qualification should be performed using one or a combination of the following methods:

- Satisfactory completion of a comprehensive written examination. The minimum passing grade should be 80 percent.
- Satisfactory completion of an oral examination by a qualified Senior Technical Safety Manager (STSM) or a qualification board of technically qualified personnel that includes at least one qualified STSM.
- Satisfactory completion of a walkthrough of a facility with a qualifying official for the purpose of verifying a candidate's knowledge and practical skills of selected key elements.

Guidance for oral interviews and written exams is contained in DOE-HDBK-1205-97, *Guide to Good Practices for the Design, Development, and Implementation of Examinations*, and DOE-HDBK-1080-97, *Guide to Good Practices for Oral Examinations*.

For oral examinations and walkthroughs, qualifying officials or board members should ask critical questions intended to integrate identified learning objectives during qualification. Field element managers/Headquarters program managers or designees should develop formal guidance for oral examinations and walkthroughs that includes:

- Standards for qualification
- Use of technical advisors by a board
- Questioning procedures or protocol
- Pass/fail criteria
- Board deliberations and voting authorization procedures
- Documentation process

INITIAL QUALIFICATION AND TRAINING

Qualification of safeguards and security personnel must be conducted in accordance with the requirements of DOE M 426.1-1A. Safeguards and security personnel must complete the qualification process 18 months after being enrolled in the TQP.

DOE personnel should participate in continuing education and training as necessary to improve their performance and proficiency and ensure that they stay up-to-date on changing technology and new requirements. This may include courses and/or training provided by:

- DOE
- Other government agencies
- Outside vendors
- Educational institutions

Beyond formal classroom or computer-based courses, continuing training may include:

- Self-study
- Attendance at symposia, seminars, exhibitions
- Special assignments
- On-the-job experience

A description of suggested learning activities and the requirements for the continuing education and training program for the Safeguards and Security FAQS are included in Appendix A of this document.

DUTIES AND RESPONSIBILITIES

The following are the typical duties and responsibilities expected of personnel assigned to the Safeguards and Security Functional Area:

A. Program Planning and Management (PP&M)

B. Physical Security (PS)

C. Protective Force Operations (PFO)

D. Information Protection (IP)

E. Personnel Security (PERS SEC)

F. Nuclear Materials Control and Accountability (MC&A)

G. Cyber Security (CS)

Position-specific duties and responsibilities for safeguards and security personnel are contained in their office-/site-/facility-specific qualification standard and/or position description.

BACKGROUND AND EXPERIENCE

The OPM *Qualification Standards Operating Manual* establishes minimum education, training, experience, or other relevant requirements applicable to a particular occupational series/grade level, as well as alternatives to meeting specified requirements.

The preferred education and experience for safeguards and security personnel are:

1. Education:

   Security Specialists are required to meet OPM standards for Occupational Series 0080.

2. Experience:

   Industrial, military, Federal, State, or other directly-related background that has provided specialized experience in safeguards and security. Specialized experience can be demonstrated through possession of the competencies outlined in this standard.

REQUIRED TECHNICAL COMPETENCIES

All safeguards and security personnel must satisfy the competency requirements of the Safeguards and Security General Technical Base Qualification Standard prior to or in parallel with the competency requirements contained in Sections A. through G. of this standard, as

appropriate and as determined by the supervisor (or designated individual). Each of the competency requirements defines the level of expected knowledge and/or skill that an individual must possess to meet the intent of the standard. Each of the competency requirements is further described by a listing of supporting knowledge and/or skill statements that describe the intent of the competency statements. In selected competencies, expected knowledge and/or skills have been designated as "mandatory performance activities." In these competencies, the actions are not optional.

Note: When regulations, DOE directives, or other industry standards are referenced in the FAQS, the most recent revision should be used. It is recognized that some safeguards and security personnel may oversee facilities that utilize predecessor documents to those identified. In those cases, such documents should be included in local qualification standards via the TQP.

Due to the specialized nature of the Safeguards and Security Functional Area, safeguards and security personnel must complete the competency statements at the **working level** in the following sections (Sections A through G) as determined by the supervisor (or designated individual) consistent with the assigned safeguards and security responsibilities. Additionally, safeguards and security personnel may be required to complete competencies in other safeguards and security functional areas at a level of proficiency as determined by the supervisor (or designated individual).

The following table depicts the certification requirements for Safeguards and Security personnel under the TQP.

	Familiarity	Working	Expert
Safeguards & Security GTB	✓		
Specialty Area(s) (Sections A –G)		✓	
Other, at discretion of supervisor (or designated individual)		✓ **or**	✓

A. SAFEGUARDS AND SECURITY PROGRAM PLANNING AND MANAGEMENT (PP&M)

Competencies and supporting knowledge and skills for Section A, Safeguards and Security Program Planning and Management, are derived from the following DOE Orders, Manuals, and Guides:

- DOE O 142.3 Chg 1, *Unclassified Foreign Visits and Assignment Program*
- DOE O 470.4A, *Safeguards and Security Program*
- DOE M 470.4-1 Chg 1, *Safeguards and Security Program Planning and Management*
- DOE G 226.1-1, *Safeguards and Security Oversight and Assessments Implementation Guide*
- DOE P 470.1, *Integrated Safeguards and Security Management (ISSM) Policy*
- Homeland Security Presidential Directive-3, (HSPD-3), dated 3-11-02
- Presidential Decision Directive 39, *U.S. Policy on Counterterrorism* (U), dated 6-21-95

1. Safeguards and security personnel with the responsibility for PP&M must demonstrate a working level knowledge of the 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.

Supporting Knowledge and Skills

a. Discuss the essential elements for planning of S&S programs.

b. Describe the types of facilities for which S&S plans must be developed.

c. Discuss the difference between the Site Safeguards and Security Plan (SSSP) and the Site Security Plan (SSP).

d. Discuss the documents that must be used to support program forecasts and information input used in the protection program planning process.

e. Discuss the plan review and approval process.

f. Discuss the parts of the S&S Management Plan.

g. Describe the DOE's fundamental approach to protecting nuclear weapons and components, Special Nuclear Material (SNM), or targets subject to radiological or toxicological sabotage.

h. Discuss the purpose of an armed Protective Force (PF).

i. Describe the concept of the Tactical Doctrine.

j. Discuss the essential defensive planning principles.

k. Discuss the elements of the Tactical Response Force (TRF).

l. Discuss the National Industrial Security Program (NISP) and agency responsibilities.

m. Discuss the following management considerations in applying the Tactical Doctrine:

- Training and exercise requirements for armed PF and rules of engagement and use of force including rights and responsibilities of PF
- Planning and implementation

2. Safeguards and security personnel with the responsibility for PP&M must demonstrate a working level knowledge of the requirements of the Homeland Security Advisory System.

Supporting Knowledge and Skills

a. Describe the meaning and use of threat indicators and Graded Security Protection (GSP) (formerly the Design Basis Threat [DBT]).

b. Describe the DOE SECON system and the measures to be taken in the five levels.

3. Safeguards and security personnel with the responsibility for PP&M must demonstrate a working level knowledge of the objective and elements that are contained in a SSSP and SSP.

