DOE - EM - SRP - 2010
2nd Edition

Environmental Management
Safety ▪ Performance ▪ Cleanup ▪ Closure

Standard Review Plan (SRP)

Safeguards and Security and Cyber Security Review Module

Corporate Critical Decision (CD) Review and Approval Framework Associated with Nuclear Facility Capital and Major Construction Projects

March 2010

Office of Environmental Management
U.S. Department of Energy
Washington D. C. 20585

OFFICE OF ENVIRONMENTAL MANAGEMENT

Standard Review Plan (SRP)

Safeguards and Security and Cyber Security

Review Module

Critical Decision (CD) Applicability					
CD-0	CD-1	CD-2	CD-3	CD-4	Post Operation
✓	✓	✓	✓	✓	✓

March 2010

FOREWORD

The Standard Review Plan (SRP)[1] provides a consistent, predictable corporate review framework to ensure that issues and risks that could challenge the success of Office of Environmental Management (EM) projects are identified early and addressed proactively. The internal EM project review process encompasses key milestones established by DOE O 413.3A, Change 1, *Program and Project Management for the Acquisition of Capital Assets*, DOE-STD-1189-2008, *Integration of Safety into the Design Process*, and EM's internal business management practices.

The SRP follows the Critical Decision (CD) process and consists of a series of Review Modules that address key functional areas of project management, engineering and design, safety, environment, security, and quality assurance, grouped by each specific CD phase.

This Review Module provides the starting point for a set of corporate Performance Expectations and Criteria. Review teams are expected to build on these and develop additional project-specific Lines of Inquiry, as needed. The criteria and the review process are intended to be used on an ongoing basis during the appropriate CD phase to ensure that issues are identified and resolved.

[1] *The entire EM SRP and individual Review Modules can be accessed on EM website at http://www.em.doe.gov/Pages/Safety.aspx , or on EM's internet Portal at https://edoe.doe.gov/portal/server.pt Please see under /Programmatic Folder/Project Management Subfolder.*

TABLE OF CONTENTS

ACRONYMS

CD	Critical Decision
DBT	Design Basis Threat
DOE	Department of Energy
FPD	Federal Project Director
IPT	Integrated Project Team
LOI	Lines of Inquiry
RM	Review Module
SDS	Safety Design Strategy
SME	Subject Matter Expert
SRP	Standard Review Plan
SSCS	Safeguards and Security and Cyber Security
TL	Threat Level
VA	Vulnerability Assessment

I. INTRODUCTION

As required by DOE O 413.3A, Change 1, *Program and Project Management for the Acquisition of Capital Assets*, Safeguards and Security Requirements and Cyber Security (SSCS) requirements must be identified and integrated into a project early in the Critical Decision (CD) phases. Their implementation is assessed through design, construction, readiness review, operations, and eventual decommissioning. Establishing and integrating SSCS requirements early is necessary for project planning and cost estimating to prevent project impacts that can be expected when SSCS requirements are identified late into the CD phases. DOE O 413.3A invokes the 205 and 470 series of DOE Directives regarding safeguards and security, and cyber security. Also, this Safeguards and Security and Cyber Security (SSCS) Review Module (RM) amplifies the guidance provided in DOE G 413.3-3, *Safeguards and Security for Program and Project Management,* along with the DOE requirements.

It should be noted this RM only addresses the non-classified portion of the review process. The Federal Project Director and appropriate DOE/EM-HQ line management and security representatives must coordinate the classified related security reviews.

II. PURPOSE OF THE REVIEW MODULE

The SSCS RM is a tool that assists the DOE federal project review teams in evaluating the technical sufficiency of the project SSCS activities at CD-0 through CD-4. Additionally, this RM provides broad SSCS guidance to:

- Federal Project Directors (FPD), federal program and site office, and project review teams in identifying and implementing key safeguards and security components of the projects and integrating SSCS considerations into each CD phase.

- Define security project’s features and functions as developed or required by the security program or security policy which minimizes impact on operations.

- Identify the function of the federal site security program representative who serves as security design point of contact for security features and is a member of the Integrated Project Team as appropriate during the entire project cycle**.**

- Facilitate communication and interaction between the site security professionals, other integrated project teams, and the members of the project design team.

- Identify the importance of interface and coordination between the security and safety professionals to ensure both SSCS and safety requirements are met.

