NOT MEASUREMENT SENSITIVE

DOE G 413.3-3
11-15-07

SAFEGUARDS AND SECURITY FOR PROGRAM AND PROJECT MANAGEMENT

[This Guide describes suggested nonmandatory approaches for meeting requirements. Guides are not requirements documents and are not to be construed as requirements in any audit or appraisal for compliance with the parent Policy, Order, Notice, or Manual.]

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

AVAILABLE ONLINE AT:
www.directives.doe.gov

INITIATED BY:
Office of Health, Safety and Security

FOREWORD

This Department of Energy (DOE) Guide is for use by all DOE elements.

Beneficial comments (recommendations, additions, and deletions) and any pertinent data that may improve this document should be sent to the Director, Office of Policy, U.S. Department of Energy, Washington, DC 20585, by letter or by sending the self-addressed Standardization Document Improvement Proposal (DOE F 1300.3).

This Guide is intended to provide approaches for implementing the safeguards and security requirements of DOE O 413.3A, *Program and Project Management for the Acquisition of Capital Assets*. DOE Guides, which are part of the DOE Directives Program, provide supplemental information for fulfilling requirements contained in rules, regulatory standards, and DOE directives. Guides do not establish or invoke new requirements nor are they substitutes for requirements.

CONTENTS

SECTION I. INTRODUCTION I-1
1. GOAL I-1
2. SCOPE I-1
3. OBJECTIVES I-1
4. APPLICABILITY I-1
SECTION II. ROLES AND RESPONSIBILITIES II-1
1. FEDERAL PROGRAM/SITE OFFICE MANAGER II-1
2. FEDERAL PROJECT DIRECTOR) II-1
3. SITE SECURITY PROGRAM REPRESENTATIVES II-1
4. OTHER INTEGRATED PROJECT TEAM MEMBERS II-2
5. SITE CONTRACTOR PROJECT MANAGER II-2
6. SITE CONTRACTOR SECURITY REPRESENTATIVE II-2
7. HQ SECURITY PROGRAM OFFICES II-2
SECTION III. SAFEGUARDS AND SECURITY PROGRAM BACKGROUND III-1
SECTION IV. DESIGN CONSIDERATIONS AND INTERFACES IV-1
1. BASIS FOR DESIGN STANDARDS IV-1
2. FACILITY AND PHYSICAL PROTECTION STANDARDS IV-1
3. SECURITY SYSTEM DESIGN IV-1
4. SECURITY SYSTEM ALTERNATIVES EVALUATION IV-2
SECTION V. SAFEGUARDS & SECURITY AND THE CRITICAL DECISION PROCESS V-1
1. INITIATION PHASE (PRE-CONCEPTUAL PLANNING— PRE-CRITICAL DECISION-0) V-1
2. DEFINITION PHASE (CONCEPTUAL DESIGN— POST CRITICAL DECISION-0) V-1
3. EXECUTION PHASE I (PRELIMINARY DESIGN PHASE) V-3
4. EXECUTION PHASE II (FINAL DESIGN PHASE AND CONSTRUCTION) V-4
5. TRANSITION/CLOSEOUT PHASE/OPERATION PHASE V-5
ATTACHMENT 1. SAFEGUARDS AND SECURITY PROJECT CHECKLIST
ATTACHMENT 2. REFERENCES

SECTION I. INTRODUCTION

1. GOAL. To ensure that safeguards and security requirements are identified and integrated into a project early and that their implementation is assessed throughout the project life cycle. Protection strategy for an asset should include consideration of the threat to the asset as a fundamental part of the design process. Establishing and integrating safeguards and security requirements early is necessary for project planning and cost estimating and to prevent project impacts that can be expected when safeguards and security requirements are identified late into the design process, construction, or as part of the operational readiness review. Additionally, due to potential conflicts in meeting safeguards and security requirements and the requirements of other critical disciplines (e.g., safety), the integration of all requirements is critical to developing the best overall cost effective solution for the project.

2. SCOPE. This Guide addresses the implementation steps for achieving safeguards and security systems that support the Department's protection objectives. It provides a logical process for the implementation of accepted safeguards and security principles, which are translated into system requirements and configuration with an auditable cost and schedule; from project/program initiation through the transition/closeout phases.

3. OBJECTIVES.

   a. To provide safeguards and security advice to Federal project directors and federal program/site office managers (contractors and subcontractors as applicable) in identifying and implementing key safeguards and security components of their projects and integrating safeguards and security consideration into each acquisition management phase (initiation, definition, execution and transition/closeout).

   b. To define security project's features and functions as developed or required by the security program or security policy which minimizes impact on operations.

   c. To 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**.**

   d. To facilitate communication and interaction between the site security professionals, other integrated project teams, and the members of the project design team.