Supporting Knowledge and Skills

a. Discuss the application, scope, and purpose of a SSSP.

b. Discuss the following elements of a SSSP:

- Site Description and Mission
- Site Threat Description and Target Identification
- Site Protection Strategies
- Physical Protection Systems
- Site PF
- Material Control and Accountability (MC&A) Program
- Site Personnel Security and Human Reliability Programs (HRP)
- Automated Information Security Program
- S&S Equipment Maintenance and Testing Programs
- Site Protection Evaluation Program
- Deviations from DOE Directives
- Summary of Vulnerability Assessment **(**VA) and Risk Assessment Results

c. Discuss the application, scope, and purpose of a SSP.

d. Discuss the difference between the SSSP and the SSP.

e. Discuss the plan review and approval process.

f. Discuss the application, scope and purpose of a non-possessing security plan.

4. Safeguards and security personnel with the responsibility for PP&M must demonstrate a working level knowledge of the objective and elements that are contained in a SSSP and SSP Resource Plan (RP).

Supporting Knowledge and Skills

a. Discuss the objective of the SSSP RP.

b. Describe the contents of the following RP elements:

- Operational Requirements
- Capital Equipment
- General Plan Projects
- Line Item Construction Projects
- Unfunded/Unsupported Requirements
- Data to be included in the RP

5. Safeguards and security personnel with the responsibility for PP&M must demonstrate a working level knowledge of the objective and elements that are contained in the VA Program.

Supporting Knowledge and Skills

a. Describe the seven steps in conducting a VA.

b. Discuss the determination and reporting requirements of system effectiveness.

c. Describe the actions that must be taken for the following levels of security system effectiveness:

- Low protection system effectiveness
- Marginal protection system effectiveness

d. Describe the Vulnerability Assessment Certification Program for analyst responsible for the conduct of VAs.

e. Describe the purpose and application of the VA modeling tools listed in Appendix 3—Vulnerability Assessment Modeling Tools of DOE M 470.4-1 Chg 1, *Safeguards and Security Program Planning and Management.*

f. Describe the purpose and application of the system performance effectiveness equation contained in Appendix 4—System Performance Effectiveness Equation of DOE M 470.4-1 Chg 1, *Safeguards and Security Program Planning and Management*.

6. Safeguards and security personnel with the responsibility for PP&M must demonstrate a working level knowledge of the objective and elements that are contained in the Performance Assurance Program.

Supporting Knowledge and Skills

a. Discuss the following essential S&S protection elements validated by the Performance Assurance Program:

- Operability and effectiveness
- Continuity
- Reliability
- Performance tests
- Documentation

b. Describe the contents of the Performance Assurance Program.

7. Safeguards and security personnel with the responsibility for PP&M must demonstrate a working level knowledge of the objective and elements contained in the DOE Oversight Policy.

Supporting Knowledge and Skills

a. Discuss the purpose and general requirements of the DOE Oversight Policy.

b. Describe the four essential elements of the DOE Oversight Model.

c. Describe the following security assurance activities:

- Assessments (including self-assessments or management assessments, operational awareness or management walk-throughs, quality assurance assessments, and internal independent assessments)
- Event reporting (including reporting, analyzing, and trending operational events)
- Worker feedback mechanisms
- Issues management (including analysis of causes, identification of corrective actions, corrective action tracking, monitoring and closure, verification of effectiveness, trend analysis, and identification of continuous improvement opportunities)
- Lessons learned

d. Discuss the activities conducted in contractor S&S oversight assessments.

8. Safeguards and security personnel with the responsibility for PP&M must demonstrate a working level knowledge of the objectives and elements that are contained in the surveys, reviews, and self-assessments conducted by different levels of DOE management, and demonstrate the ability to conduct surveys, reviews, and self-assessments.

Supporting Knowledge and Skills

a. Discuss the objectives of the survey, review, and self-assessment programs.

b. Discuss the various types and frequencies of the following surveys and assessments:

- Initial surveys
- Periodic surveys
- Special surveys
- Termination surveys
- Periodic reviews
- Self-assessments
- Reviews or inspections by other DOE elements or Other Government Agencies (OGA)
- Extension of frequency

c. Discuss the following activities and the methods that must be included in surveys and assessments:

- Compliance
- Performance
- Comprehensiveness

- Determinations of survey scope predicated on the nature or status of operations at the facility, activity, or element being surveyed

d. Discuss the survey or self-assessment procedures that must be developed, documented, approved by the Cognizant Security Authority (CSA), and performed including the following:

- Team composition
- Planning, scheduling, and integration
- Validation
- Exit briefing

e. Discuss the definition of the term “findings” as it relates to surveys, reviews, or self-assessment programs.

f. Discuss the requirements for the administration of the identified finding.

g. Discuss the following types of ratings that must be used for all surveys (except termination), reviews, and self-assessments:

- Satisfactory
- Marginal
- Unsatisfactory
- Inspection Ratings
- Does Not Apply (DNA)
- Not Rated (NR)

h. Discuss the factors used to determine the assigned ratings.

i. Discuss the items that must be contained in the following reports:

- Initial/periodic survey and self-assessment
- Special survey
- Non-possessing facilities
- Termination survey
- Memorandum

j. Conduct a survey, review, or self-assessment.

9. Safeguards and security personnel with the responsibility for PP&M must demonstrate a working level knowledge of 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/or without foreign involvement.

Supporting Knowledge and Skills

a. Discuss the objectives of the FOCI Program.

b. Discuss the entities required to obtain FOCI determinations.

c. Discuss the DOE Acquisition Regulation (DEAR) restrictions on awarding of classified contracts prior the issuance of a FCL.

d. Describe the procedures for using the Department's electronic system for applicants to submit FOCI information to DOE in an electronic format.

10. Safeguards and security personnel with the responsibility for PP&M must demonstrate a working level knowledge of the policies and procedures for FCLs and registration of S&S activities.

Supporting Knowledge and Skills

a. Discuss the eligibility requirements of the FCL Program.

b. Discuss the activities that occur on premises occupied by the Department or its contractors that require an FCL.

c. List the company officials that must be granted access authorizations in order for the company to qualify for an FCL involving classified information or matter, or SNM.

d. Define the term "non-possessing facility."

11. Safeguards and security personnel with the responsibility for PP&M must demonstrate a working level knowledge of the S&S Training Program.

Supporting Knowledge and Skills

a. Discuss the objectives of the S&S Training Program.

b. Discuss the following requirements of the S&S Training Program:

- Key program elements
- Job analysis
- Testing
- Training content
- Training course development.
- Training Approval Program (TAP)
- Training records management
- Training plans

12. Safeguards and security personnel with the responsibility for PP&M must demonstrate a working level knowledge of the S&S Awareness Program.

Supporting Knowledge and Skills

a. Discuss the objectives and requirements of the S&S Awareness Program.

b. Discuss the elements required in the design and development of S&S Awareness Programs.

c. Discuss the types of briefings required by the S&S Awareness Program.

d. Discuss the administration, retention, and storage of the Classified Information Nondisclosure Agreement (SF 312).

e. Discuss the purpose of the supplementary awareness activities.

13. Safeguards and security personnel with the responsibility for PP&M must demonstrate a working level knowledge of the policies and procedures contained in the Incidents of Security Concern Program.