III. ROLES AND RESPONSIBILITIES

A critical element of the SSCS review is the qualifications, training and most importantly the experience of the personnel selected to conduct the review. To the maximum extent possible, the personnel selected to participate in the reviews should have "on the ground", first hand experience (as opposed to an oversight role) in SSCS. The table below provides a compilation of SSCS review roles and responsibilities.

Position	Responsibility
Field Element Manager	Provides support and resources to the FPD and Review Team Leader in carrying out the SSCS review. This review can be conducted in conjunction with other project reviews, including design, construction, commissioning, and readiness reviews.
	Facilitates the conduct of the SSCS review. Assigns office space, computer equipment, and support personnel to the team as necessary to accomplish the review in the scheduled time frame
Federal Project Director	Coordinates with the Review Team Leader in the selection of technical areas for the review and in developing the review criteria.
	In conjunction with the Contractor Project Manager, develops the briefing materials and schedule for the review activities.
	Coordinates the review team pre-visit activities and follows up review team requests for personnel to interview or material to review.
	Coordinates the necessary training and orientation activities to enable the review team members to access the facility and perform the review.
	Unless other personnel are assigned, acts as the site liaison with the review team. Tracks the status of requests for additional information.
	Coordinates the Federal site staff factual accuracy review of the draft report.
	Leads the development of the corrective action plan if required. Tracks the corrective actions resulting from the review.
Review Team Leader	In coordination with the Federal Project, selects the areas to be reviewed.
	Based on the project size, complexity and hazards involved, selects the members of the review team.
	Verifies the qualifications: technical knowledge; process knowledge; facility specific information; and independence of the Team Members.
	Leads the SSCS review pre-visit, if needed.
	Leads the review team in completing the Lines of Inquiry for the various areas to be reviewed.
	Coordinates the development of and forwards to the Federal Project Director, the data call of documents, briefings, interviews, and presentations needed for the review.
	Forwards the final review plan to the Field Element Manager for approval
	Leads the on-site portion of the review.
	Ensures the review team members complete and document their portions of the review. Coordinates the characterization of the significance of the findings.
	Coordinates the review team handling of factual accuracy comments by Federal and Contractor personnel on the draft report.

Position	Responsibility
	Remains available as necessary to participate in the closure verification of the findings from the review report.
Review Team Member	Refines and finalizes the Lines of Inquiry for the appropriate area of the review.
	Develops and provides the data call of documents, briefings, interviews, and presentations needed for his or her area of the review.
	Completes training and orientation activities necessary for the review. Conducts any necessary pre visit document review.
	Participates in the on-site review activities, conducts interviews, document reviews, walk downs, and observations as necessary.
	Based on the criteria and review approaches in the Review Plan, assesses whether his or her assigned criteria have been met.
	Documents the results of the review for his or her areas. Prepares the review report.
	Makes recommendations to the Review Team Leader for characterization of findings in his or her area of review.
	Resolves applicable Federal and Contractor factual accuracy comments on the draft review report.
	Prepares the final review report for his or her area of review.
	Concurs in the findings for his or her area of the review.

IV. REVIEW SCOPE AND CRITERIA

The scope of the SSCS RM is focused on the requirements and guidance of DOE O 413.3A and supporting DOE G 413.3-3 and those established in the 470 series of DOE Directives for safeguards and security, and the 205 series of DOE Directives for cyber security. This RM provides the review team with a “straw-man” template from which they may derive and pursue Lines of Inquiry that are applicable to the specific projects. The scope of the SSCS RM is captured by performance objectives and criteria that are presented in several broad categories listed below. For each category, Appendix A of this RM provides overall performance objectives and criteria that satisfy each performance objective. Some of the performance objectives and criteria in Appendix A are broad scope in nature since project-specific design basis threat assessments and other associated requirements and guidance may constitute classified information. The classified portion of the security review is not a part of this review module.

These performance objectives and review criteria will provide consistent guidance to review teams to develop their project-specific Lines of Inquiry. The selection of the review categories should be tailored to the specific project. The review teams may develop additional review categories based on the review of the DOE Directives.

Critical Decisions Requirements/Guidance

This review area focuses on how the SSCS requirements/guidance should be integrated into the Critical Decision (CD) activities from CD-0 through CD-4. The inclusion of SSCS principles should be implemented during pre-conceptual planning, conceptual design, preliminary design, final design, construction, and commissioning of the new projects and modifications of the existing projects.