4. APPLICABILITY. This guide applies to all DOE elements, including the National Nuclear Security Administration (NNSA), which fund, direct and manage acquisition projects as defined by DOE O 413.3A.

   As used in this guide, "security" refers to both safeguards and security as it is applicable to the project or facility regardless of the type of building, structure, or facility and whether new or a modification.

This Guide provides approaches for implementing security provisions within the security functional areas as specified in DOE O 413.3A, *Program and Project Management for the Acquisition of Capital Assets*.

The DOE G 413.3-X series provides companion supplemental project management guidance. Specific regulatory citations are provided in the body of the Guide. This Guide provides explanations and examples for implementing requirements of DOE O 413.3A.

Except for requirements established by a regulation, contract, or administrative means, the provisions in this Guide are DOE's views on acceptable methods of program implementation and are not mandatory. Conformance with this Guide should, however, create an inference of compliance with the related requirements. Alternative methods that are demonstrated to provide an equivalent or better level of protection are acceptable. DOE encourages its contractors to go beyond the minimum requirements and to pursue excellence in their programs.

The words "should" and "may" are used to denote optional program recommendations and allowable alternatives, respectively. This Guide is applicable to all DOE activities that are subject to the requirements of DOE O 413.3A.

SECTION II. ROLES AND RESPONSIBILITIES

1. FEDERAL PROGRAM/SITE OFFICE MANAGER.

   a. Ensures that the Federal project director has adequate support on the federal integrated project team and access to other project specific support as needed throughout the project life cycle for safeguards and security.

   b. Approves the integrated project team membership and ensures that the identified individuals have adequate time to devote to the task.

   c. Approves change control actions at the levels agreed upon in the project execution plan, including security scope changes.

   d. Approves security project's management documents as stipulated in the project execution plan.

2. FEDERAL PROJECT DIRECTOR.

   a. As head of the integrated project team, relies on team members to help identify requirements and security issues.

   b. Works with integrated project team members to assure cost effective integration of security with safety and other project areas.

   c. Works with the contractor project manager and integrated project team representatives and design team to resolve security issues in an effective and efficient manner.

   d. Integrates safeguards and security requirements into project documents.

   e. Approves changes within control ranges set in the security project execution plan.

3. SITE SECURITY PROGRAM REPRESENTATIVES.

   a. Represent the security interests of the site and are points of contact for security on the integrated project team.

   b. Responsible for ensuring that safeguards and security concerns and criteria are identified.

   c. Works with the Federal project director, contractor project manager, and contractor site security representatives to monitor incorporation of security requirements into the design and construction of a project.

   d. Participate in/lead in facility security vulnerability assessments and/or risk analysis.

e. Review design documents (i.e., safety), operations procedures, and readiness assessments.

f. Concur in security operations procedures for facilities being built.

g. Monitor any changes to site operational requirements which may affect security project's approved baseline.

4. OTHER INTEGRATED PROJECT TEAM MEMBERS represent their disciplines and work to ensure that design and construction incorporate the security area concerns and requirements.

5. SITE CONTRACTOR PROJECT MANAGER.

a. Implements the design and construction activities for security.

b. Works with the Federal project director and integrated project team to ensure that security project requirements are being met.

c. Approves changes within control ranges set in the project execution plan.

d. Ensures that plans developed in the previous phase and increasing maturity of planning be implemented throughout the project life cycle.

6. SITE CONTRACTOR SECURITY REPRESENTATIVE works with site project manager to ensure that security requirements and issues are being properly represented and resolved.

7. HQ SECURITY PROGRAM OFFICES.

a. Provide assistance in the areas of guidance and expert opinion in the resolution of security requirements, issues, and technologies.

b. Exercise project oversight responsibilities and monitors the program requirements as outlined in the program requirements document and the project execution plan.

SECTION III. SAFEGUARDS AND SECURITY PROGRAM BACKGROUND

All DOE facilities are evaluated for potential risks to employees, the public, and the environment. DOE M 470.4 series directives contain requirements for determining the level of protection, based on facility functions and potential security risks and design basis threat requirements. This also includes Cyber Security under the provisions of DOE O 205.1A *Department of Energy Cyber Security Management.*

A preliminary security review should be initiated during the project conceptual design phase and further developed during the preliminary and final design phases. In most situations, these reviews are included in the project planning and design documentation (e.g., in conceptual design reports, or critical decisions). Facility design and construction features, identified as a result of security review, should be factored into the conceptual design before establishing the project cost estimate and requesting funding authorization for design and construction.

An appropriate security plan should be completed and approved prior to the start of construction (including site preparation), consistent with DOE M 470.4-1, *Safeguards and Security Program Planning and Management*. The plan should be updated as appropriate to reflect changes affecting security that are made to the facility during its lifetime.