Supporting Knowledge and Skills

a. Discuss the requirements for implementing the Incidents of Security Concern Program.

b. Discuss the elements that provide the basis for identification and categorization of incidents of security concern.

c. Define the actions, inactions, or events that apply to the four categories identified by impact measurement index numbers IMI-1 through IMI-4.

d. Discuss the incidents of security concern reporting requirements.

e. Discuss the authorization and limits of authority of inquiry officials.

f. Discuss the policies and procedures for cooperating with Federal, state, and local law enforcement personnel.

g. Discuss the criteria used to determine the lead organization responsible for conducting an inquiry of an incident of security concern.

h. Describe the actions that must be taken when conducting inquiries into incidents of security concern.

i. Discuss the inquiry report content/closure consideration and administrative actions.

j. Discuss the requirements for the retention of records pertaining to incidents of security concern.

k. Discuss the requirements for inquiries into compromise of, potential compromise of, or missing classified information.

l. Discuss the purpose for damage assessments when classified information has been compromised.

m. Discuss the required damage assessment procedures and the contents of the damage assessment reports.

14. Safeguards and security personnel with the responsibility for PP&M must demonstrate a working level knowledge of the policies and procedures contained in the Control of Classified Visits Program.

Supporting Knowledge and Skills

a. Discuss the procedures that must be in place at the local level for the control of classified visits.

b. Discuss the policies and procedures for classified visits by Departmental employees, contractors, and subcontractors.

c. Discuss the policies and procedures for classified visits to Department of Defense (DoD) and National Aeronautics and Space Administration (NASA) facilities.

d. Discuss the policies and procedures for Restricted Data (RD) visits by Nuclear Regulatory Commission (NRC) employees.

e. Discuss the policies and procedures for RD and other classified visits by DoD, NASA, and OGA employees.

f. Discuss the policies and procedures for Congressional and State classified visits.

g. Discuss the policies and procedures for emergency visits to classified areas and facilities.

15. Safeguards and security personnel with the responsibility for PP&M must demonstrate a working level knowledge of the Unclassified Visits and Assignments of Foreign Nationals Program.

Supporting Knowledge and Skills

a. Describe the policies and procedures for requesting, processing, and approving visits and assignments by foreign nationals.

b. Describe the controls in place regarding the issuance of access badges for foreign nationals.

c. Discuss the appropriate policies and procedures for escorting foreign nationals.

d. Describe the system for communicating between the various site organizations to ensure appropriate control and oversight of foreign nationals.

e. Describe the proper use of specific security plans for foreign nationals or generic plans and whether those plans need to be reviewed and by whom.

f. Describe the system used to contain data on foreign nationals and the information needed for inclusion.

g. What are the prescribed timing requirements for advance notification of a visit of a foreign national?

h. Describe the processes in place for making changes to approved security plans for foreign nationals, for making changes in assigned escorts and how it is reported, and for submitting host reports.

i. Discuss and describe the systems in place to ensure there are no unauthorized access/unintentional disclosure of classified matter, SNM, and/or sensitive unclassified information/technology (including Cooperative Development Agreements and export control information).

j. Discuss the counterintelligence requirements of the Unclassified Visits and Assignments of Foreign Nationals Program.

B. PHYSICAL SECURITY (PS)

Competencies and supporting knowledge and skills for Section B, Physical Security, are derived from the following DOE Orders, Manuals, and Guides:

- 10 CFR Part 860, Trespassing on Department of Energy Property
- 41 CFR Part 101, Federal Property Management Regulations
- 10 CFR Part 1046, Physical Protection of Security Interests
- DOE O 470.3B, *Graded Security Protection (GSP) Policy*
- DOE M 470.4-1 Chg 1, *Safeguards and Security Program Planning and Management*
- DOE M 470.4-2 Chg 1, *Physical Protection*
- DOE O 470.3B, *Graded Security Protection (GSP) Policy*
- DOE M 470.4-6 Chg 1, *Nuclear Material Control and Accountability*
- DOE O 471.1A, *Identification and Protection of Unclassified Controlled Nuclear Information*
- DOE M 471.1-1 Chg 1, *Identification and Protection of Unclassified Controlled Nuclear Information Manual*

16. Safeguards and security personnel with the responsibility for PS must demonstrate a working level knowledge of graded physical protection programs and site physical protection programs.

Supporting Knowledge and Skills

a. Describe the planning, execution, evaluation, and documentation requirements required for site physical protection programs as outlined in the SSSP. For sites not requiring a SSSP, describe the planning, execution, evaluation, and documentation requirements required for site physical protection programs as outlined in a SSP.

b. Describe the following five elements of protection and control planning:

- Site-specific characteristics
- Threat
- Protection strategy
- Planning
- Graded protection

c. Describe how the GSP Policy is used in S&S program planning.

d. Describe the principles of the VA process and how the PS program is a part of a facility's VA program.

e. Describe the method used to identify and characterize the range of potential adversary threats.

f. Discuss the denial strategy used to protect S&S interests.

g. Discuss the performance testing requirements for physical protection systems.

17. Safeguards and security personnel with the responsibility for PS must demonstrate a working level knowledge of physical protection systems.

Supporting Knowledge and Skills

a. Describe the three primary functions of a physical protection system.

b. Describe the characteristics of an effective physical protection system.

c. Describe the fundamental characteristics of exterior and interior intrusion sensors.

d. Using a list of exterior and interior sensors, describe the operating characteristics of each type of sensor.

e. Describe the types of exterior and interior sensors used within DOE.

f. Describe the components of a comprehensive entry control and contraband detection system.

g. Describe the types of access control systems used within DOE.

h. Describe the purpose of access delay in a physical protection system.

i. Describe the type of access delay mechanisms used within DOE.

j. Discuss the following terms:

- Defense-in-depth
- Probability of detection
- Delay time
- Active and passive barriers
- Complementary sensors
- Assessment
- Detection
- Compensatory measures

k. Demonstrate the modeling of a physical protection system using an adversary sequence diagram.

18. Safeguards and security personnel with the responsibility for PS must demonstrate a working level knowledge of the protection of nuclear weapons, components, and SNM.

Supporting Knowledge and Skills

a. Discuss the graded approach in relation to the protection of S&S interests.

b. Describe protection strategies for Category I and II SNM, such as denial and containment, and recapture, recovery, and/or pursuit.

c. Describe the physical protection for each category of SNM considering the following factors:

- Quantities,
- Chemical forms
- Isotopic composition purities (ease of separation, accessibility, concealment, and portability)
- Radioactivity
- Self-protecting features

d. Discuss the following as they relate to the integrated physical protection of nuclear weapons and Category I and II quantities of SNM:

- Intrusion detection systems
- Delay mechanisms
- PF
- Storage controls

e. Discuss the programs designed to mitigate radiological/toxicological sabotage.

f. Describe access procedures to storage repositories.

g. Describe procedures to prevent and detect unauthorized access to a storage repository.

h. Describe escort responsibilities when SNM is in transit.

i. Discuss the protection standards for Category I thru IV SNM.

19. Safeguards and security personnel with the responsibility for PS must demonstrate a working level knowledge of protection of classified information and matter.

Supporting Knowledge and Skills

a. Describe the methods for protection and control of classified matter.

b. Describe the classification levels and appropriate control of classified matter at each level.

c. Discuss access controls, such as need-to- know, that must be established to detect and deter unauthorized access to classified matter.

d. Describe access procedures to storage repositories.

e. Describe procedures to prevent and detect unauthorized access to a storage repository.

f. Describe the level of protection for Sensitive Compartmented Information Facilities (SCIF).

g. Describe the requirements of a Technical Surveillance Countermeasures Program.