Safety Interface

The review area focuses on the integration process which assures that both the SSCS and safety requirements are met. The SSCS and safety professionals should work together early in the design process to allow achievement of the Design Basis Threat (DBT) objectives while ensuring safety is appropriately considered.

Threat Description and Target Identification

This review area focuses on the compliance with DOE O 470.3B, if appropriate, regarding DBT and Threat Level.

Protection Strategies

This review area focuses on the development and implementation of the project protection strategies for areas such as Government property protection, terrorist, and personnel and vehicle inspection. Protection strategies requirements are defined in the 470 series of DOE Directives.

Physical Protection

This review area focuses on the development and implementation of physical protection as required by the 470 series of DOE Directives.

Protective Force

This review area focuses on the establishment and implementation of physical protection as required by the 470 series of DOE Directives. It may be more important during later stage of the acquisition process during construction, commissioning and pre-operations.

Material Control and Accountability

This review area focuses on the establishment and implementation of a Material Control and Accountability requirements in DOE M 470.4-6, Change 1.

Personal Security

This review area focuses on personnel security as required by DOE M 470.4-5 to assure the insider threat to the project is minimized.

Cyber Security

This review area focuses on information and cyber security as required by both 205 and 470 series of DOE Directives.

Safeguards and Security Equipment, Maintenance and Testing

This review area focuses on the testing of critical security and surveillance systems as required by DOE O 470.4A. This review area is probably more relevant during construction and commissioning phases of the project.

Reporting Security Incidents and Concerns

This review area focuses on the timely reporting of security incidents and concerns as required by DOE M 470.4-1.

V. REVIEW PLANS AND DOCUMENTATION

The results of a SSCS review will be used by the DOE FPD and ultimately the Acquisition Executive to help determine whether project funds may be authorized at each Critical Decision approval stage. It is important to clearly document the methods, assumptions and results of the SSCS review. This review can be conducted as part of other project reviews, such as part of the design, engineering, technology, construction, and readiness reviews. The Standard Review Plan (SRP) provides guidelines for preparing a Review Plan and a final report.

The following activities should be conducted as part of the Review Plan development and documentation or closure of the review:

- Subsequent to the selection, formation and chartering of the review team and receipt and review of the prerequisite documents, assignment of responsibilities for the development of specific LOIs should be made.
- The review team members should develop specific LOIs using the topics and areas listed in the Appendix A of this module.
- The individual LOIs should be compiled and submitted to the review team leader authorizing the review for concurrence prior to starting the review.
- The project-specific review plan should be compiled with a consistent and uniform numbering scheme that provided for a unique identifier for each line of inquiry, arranged by subject area such that the results of each LOI can be documented and tracked to closure.
- The LOIs should be satisfied via document review and personnel interviews and any combination of these methods. The method used the basis for closure/comment/finding and the result of the inquiry should all be documented and tracked.

VI. REFERENCE MATERIAL[2]

- 42 U.S.C. 7144a, *Establishment of Security, Counterintelligence, and Intelligence*
- 41 CFR 102-74, *Facility Management*
- 48 CFR 952.204-2, *Security Requirements*
- DOE O 413.3A, Change 1, *Program and Project Management for the Acquisition of Capital Asset*s, 11-17-2008
- DOE G 413.3-3, *Safeguards and Security for Program and Project Management*, 11-15-07
- DOE-STD-1189, *Integration of Safety into the Design Process*, 03-08
- DOE P 470.1, *Integrated Safeguards and Security Management (ISSM) Policy*. 05-08-01
- DOE N 470.4, *Reciprocal Recognition of Existing Personnel Security Clearances/Access Authorizations*, 1-09-09
- DOE O 470.2B, Independent Oversight and Performance Assurance Program, 10-31-02
- DOE O 470.3B, *Graded Security Protection (GSP) Policy*, 08-12-08
- DOE O 470.4A, *Safeguards and Security Program*, 05-25-07
- DOE M 470.4-1 Chg 1, *Safeguards and Security Program Planning and Management*, 08-26-05
- DOE G 470.4-1, *Asset Protection Analysis Guide*, 08-21-08
- DOE M 470.4-2 Chg 1, *Physical Protection*, 08-26-05
- DOE M 470.4-3 Chg 1, *Protective Force*, 08-26-05
- DOE M 470.4-3A, *Contractor Protective Force*, 11-05-08
- DOE M 470.4-4A, *Information Security Manual*, 01-16-09
- DOE M 470.4-3A , *Contractor Protective Force*, 11-05-08
- DOE M 470.4-5, *Personnel Security*, 08-26-05
- DOE M 470.4-6 Chg 1, *Nuclear Material Control and Accountability*, 08-26-05
- DOE M 470.4-7, *Safeguards and Security Program References*, 08-26-05
- DOE O 471.1A, *Identification and Protection of Unclassified Controlled Nuclear Information*, 06-30-00
- DOE M 471.1-1 Chg 1, *Identification and Protection of Unclassified Controlled Nuclear Information Manual*, 10-23-01
- DOE M 471.2-3B, *Special Access Program Policies, Responsibilities, and Procedures*, 10-29-07