DOE assets are defined and protection standards outlined in DOE O 470.3A, *Design Basis Threat Policy* (U). Depending on the asset being protected, protection strategies range from a combination of compliance with DOE security policies to specific performance standards that should be met. This constitutes a graded and risk-based approach ensuring the highest levels of protection for those assets where loss, theft, compromise, and/or unauthorized use would seriously affect national security, the environment, Departmental programs, and/or public/employee health and safety.

For those assets designated as Threat Level 1, 2, or 3, the Federal project director should reference the design basis threat policy because additional performance-based security measures may necessitate a vulnerability assessment to be performed by the site to determine what additional security measures are necessary to achieve an integrated protection system consisting of sensing, assessment, communication, response, interruption, and neutralization.

The DOE O 470 series of directives establishes minimum design principles. Adherence to these directives should provide reasonable assurance that safeguards and security designs embellish the DOE tenets of providing graded security and establishing defense in-depth. For example, a security area denotes a physically defined space containing departmental security assets and subject to physical protection and access controls. Security areas are established per the requirements of DOE M 470.4-2, *Physical Protection.*

The type of security area established depends on the nature of the security interests to be protected, with the following types required for the protection of the listed security interests. These are—

- property protection area,

- limited area,
- exclusion area,
- protected area,
- material access area, and
- vital area.

The property protection area (an office building or administrative area) is the least restrictive area, and the most restrictive is a material access area which is located within a protected area. The descriptions are provided in DOE M 470.4-7, *Safeguards and Security Program References*.

DOE safeguards and security programs are established through DOE 470 series Orders and Manuals. The following are Safeguards and Security Orders and Manuals that are most applicable to projects.

- DOE O 470.3A, *Design Basis Threat Policy* (U), dated 11-29-05;
- DOE O 470.4A, *Safeguards and Security Program, Performance Assurance*, dated 5-25-07;
- DOE M 470.4-1, Chg 1, *Safeguards and Security Program Planning and Management*, dated 8-26-05;
- DOE M 470.4-2, Chg 1, *Physical Protection*, dated 8-26-05;
- DOE M 470.4-4, Chg 1, *Information Security*, dated 8-26-05; and
- DOE M 470.4-6, Chg 1, *Nuclear Material Control and Accountability*, dated 8-26-05.

In projects, the identification and protection of Unclassified Controlled Nuclear Information is specified in the follow directives:

- DOE P 470.1, *Integrated Safeguards and Security Management (ISSM) Policy,* dated 5-8-01;
- DOE O 471.1A, *Identification and Protection of Unclassified Controlled Nuclear Information,* dated 6-30-00; and
- DOE M 471.1-1, Chg. 1, *Identification and Protection of Unclassified Controlled Nuclear Information Manual,* dated 10-23-01.

Also for unusual or special conditions the following directive provides the construction requirements for the protection of classified information requiring extraordinary security protection.

> Director of Central Intelligence Directives 6/9, *Physical Security Standards for Sensitive Compartmented Information Facilities*, 11-18-02

Additionally, program office specific guidance (if any) should be referenced in the design and construction of security related projects.

SECTION IV. DESIGN CONSIDERATIONS AND INTERFACES

1. BASIS FOR DESIGN STANDARDS.

   a. DOE security assets are to be protected from theft or diversion, sabotage, espionage, loss or theft of classified matter or government property, and other hostile acts which could cause unacceptable adverse impacts on national security, program continuity, or the health and safety of employees, the public, or the environment.

   b. Levels of protection appropriate to particular safeguards and security interests are to be provided in a graded fashion in accordance with potential risks to national security and the health and safety of employees and the public.

   c. Protection programs are tailored to address site-specific characteristics on the basis of DOE directives and other requirements.

   d. Site-specific protection programs describing the implementation of these requirements are documented in protection program plans and/or site security plans.

2. FACILITY AND PHYSICAL PROTECTION STANDARDS.

   a. Planning, design, and installation of security systems should be determined in consultation with the cognizant DOE security authority and should be consistent with security policies.

   b. A key role of the security professional assigned to the project team as part of the integrated project team should be to ensure that the best approach to meeting policy objectives are identified.

   c. The approach should provide a security solution that maintains compliance with requirements and provides effective security, while minimizing security's impact on project cost, potential safety concerns, and operational impacts.

3. SECURITY SYSTEM DESIGN. The basis for each discipline standard should be addressed.

   a. For example, DOE nuclear safety directives do not address malevolent acts, sabotage, or terrorist activities, while security requirements are focused primarily on such actions. However, successful design accounts for all requirements within the area's applicability and expected environmental conditions for the system to operate.

   b. Design should necessitate accommodating potential interactions and overlaps among applicable requirements, such as those that might be encountered between postulated security technologies and normal operation or accident conditions, such as those required to be evaluated for life safety.

c. Controls should be established to prevent unauthorized access to security areas, unauthorized activities within security areas, and removal of security interests. Where there are conflicts between the security requirements and those of other disciplines, these need to be defined as early in the project as practicable, so as to provide the time to reach the best overall solution to all requirements. For example:

(1) Although building access points are often minimized for security reasons, personnel egress from security areas should meet the requirements of National Fire Protection Association 101 and the applicable portions of the project building code (e.g., International Building Codes or National Fire Protection Association 5000).