20. Safeguards and security personnel with the responsibility for PS must demonstrate a working level knowledge of radiological, chemical, and biological sabotage protection programs.

Supporting Knowledge and Skills

a. Describe the site/facility requirements for S&S functions for radiological, chemical, or biological sabotage protection to be coordinated and integrated into its emergency management plan and radiation protection program.

b. Discuss the physical protection strategies that must be developed, documented, and implemented consistent with the GSP to protect radiological, chemical, or biological sabotage targets.

c. Discuss the following prevention and mitigation measures that must be based on the results of the radiological, chemical, or biological sabotage analysis:

- S&S features to detect or delay adversary actions
- Additional controls or equipment that would prevent a sabotage release scenario
- Event-mitigating actions such as establishing shelters, emergency notifications/evacuations, reducing and/or removing inventory quantities, or changing storage locations

21. Safeguards and security personnel with the responsibility for PS must demonstrate a working level knowledge of security areas.

Supporting Knowledge and Skills

a. Describe the level of protection, access requirements, storage requirements, and alarm response requirements given to the following types of concentric security areas and the assets they protect::

- Property protection areas
- Limited area
- Exclusion area
- Protected Area (PA)

- Vital areas
- Material Access Areas (MAA)

b. Discuss the specific access requirements for the following types of special designated security areas as applicable to your site:

- Special access programs
- Alarm areas
- Sensitive compartmented information facilities
- Other designated security alarm stations
- Secure communication centers and automated information system centers

c. Discuss methods to detect, assess, deter, and prevent unauthorized access to security areas.

d. Describe when random entry/exit inspections are conducted and give reasons for those inspections.

e. List the types of privately owned and controlled articles prohibited from a security area.

22. Safeguards and security personnel with the responsibility for PS must demonstrate a working level knowledge of alarm management and control systems.

Supporting Knowledge and Skills

a. Discuss the characteristics/capabilities of alarm stations as they relate to monitoring and assessing alarms and initiating responses to incidents.

b. Discuss the protection and access requirements for facilities holding Category I and II quantities of SNM, or other high-consequence targets as identified by VAs.

23. Safeguards and security personnel with the responsibility for PS must demonstrate a working level knowledge of protection of security system elements.

Supporting Knowledge and Skills

a. Describe how security-related equipment must be protected from unauthorized access in a graded manner consistent with the security interest under protection.

24. Safeguards and security personnel with the responsibility for PS must demonstrate the ability to review and access the contractor's protection program.

Supporting Knowledge and Skills

a. Conduct an assessment of the contents and accuracy of the contractor's protection and control planning.

b. Assess the contractor's methods for protecting SNM and vital equipment.

c. Assess the contractor's program for protecting and controlling classified matter and computer resource assets.

d. Assess the contractor's program for establishing, controlling, and maintaining security and restricted access areas.

e. Assess and approve the protection elements established by the contractor.

C. PROTECTIVE FORCE OPERATIONS (PFO)

Competencies and supporting knowledge and skills for Section C, Protective Force Operations, are derived from the following DOE Orders, Manuals, and Guides:

- 10 CFR Part 1047, Limited Arrest Authority and Use of Force by Protective Force Officers
- DOE O 440.1B, *Worker Protection Program for DOE (Including the National Nuclear Security Administration) Federal Employees*
- DOE O 440.2B Chg 1, *Aviation Management and Safety*
- DOE O 470.4A, *Safeguards and Security Program*
- DOE M 470.4-1 Chg 1, *Safeguards and Security Program Planning and Management*
- DOE M 470.4-2 Chg 1, *Physical Protection*
- DOE Manual 470.4-3 Chg 1, *Protective Force*
- DOE Manual 470.4-3A, *Contractor Protective Force*
- DOE M 470.4-6 Chg 1, *Nuclear Material Control and Accountability*
- DOE O 470.3B, *Graded Security Protection (GSP) Policy*
- DOE O 471.1A, *Identification and Protection of Unclassified Controlled Nuclear Information*
- DOE M 471.1-1 Chg 1, *Identification and Protection of Unclassified Controlled Nuclear Information Manual*

25. Safeguards and security personnel with the responsibility for PFO must demonstrate a working level knowledge of the planning for PFO.

Supporting Knowledge and Skills

a. Discuss the planning requirements to ensure appropriate response or defense by the site PFs.

b. Describe the purpose of the following types of plans as they relate to PFO:

- Security Incident Response Plans
- Facility Evacuation Response Plans
- Security Contingency Response Plans
- Target folders
- Fresh pursuit for property or SNM theft

c. Describe the principle and applicability of non-Departmental law enforcement agency support.

d. Describe the levels, associated responsibilities, and qualification requirements of PF personnel within DOE.

e. Discuss the authority and responsibility for issuing credentials and shields for each level of PF personnel within DOE.

f. Discuss the general guidelines for fresh pursuit.

26. Safeguards and security personnel with the responsibility for PFO must demonstrate a working level knowledge of PF duties.

Supporting Knowledge and Skills

a. Discuss the general duties and response categorization requirements of the three PF levels.

b. Discuss how responsibilities identified in a PF job analysis relate to proficiency in the skills and abilities necessary to perform job tasks.

c. Discuss the use of deadly force and limited arrest authority as set forth in 10 CFR 1047, Limited Arrest Authority and Use of Force by Protective Force Officers.

d. Describe DOE's policy for rules of engagement for the use of PF and remotely-operated weapons systems.

e. Describe the following safety, training, authorization requirements for an armed PF:

- Firearms safety procedures related to duty weapons
- Firearms training and qualification requirements for all duty weapons
- Application of the authorization to carry firearms and make arrests without a warrant while performing official duties

27. Safeguards and security personnel with the responsibility for PFO must demonstrate a working level knowledge of the Special Response Team (SRT).

Supporting Knowledge and Skills

a. Discuss mission requirements of a SRT as they relate to the following:

- Interdiction
- Interruption
- Neutralization
- Containment
- Denial
- Recapture
- Recovery
- Pursuit

b. Discuss the mission and special training requirements of Precision Rifle Forward Observer Team members and Tactical Entry Specialists.

c. Discuss the SRT program certification/recertification requirements.

28. Safeguards and security personnel with the responsibility for PFO must demonstrate a working level knowledge of PF training and qualification.

Supporting Knowledge and Skills

a. Discuss the requirement for developing and revising a job analysis for PF positions.

b. Discuss the required elements of a PF training program.

c. Discuss the special training requirements required to support the maintenance of a qualified instructor cadre.

29. Safeguards and security personnel with the responsibility for PFO must demonstrate a working level knowledge of security helicopter flight operations.

Supporting Knowledge and Skills

a. Discuss the purpose of an Aviation Implementation Plan.

b. Discuss the mission readiness requirements and operations of security helicopters.

c. Discuss the conditions and rules of engagement if a helicopter is used as a firing platform.

d. Discuss the requirement for, and contents of, a Safety Analysis Review (SAR) of aerial firing.

30. Safeguards and security personnel with the responsibility for PFO must demonstrate a working level knowledge of PFs' equipment and facilities.

Supporting Knowledge and Skills

a. Discuss the types and quantity of equipment and facilities provided to PFs to effectively and efficiently conduct routine and emergency operations to meet the GSP Policy.

31. Safeguards and security personnel with the responsibility for PFO must demonstrate a working level knowledge of PF performance testing.