[2] *This Review Module only addresses the non-classified portion of the review process. The Federal Project Director and appropriate DOE/EM-HQ line management and security representatives must coordinate the classified related security reviews.*

- DOE O 471.3, *Identifying and Protecting Official Use Only Information*, 04-09-03
- DOE M 471.3-1, *Manual for Identifying and Protecting Official Use Only Information*, 04-09-03
- DOE G 471.3-1, *Guide to Identifying Official Use Only Information*, 04-09-03
- DOE G 473.2-1, *Guide for Establishment of a Contingency Protective Force*, 03-27-03
- DOE P 205.1, *Departmental Cyber Security Management Policy*, 05-08-01
- DOE O 205.1A, *Department of Energy Cyber Security Management*, 12-04-06
- DOE M 205.1-3, *Telecommunications Security Manual*, 04-17-06
- DOE M 205.1-4, *National Security System Manual*, 03-08-07
- DOE M 205.1-5, *Cyber Security Process Requirements Manual*, 08-12-08
- DOE M 205.1-6, *Media Sanitization Manual*, 12-23-08
- DOE M 205.1-7, *Security Controls for Unclassified Information Systems Manual*, 01-05-09
- DOE M 205.1-8, *Cyber Security Incident Management Manual*, 01-08-09

APPENDIX A - PERFORMANCE OBJECTIVES AND CRITERIA

Legend of Safeguards and Security Review Topics

Review Topical Area	**Identifier**
Critical Decision Requirements/Guidance	CR
Safety Interface	SI
Threat Description and Target Identification	TD
Protection Strategies	PR
Physical Protection	PP
Protective Force	PF
Material Control and Accountability	MC
Personal Security	PS
Cyber Security	CS
Safeguards and Security Equipment, Maintenance and Testing	SE
Reporting Security Incidents and Concerns	RS

ID #	**Performance Objectives and Criteria**[3]	**Met?**
Critical Decision Requirements and Guidance		
CD-0	Prior to Critical Decision-0, has the project integrated the SSCS requirements and disciplines into the pre-conceptual planning and mission need determination as required by DOE O 413.3A, Change 1?	
	Has the SSCS subject matter experts (SMEs) been designated by the site and/or program office manager to support the project? **(CD-0.1)**	
	Has the evaluation begun on the potential security needs in regards to the design basis threat? **(CD-0.2)**	
	If the preliminary security evaluation indicates the project is classified, has the level of security and the associated requirements been identified? **(CD-0.3)**	
	Have the SSCS SMEs initiated project activities, including coordination with other disciplines (such as project management, safety and engineering)? **(CD-0.4)**	
CD-1	Prior to Critical Decision-1, has the project continued the integration the SSCS requirements and activities into the conceptual design development?	
	For project classified as security categories I or II, has a Vulnerability Assessment (VA) been conducted and recommendations made regarding physical security, protective force, cyber security, and/or administrative controls based on identified security risks? **(CD-1.1)**	
	Has the SSCS assessments been integrated into the conceptual design and cost estimates? **(CD-1.2)**	

[3] The site should provide the technical bases and assumptions that support the answers provided to each Line of Inquiry. If possible, the review teams should independently verify the technical bases and assumptions.