Supporting Knowledge and Skills

a. Define and discuss the purpose and frequency of the following:

- Limited Scope Performance Tests (LSPT)
- Alarm Response and Assessment Performance Tests (ARAPT)
- Validation Force-on-Force (VFoF)
- Command Post Exercise (CPX)

- Command Field Exercise (CFX)
- Joint Training Exercise (JTX)

b. Discuss the five major types of Engagement Simulations Systems (ESS).

c. Discuss the safety factors and rules of engagement involved with the deployment of ESS.

d. Demonstrate the ability to assess the contractor's performance test plans involving ESS; examining the activity, command and control, and safety as applicable to S&S planning principles.

e. Discuss the use of the computer modeling Joint Conflict and Tactical Simulation (JCATS) and tabletop modeling Analytic System and Software for Evaluating Safeguards and Security (ASSESS) to evaluate PFO.

D. INFORMATION PROTECTION (IP)

The information protection program includes Classified Matter Protection and Control (CMPC); Operations Security (OPSEC); Technical Surveillance Countermeasures (TSCM); security of Foreign Government Information (FGI) and Sensitive Compartmented Information (SCI); security of Special Access Programs (SAP); and unclassified information required to be controlled by statutes, regulations, or DOE directives, generally referred to as Controlled Unclassified Information (CUI). Competencies and supporting knowledge and skills for Section D, Information Protection, are derived from the following DOE Orders, Manuals, and Guides:

- 10 CFR Part 1016, Safeguarding of Restricted Data
- 32 CFR Part 2003, National Security Information-Standard Forms
- DOE O 470.4A, *Safeguards and Security Program*
- DOE M 470.4-4A, *Information Security Manual*

32. Safeguards and security personnel with the responsibility for IP must demonstrate a working level knowledge of the security requirements for the protection and control of information and matter required to be classified or controlled by statutes, regulations, or DOE directives.

Supporting Knowledge and Skills

a. Discuss the requirements for the planning and implementation of a CMPC Program.

b. Discuss the training requirements for the CMPC Program.

c. Describe the storage requirements that apply to security containers, vaults, or Vault-Type Rooms (VTRs) that contain classified matter or other S&S interests.

d. Discuss the policies and procedures for the documentation requirements that must be met for each security container, vault, or VTR approved to store classified matter.

e. Discuss the requirements for classifying and protecting combinations for containers that store classified matter.

33. Safeguards and security personnel with the responsibility for IP must demonstrate a working level knowledge of the policies and procedures for CMPC.

Supporting Knowledge and Skills

a. Discuss the CMPC requirements.

b. Discuss the requirements for the use of a cover sheet for a document undergoing classification review.

c. Discuss the policies and procedures pertaining to access to classified matter in an emergency.

d. Discuss the policies and procedures pertaining to protection and control of classified matter that is in use.

e. Discuss the policies and procedures pertaining to protection and control of classified matter that is in storage, including non-conforming storage.

f. Discuss the policies and procedures pertaining to protection and control of classified matter that is being transmitted and received.

g. Discuss the policies and procedures pertaining to accountability of classified matter.

34. Safeguards and security personnel with the responsibility for IP must demonstrate a working level knowledge of the policies and procedures for marking classified matter.

Supporting Knowledge and Skills

a. Discuss the requirements for the marking of classified matter.

b. Discuss the requirement for the proper identification of the originating organization, date, and classification level on all classified matter.

c. Discuss the marking of classified matter with the assigned classification level and category.

d. Discuss the requirements for marking classified matter that has mixed levels and categories.

e. Discuss the requirements for marking classified matter that has multiple components that can be used separately.

f. Discuss the marking of unclassified matter that is embedded in classified matter.

g. Discuss the requirements for marking portions of classified documents.

h. Discuss the use and marking of subjects and titles used for classified documents.

i. Discuss the policies and procedures for using caveats and special control markings.

j. Discuss the policies and procedures for remarking, upgrading, and downgrading classified matter.

k. Discuss the policies and procedures for marking declassified matter.

l. Discuss the policies and procedures for marking the following:

- Charts, maps, drawings and tracings
- Messages
- Classified electronic mail (E-Mail) messages
- Facsimiles
- Microfiche, microfilm, and aperture cards
- Motion picture films and video tapes
- Photographs and negative rolls
- Transparencies, slides, and sheet film
- Magnetic, electronic, or sound recordings
- Classified information system media
- U.S. classified information translated into a foreign language.
- Unclassified matter used to simulate or demonstrate classified matter for training purposes
- Classified page changes that result from periodic updates to a classified document
- File folders and other containers containing classified matter
- Working papers

35. Safeguards and security personnel with the responsibility for IP must demonstrate a working level knowledge of the policies and procedures for the management of the marking of classified documents received from OGA and foreign governments not conforming to DOE requirements.

Supporting Knowledge and Skills

a. Discuss the procedures for the proper marking of documents received from OGA and/or foreign governments.

36. Safeguards and security personnel with the responsibility for IP must demonstrate a working level knowledge of the policies and procedures for control and accountability systems used to prevent unauthorized access to or removal of classified information.

Supporting Knowledge and Skills

a. List the different types of accountable matter.

b. Discuss the policies and procedures for the accounting of Classified Removable Electronic Media (CREM).

c. Discuss the policies and procedures for the use of control stations to maintain records and access lists.

d. Discuss the development and maintenance of accountability systems and records.

e. Discuss the policies and procedures for maintaining an inventory of accountable documents and matter.

f. Discuss the policies and procedures for the maintenance of records, master files and databases, and working papers and drafts.

g. Discuss the requirements governing the establishment and use of automated accountability systems and electronic receipting.

37. Safeguards and security personnel with the responsibility for IP must demonstrate a working level knowledge of the policies and procedures for the reproduction of classified information.

Supporting Knowledge and Skills

a. Discuss the general regulations for reproducing classified documents.

b. Discuss the policies and procedures concerning the use of equipment used to reproduce classified information.

c. Discuss the procedures for reproducing documents received from outside agencies.

d. Discuss the requirements for reproduction of CREM.

38. Safeguards and security personnel with the responsibility for IP must demonstrate a working level knowledge of the policies and procedures for receiving and transmitting classified matter.

Supporting Knowledge and Skills

a. Discuss the general rules for the transmission and receipt of classified matter.

b. Discuss the controls that must be applied to classified matter received at a facility.

c. Discuss the methods for packaging classified matter that is be transmitted outside or inside a facility.

d. Discuss the use and contents of form DOE F 5635.3, Classified Document Receipt.

e. Discuss the policies and procedures for using classified addresses.

f. Discuss the policies and procedures for hand-carrying classified matter outside of a facility.

g. Discuss the policies and procedures for the use of commercial express service organizations for transmitting classified matter outside of a facility.

39. Safeguards and security personnel with the responsibility for IP must demonstrate a working level knowledge of the policies and procedures for the disposition of classified matter in the event of a contract closeout or a FCL termination.

Supporting Knowledge and Skills

a. Discuss the reporting requirements for the disposition of classified matter upon contract completion.

b. Discuss the policies and procedures for disposition of classified matter in the termination of a FCL.

40. Safeguards and security personnel with the responsibility for IP must demonstrate a working level knowledge of the policies and procedures for the destruction of classified matter.

Supporting Knowledge and Skills

a. Discuss the identification of classified matter subject to destruction.

b. Discuss the procedures to be followed in the destruction of classified matter under a court order prohibiting destruction.

c. Discuss the authorized types of destruction and the special requirements that must be satisfied when classified matter is destroyed.

d. Discuss the policies and procedures for the destruction of classified matter by the use of approved equipment.

e. Discuss the requirement for witnesses during the destruction of classified matter.

f. Discuss the requirements for creation and retention of records of destruction when classified matter is destroyed.

g. Discuss the policies and procedures for the disposition of classified waste.

41. Safeguards and security personnel with the responsibility for IP must demonstrate a working level knowledge of the policies and procedures for managing foreign government information.

Supporting Knowledge and Skills

a. Discuss the policies and procedures for safeguarding classified matter furnished by foreign governments and U.S. information that may be combined with it.

42. Safeguards and security personnel with the responsibility for IP must demonstrate a working level knowledge of the policies and procedures for the marking and accountability of classified material.

Supporting Knowledge and Skills

a. Discuss the policies and procedures for marking classified material.

b. Discuss the accountability requirements for classified material.

43. Safeguards and security personnel with the responsibility for IP must demonstrate a working level knowledge of the policies and procedures for OPSEC.

Supporting Knowledge and Skills

a. Discuss the required activities that must be included in an OPSEC program.

b. Discuss the planning, reviewing, and updating requirements for the OPSEC plan.

c. Discuss the identification and maintenance of Critical Program Information (CPI), including a discussion of indicators of CPI.

d. Discuss the policies and procedures for conducting and reporting the results of OPSEC assessments.

e. Discuss the policies and procedures for conducting and reporting the results of OPSEC reviews.

f. Discuss the restrictions on information that will be posted to publicly available web sites.

g. Discuss vulnerabilities and countermeasures.

44. Safeguards and security personnel with the responsibility for IP must demonstrate a working level knowledge of the policies and procedures for SAPs.

Supporting Knowledge and Skills

a. Discuss the policies and procedures for SAPs authorized for use within the Department.

45. Safeguards and security personnel with the responsibility for IP must demonstrate a working level knowledge of the policies and procedures for protecting and controlling CUI.

Supporting Knowledge and Skills

a. Discuss the policies and procedures for protecting and controlling CUI.

E. PERSONNEL SECURITY (PERS SEC)

Competencies and supporting knowledge and skills for Section E, Personnel Security, are derived from the following DOE Orders, Manuals, and Guides:

- 10 CFR 710, Criteria and Procedures for Determining Eligibility for Access to Classified

Matter or Special Nuclear Material
- 10 CFR 712, Human Reliability Program
- DOE O 470.4A, *Safeguards and Security Program*
- DOE M 470.4-5, *Personnel Security*
- DOE M 470.4-5, *Personnel Security*

46. Safeguards and security personnel with the responsibility for PERS SEC must demonstrate a working level knowledge of the access authorization (security clearance) process.

Supporting Knowledge and Skills

a. Discuss the following terms:

- Derogatory information
- Access authorization
- Types of security clearances
- Types of access authorizations
- Types of background investigations
- Federal investigative standards
- Reciprocity
- Suspension
- Administrative Review (AR)

b. Discuss the process for screening reports of investigation for “Q” and “L” access authorizations.

c. Explain the purpose of the PERS SEC interview.

47. Safeguards and security personnel with the responsibility for PERS SEC must demonstrate a working level knowledge of the policies, procedures, and governing requirements of the DOE PERS SEC program.

Supporting Knowledge and Skills

a. Describe the general requirements for determining the type of access authorization and investigative requirements, including those involving dual citizenship and foreign nationals.

b. Describe the processes used for screening and analysis of PERS SEC cases and methods for determining access authorization eligibility.

c. Describe the six types of investigations most frequently conducted for the DOE.

d. Discuss the tasks associated with the processing of a change to spouse/cohabitant form submitted by personnel with a “Q” or ”L” clearance.

e. Discuss the extension, transfer, termination, and reinstatement of access authorizations.

f. Describe the reinvestigation program.

48. Safeguards and security personnel with the responsibility for PERS SEC must demonstrate the ability to assess the PERS SEC program elements.

Supporting Knowledge and Skills

a. Discuss the procedures used to assess the effectiveness of the DOE or contractor strategies for maintaining the minimum number of access authorizations consistent with operational efficiency.

b. Discuss methods used to determine the effectiveness of management and operating contractor pre-employment checks conducted in accordance with the DEAR.

c. Discuss procedures for determining contractor compliance with requirements for timely notification of access authorization termination to the DOE.

d. Discuss the methods used in background investigations of funding estimates in response to budget calls.

49. Safeguards and security personnel with the responsibility for PERS SEC must demonstrate a working level knowledge of all aspects and actions required of the access authorization process.

Supporting Knowledge and Skills

a. Describe the tasks associated with processing access authorization requests for access to classified matter or SNM.

b. Describe the tasks associated with downgrading, transferring, or extending an access authorization for access to classified matter or SNM.

c. Describe the tasks associated with ensuring a reinvestigation is completed.

d. Discuss the tasks associated with terminating an access authorization.

e. Discuss the tasks associated with the processing of a change to spouse/cohabitant form submitted by personnel with a “Q” or “L” clearance.

f. Discuss the tasks associated with processing a Report of Investigation (ROI).

g. Describe the tasks associated with processing reconsiderations.

50. Safeguards and security personnel with the responsibility for PERS SEC must demonstrate a working level knowledge of all aspects and actions required of the PERS SEC adjudication process.

Supporting Knowledge and Skills

a. Describe the procedures for conducting a screening of requests for access to classified matter or SNM.

b. Describe the evaluation (second review) process.

c. Discuss the processing of a Letter of Interrogatory (LOI).

d. Discuss the methods for conducting a Personnel Security Interview (PSI).

e. Describe the process used in coordinating a mental evaluation.

f. Describe the processing of a suspension.

51. Safeguards and security personnel with the responsibility for PERS SEC must demonstrate a working level knowledge of all aspects and actions required of the AR process.

Supporting Knowledge and Skills

a. Describe the processing of an AR.

b. Discuss the tasks associated with participating in an AR hearing.

c. Describe the tasks associated with taking actions following an AR hearing.

52. Safeguards and security personnel with the responsibility for PERS SEC must demonstrate a working level knowledge of the HRP.

Supporting Knowledge and Skills

a. Describe the purpose of the HRP.

b. Describe the process for identifying or removing positions from the HRP.

c. Describe the general requirements for HRP certification.

F. NUCLEAR MATERIAL CONTROL AND ACCOUNTABILITY (MC&A)

Competencies and supporting knowledge and skills for Section F, Nuclear Materials Control and Accountability, are derived from the following DOE Orders, Manuals, and Guides:

- DOE M 470.4-6 Chg 1, *Nuclear Material Control and Accountability*

53. Safeguards and security personnel with the responsibility for MC&A must demonstrate a working level knowledge of program administration of MC&A systems.