ID #	Performance Objectives and Criteria[3]	Met?
	Have the SSCS SMEs continued coordination with other project activities, including other disciplines, such as project management, safety and engineering? **(CD-1.3)**	
CD-2	Prior to Critical Decision-2, has the project continued the integration of SSCS requirements and activities into the preliminary design development?	
	Are the SSCS SMEs working closely with the Integrated Project Team (IPT), or part of the IPT, to ensure that SSCS principles and activities are part of the preliminary design? **(CD-2.1)**	
	Has a VA been refined and recommendations made regarding physical security, protective force, cyber security, and/or administrative controls based on identified security risks? **(CD-2.2)**	
	Has the SSCS assessments been integrated into the preliminary design and cost estimates? **(CD-2.3)**	
	Have security-related training strategies been initiated? **(CD-2.4)**	
	Have security-related operational strategies been initiated? **(CD-2.5)**	
	Does the project Performance Baseline appropriately address the cost, schedule and integration aspects of SSCS? **(CD-2.6)**	
CD-3	Prior to Critical Decision-3, has the project continued SSCS activities into the final design and preparation for construction?	
	Have the SSCS SMEs been working closely with the IPT, or part of the IPT, to ensure that SSCS principles and activities are part of the final design? **(CD-3.1)**	
	Has a VA been refined and recommendations made regarding physical security, protective force, cyber security, and/or administrative controls based on identified security risks? **(CD-3.2)**	
	Has the SSCS assessments been integrated into the final design and cost estimates? **(CD-3.3)**	
	Have security-related training development continued? **(CD-3.4)**	
	Have testing requirements and acceptance criteria been prepared and implemented for security systems? **(CD-3.5)**	
CD-4	Prior to Critical Decision-4, has the project continued SSCS activities during commissioning and closeout phase prior to operations?	
	Has the Final VA Report prepared? **(CD-4.1)**	
	Has operations readiness review for security been conducted? **(CD-4.2)**	
	Has SSCS training been conducted for the operations work force? **(CD-4.3)**	
	Are there approved security plans and procedures for operations? **(CD-4.4)**	
Safety Interface		
SI-1	Are security and safety professionals interfacing to identify and resolve any potential conflicts and/or identify risks that can impact safety, security, and project costs?	
SI-2	Is safety and security interface occurring to meet and resolve the Design Basis Threat (DBT) objectives while ensuring safety is appropriately considered?	
SI-3	Is security Vulnerability Assessment being performed, beginning early in the design and continued updating through the final design?	
SI-4	Are recommendations from the Vulnerability Assessments being incorporated into safety-in-design decisions, including the need for new technologies, or incorporating of new technologies, and factors into the safety bases analyses?	
SI-5	Is the strategy for security design documented and incorporated, as appropriate, into the Safety Design Strategy (SDS)?	

ID #	Performance Objectives and Criteria[3]	Met?
SI-6	Is security and worker safety interface occurring to assure that workers and safety professionals can enter and exit the facility during emergency situations?	
Threat Description and Target Identification		
TD-1	Has the project applied the requirements of DOE O 470.3B, *Graded Security Protection Policy*?	
TD-2	Has the project determined the Design Basis Threat (DBT) Threat Level (TL)?	
TD-3	Has all the security targets been identified, including government and private property, UCI, unclassified cyber systems, and People?	
TD-4	Are there radiological, chemical, and biological sabotage targets identified for the project?	
Protection Strategies		
PR-1	Has the project established protection strategies as required by the 470 series of DOE Directives?	
PR-2	Have protection strategies been developed, such as using access control procedures, information compartmentalization, physical barriers, locks and keys, material controls, employee awareness, and training for areas such as Government property; unauthorized entry, trespass, site intruder, or terrorist; emergency response, and personnel and vehicle inspection?	
Physical Protection		
PP-1	Has the project established and implemented physical protection requirements established by the 470 series of DOE Directives?	
Protective Force		
PF-1	Has the project incorporated and implemented Protective Force requirements established by the 470 series of DOE Directives?	
Material Control and Accountability		
MC-1	If appropriate, has the project incorporated and implemented Material Control and Accountability requirements established by the 470 series of DOE Directives, specifically, DOE M 470.4-6, Change 1?	
Personnel Security		
PS-1	Has the project incorporated and implemented Personnel Security requirements established by the 470 series of DOE Directives, specifically, DOE M 470.4-5?	
PS-2	Is insider threat to the project being minimized using security measures such as badging, pre-employment investigation and fitness for duty, training, and security awareness?	
Cyber Security		
CS-1	Has the project incorporated and implemented cyber security requirements established by both 205 series and 470 series of DOE Directives?	
Safeguards and Security Equipment, Maintenance and Testing		
SE-1	Are critical security and surveillance systems and devices being tested as required by DOE O 470.4A?	
Reporting Security Incidents and Concerns		
RS-1	Does the project have procedures on reporting of incidents security concern within specific timelines based on actions, inactions, or events as defined in DOE M 470.4-1?	