Supporting Knowledge and Skills

a. Describe the MC&A program for controlling and accounting for all identified nuclear materials and the prevention of theft and diversion of SNM.

b. Discuss the procedures in place for the prevention of the unauthorized control of a weapon, test device, or materials that can be used to make an improvised nuclear device.

c. Describe the procedures for receiving, processing, and storing of SNM at an approved facility.

d. Describe the methods in place designed to deter and detect theft and diversion of nuclear material by both outside and inside adversaries.

e. Discuss the performance testing program to verify MC&A procedures and practices and to demonstrate that material controls are effective.

f. Describe the use of the Reporting Identification Symbol (RIS) in the inventory of nuclear materials, and the methods for reporting and submitting data to the Nuclear Materials Management and Safeguards Systems (NMMSS).

g. Describe the authorities and responsibilities for the MC&A functions (e.g., accounting system, measurements, measurement control, inventories, audit, material access controls, and surveillance).

h. Describe the contents and use of the Table I-1, Nuclear Materials, contained in DOE M 470.4-6 Chg 1, *Nuclear Material Control and Accountability*.

i. Describe how nuclear material inventory holdings are accounted for and controlled.

j. Explain the elements of the MC&A program that are designed to deter and detect loss, theft, and diversion of nuclear materials and the unauthorized control of a weapon, test device, or materials that can be used to make an improvised nuclear device. Discuss the measures used to ensure that nuclear materials are in their authorized locations and being used for their intended purposes.

k. Describe the facility-specific requirements approved by the DOE CSA including, but not limited to, agreements between Government and contractor organizations, access control and material surveillance testing measures, and the scope and extent of the performance testing program.

l. Discuss the MC&A plan review frequency and change control mechanisms.

m. Discuss the established procedures used by the site/facility operator for emergency conditions and periods when MC&A systems are inoperative, and explain the measures in place to ensure that access to or removal of SNM would be detected during these periods, and the control of SNM and measures to be taken before resuming operations following the emergency.

n. Describe the policies and procedures for the termination of safeguards of nuclear materials that exempts nuclear materials from requirements of DOE M 470.4-6 Chg 1, *Nuclear Material Control and Accountability*.

o. Describe the policies and procedures for applying reduced safeguards to materials that both meet the criteria of Table I-3, Technical Criteria for Retained Waste, and have been removed from processing Material Balance Areas (MBAs).

p. Describe the policies and procedures for decommissioning, closure, or deactivation of facilities where MBAs have been established.

q. Describe the graded safeguards program for the control and accountability for the types and quantities of SNM that can be most effectively used in a nuclear explosive device.

r. Discuss the MC&A requirements for source and other nuclear materials.

s. Describe the policies and procedures required in loss detection evaluation, performance testing, and performance requirements.

t. Describe the policies and procedures required in reporting incidents of security concern.

u. Describe the program to periodically review and assess the integrity and quality of its MC&A program and practices for normal operations and emergency conditions.

54. Safeguards and security personnel with the responsibility for MC&A must demonstrate a working level knowledge of the methods for materials accountability.

Supporting Knowledge and Skills

a. Discuss the accounting system for tracking nuclear material inventories, documenting nuclear material transactions, issuing periodic reports, and assisting with the detection of unauthorized system access, data falsification, and material gains or losses.

b. Describe the physical inventory program for nuclear materials to demonstrate that materials are present in their stated quantities and to detect the unauthorized removal of nuclear materials.

c. Describe the Measurement and Measurement Control Programs used to determine Category I or II inventories of SNM.

d. Discuss the Nuclear Material Transfers Program used to control and account for both internal and external transfers of nuclear materials for each facility. Define the procedures that specify requirements for authorization, documentation, tracking, verification, and response to abnormal situations that may occur during transfer of nuclear materials.

e. Describe the graded system of measurements and records that monitors internal and external transfers of nuclear material to deter/detect unauthorized removal of material during such transfers.

f. Describe the Material Control Indicators Program for detecting losses through evaluation and assessment of shipper/receiver differences, inventory differences, and other inventory adjustments.

55. Safeguards and security personnel with the responsibility for MC&A must demonstrate a working level knowledge of the methods for materials control.

Supporting Knowledge and Skills

a. Describe the Access Controls Program that controls personnel access to nuclear materials; nuclear materials accountability, inventory, and measurement data; data-generating equipment; and other items/equipment the misuse of which could compromise the safeguards system.

b. Describe the Nuclear Material Surveillance Program used to ensure that nuclear materials are in their authorized locations, detect unauthorized activities or anomalous conditions, and report material status in both normal and emergency conditions.

c. Describe the Material Containment Program that provides controls for nuclear materials operations relative to MAA, PA, MBA, other authorized storage repositories, and processing areas.

d. Describe detection/assessment systems that are in place to detect and assess the unauthorized removal of nuclear materials, consistent with the graded safeguards concept.

e. Define how the detection/assessment system(s) are interfaced with the facility's physical protection and other organizational systems, as appropriate, and how they detect and localize removal of SNM from its authorized location, and notify the PF and other organizations to respond when such events are detected.

f. Discuss the detection/assessment of unauthorized removal of nuclear material.

56. Safeguards and security personnel with the responsibility for MC&A must demonstrate a working level knowledge of the requirements for NMMSS reporting and data submission.

Supporting Knowledge and Skills

a. Discuss the documentation and reporting requirements for all RIS level nuclear materials transactions, material balances, and inventories into the NMMSS.

b. Describe the data collection forms (or the electronic equivalent) used to document and report nuclear materials transactions, material balances, and inventories.

c. Discuss the establishment, maintenance, and deactivation of an individual RIS.

57. Safeguards and security personnel with the responsibility for MC&A must demonstrate a working level knowledge of the requirements for nuclear materials transaction reporting.

Supporting Knowledge and Skills

a. Describe the documentation and reporting of the physical transfer of nuclear material.

58. Safeguards and security personnel with the responsibility for MC&A must demonstrate a working level knowledge of the requirements for nuclear material balance reporting.

Supporting Knowledge and Skills

a. Describe the instructions to DOE license-exempt contractors, the NRC, and Agreement State licensees that are DOE contractors for the preparation and distribution of DOE/NRC F 742, Material Balance Report (MBR), or its electronic equivalent.

b. Describe the special procedures for facilities that have been selected under the terms of either the U.S./International Atomic Energy Agency (IAEA) Safeguards Agreement or Protocol for the preparation and distribution of DOE/NRC F 742, MBR, or its electronic equivalent.

59. Safeguards and security personnel with the responsibility for MC&A must demonstrate a working level knowledge of the requirements for inventory reporting.

Supporting Knowledge and Skills

a. Discuss the instructions to license-exempt contractors, the NRC, and Agreement State licensees that are contractors for the preparation and distribution of DOE/NRC F 742C, Physical Inventory Listing.

b. Describe the use of the following:

- Nuclear material composition codes and descriptions
- Authorized profiles of inventory data
- Nuclear material type codes

c. Describe the procedures for the following:

- Reconciliation of facility data with NMMSS
- Preparation of DOE/NRC F 742C
- Distribution of DOE/NRC F 742C data

G. CYBER SECURITY (CS)

Competencies and supporting knowledge and skills for Section G, Cyber Security, are derived from the following DOE Orders, Manuals and Guides:

- DOE O 205.1A, *Department of Energy Cyber Security Management*

- DOE P 205.1, *Departmental Cyber Security Management Policy*
- DOE M 205.1-4, *National Security System Manual*
- DOE M 205.1-5, *Cyber Security Process Requirements Manual*
- DOE M 205.1-6, *Media Sanitization Manual*
- DOE M 205.1-7, *Security Controls for Unclassified Information Systems Manual*
- DOE M 205.1-8, *Cyber Security Incident Management Manual*

60. Safeguards and security personnel with the responsibility for CS must demonstrate a working level knowledge of the CS Program.

Supporting Knowledge and Skills

a. Discuss the DOE Cyber Security Plan and the genesis of it.

b. Discuss the roles and responsibilities of Federal and contractor personnel as they relate to the CS Program and the onsite management of the program.

c. Discuss the site's cyber risk management processes – including the threat and risk statements and how they are integrated into the site's processes.

d. Discuss the site's cyber configuration management program.

e. Discuss the following as they pertain to CS:

- Deviation process
- Incident management process
- Information condition process
- Vulnerability management
- Foreign national access
- Password generation, protection, and use
- Portable electronic devices
- Wireless technologies, remote access, and peer-to-peer networking technologies
- Training and awareness
- Federal and contractor self-assessment processes
- Contingency planning and disaster recovery
- Clearing, purging, and destroying media and associated Federal approval roles

f. Discuss the Cyber Security Program Plan (CSPP), including the approvals and review timeframes.

g. Discuss how telecommunications security integrates with CS.

61. Safeguards and security personnel with the responsibility for CS must demonstrate a working level knowledge of the Federal planning processes as well as the contractor feedback processes (i.e., oversight) as it pertains to the CS budget and oversight.

Supporting Knowledge and Skills

a. Discuss the process between the site office, the contractor site, and Headquarters in terms of planning, prioritizing, submission, and periodic reviews.

b. Discuss the current Headquarters Program Execution Guidance and how it is integrated with the site's implementation plan and the Performance Execution Plan (PEP).

c. Discuss the methodology used to provide contractors feedback regarding their CS performance.

d. Discuss how federally-issued; including those from Headquarters, the Office of Health, Safety, and Security, the Office of the Inspector General, the Government Accountability Office, etc; findings/deficiencies are tracked and evaluated.

62. Safeguards and security personnel with the responsibility for CS must demonstrate a working level knowledge of the associated processes.

Supporting Knowledge and Skills

a. Discuss the Plan of Actions and Milestones (POAM) process, including the types of issues tracked and how those issues are determined.

b. Define a Federal Information Security Management Act (FISMA) of 2002 system.

c. Discuss how the site tracks and manages FISMA systems.

d. Discuss the system inventory process.

63. Safeguards and security personnel with the responsibility for CS must demonstrate the ability to conduct oversight in accordance with the site's policies, including programmatic reviews, performance tests, and reviews of technical processes.

Supporting Knowledge and Skills

a. Demonstrate the ability by conducting a CS programmatic review documented in accordance with site procedures.

b. Demonstrate the ability by conducting a CS performance test documented in accordance with site procedures.

c. Demonstrate the ability by conducting a CS review of a selected technical implementation documented in accordance with site procedures.

64. Safeguards and security personnel with the responsibility for CS must demonstrate a working level knowledge of the *Certification and Accreditation (C&A) Processes for Information Systems* or its subsequent revisions.

Supporting Knowledge and Skills

a. Describe the national drivers for the C&A process.

b. Describe the C&A process, including approvals and associated timeframes.

c. Describe the differences between the “Approval to Operate,” “Interim Approval to Operate,” and “Interim Approval to Test.”

d. Describe the differences between a Type, Site, and System Accreditation.

e. Describe system categorization, the consequence of loss, and the methodology used to determine the correct management, operational, and technical controls.

f. Describe the information groups, their respective consequence of loss, and how this is considered in determining appropriate security controls.

g. Describe the site’s major applications.

h. Describe security testing and evaluation as they relate to C&A.

i. Discuss the risk assessment as it relates to C&A.

j. Discuss the privacy impact assessment as it relates to C&A.

k. Describe the Interconnection Security Agreement (ISA) as it relates to C&A.

l. Describe the approvals associated with a C&A package.

65. Safeguards and security personnel with the responsibility for CS must demonstrate the ability to evaluate information system security plans, risk assessments, and issue approval to operate.

Supporting Knowledge and Skills

a. Demonstrate the ability to evaluate an information system security plan, including a risk assessment.

b. Demonstrate the ability to accredit a CS system, including conducting an assessment that supports an accreditation decision.

66. Safeguards and security personnel with the responsibility for CS must demonstrate a working level knowledge of the following concepts, as taken from the Common Body of Knowledge, as they relate to CS and oversight.

Supporting Knowledge and Skills

a. Describe “access controls” as it relates to CS.

b. Describe “application security” as it relates to CS.

c. Describe “cryptography” as it relates to CS.

d. Describe “legal, regulations, compliance and investigations” as they relate to a cyber system.

e. Describe “OPSEC” as it relates to CS.

f. Describe “physical (environmental) security” as it relates to CS.

g. Describe “security architecture and design” as they relate to CS.

h. Describe “telecommunications and network security” as it relates to CS.

67. Safeguards and security personnel with the responsibility for CS must demonstrate a working level knowledge of information technology disciplines.

Supporting Knowledge and Skills

a. Describe the following information technology elements and how they relate to CS:

- Networks
- Hardware
- Software
- Databases
- Websites
- Programming
- Operating systems

INTENTIONALLY BLANK

APPENDIX A
CONTINUING EDUCATION, TRAINING, AND PROFICIENCY PROGRAM

The following list represents suggested continuing education, training, and other opportunities that are available for DOE personnel after completion of the competency requirements in this technical FAQS. It is extremely important that personnel involved with this program maintain their proficiency primarily by regularly demonstrating their competency through on-the-job performance, supplemented with continuing education, training, reading, or other activities, such as workshops, seminars, and conferences. The list of suggested activities was developed by the subject matter experts involved in the development of the FAQS and is not all-inclusive.

Based on the knowledge and experience of the subject matter experts, it is suggested that the following activities support the maintenance of proficiency in the Safeguards and Security Functional Area after completion of the competencies in the standard and other requirements of the TQP.

LIST OF CONTINUING EDUCATION, TRAINING, AND OTHER ACTIVITIES

1. Continuing technical education and/or training covering topics directly related to the Safeguards and Security Functional Area as determined appropriate by management. This may include courses/training provided by DOE, OGA, outside vendors, or local educational institutions. Continuing training topics should also address identified weaknesses in the knowledge or skills of the individual personnel.

2. Actively perform the duties of a security specialist at a DOE facility.

3. Attend seminars, symposia, or technical meetings related to S&S.

4. Engage in self-study of new regulations, requirements, or advances related to S&S.

5. Participation in practical exercises such as emergency or operational drills, simulations, or laboratory-type exercises.

6. Specific continuing training requirements must be documented in Individual Development Plans (IDPs).

7. Participate in a rotational assignment at another DOE site/facility or at Headquarters in the S&S area.

INTENTIONALLY BLANK

DOE-STD-1171-2009

CONCLUDING MATERIAL

Review Activity:
EM
NNSA
NE
SC

Preparing Activity:
NA-70

Project Number:
TRNG-0067

Field and Operations Offices:
CBFO
CH
ID
ORO
ORP
RL
SR

Site Offices:
Argonne Site Office
Brookhaven Site Office
Fermi Site Office
Kansas City Site Office
Livermore Site Office
Los Alamos Site Office
NNSA Service Center
Nevada Site Office
Pantex Site Office
Savannah River Site Office
Sandia Site Office
Y-12 Site Office