(2) Entrances to and exits from security areas should be designed for efficient, yet controlled, movement of personnel or vehicles through designated portals.

(3) Due to the security limitations on exiting certain buildings, alternative life safety approaches, such as a safe haven, based on performance based compliance with the National Fire Protection Association requirements, may be necessary to meet the requirements of both disciplines.

(4) External and internal areas within security boundaries should be provided with infrastructure support (e.g., electrical power, alarm communications and control systems).

4. SECURITY SYSTEM ALTERNATIVES EVALUATION.

a. During the conceptual and preliminary design phase, alternatives analysis of the security system is performed along with the other major activities of the project, including the security implications of the various proposed sites.

b. To ensure consideration of all alternatives appropriate to the significance of the threat, the project team should consult departmental programs supporting the development or deployment of security technologies. Currently these include the DOE Office of Health, Safety and Security and the NNSA Chief, Defense Nuclear Security. These organizations should be able to provide technical and contact information for security technologies being developed, tested, or deployed by the Department or other agencies of the United States. Care should be taken to avoid new untested systems. They should not be installed at DOE facilities unless there is a conscious decision that the site should be a field test facility for those systems.

c. Project teams may request technical assistance from their cognizant security authority offices. Communication is essential to ensure that the facility is able to receive the technology and that its deployment is appropriate for the facility.

SECTION V. SAFEGUARDS & SECURITY AND THE CRITICAL DECISION PROCESS

Figure V-1 depicts the overall timeline of a project. The key security tasks associated with each project phase are presented in Table V-1, Overarching Areas of Consideration. Note that these tasks need to be finished to complete the phase and support the Critical Decision. However, it is important to start these efforts early in the phase, providing time for project interaction in support of these tasks and to address project changes they drive.

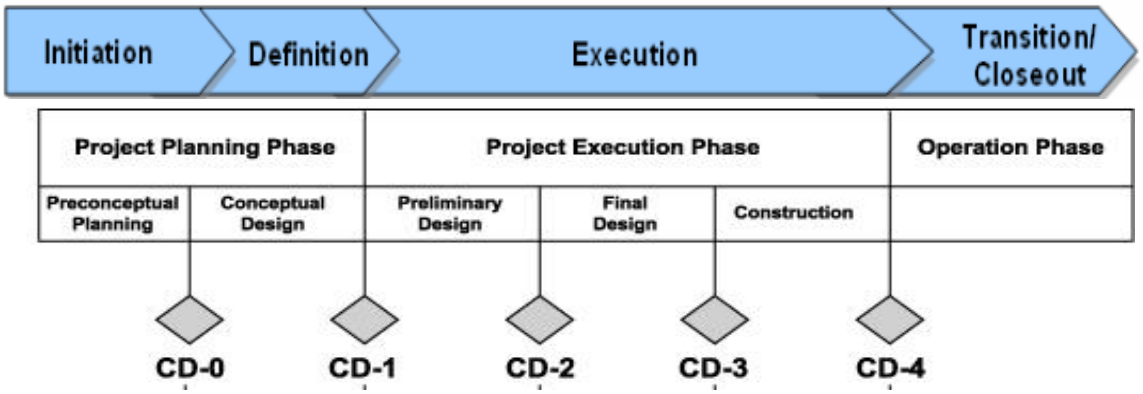

Figure V-1 Typical DOE Project Timeline

1. INITIATION PHASE (PRE-CONCEPTUAL PLANNING—PRE-CRITICAL DECISION-0).

   For all projects, an early evaluation of probable security concerns and design basis threat assessment should be made by the federal program/site office manager. The site security office and contractor's security office should evaluate the potential security needs of the project in regards to the design basis threat. When indicated by this evaluation, a security professional for the project should be identified to serve as technical advisor and integrated project team member on security matters for the life of the project.

   If this preliminary security evaluation indicates that the project is classified, the DOE site office manager and Federal project director should determine, with assistance from the security staff, the actions necessary for identifying the level of security and the associated requirements cited in Part 2, Section I, Chapter VII of DOE M 470.4-1, *Safeguards and Security Program Planning and Management*. This action should identify the scope of the access authorizations required for project personnel and the need for procedures for processing the Facility Data and Approval Record and any subsequent changes.

2. DEFINITION PHASE (CONCEPTUAL DESIGN—POST CRITICAL DECISION-0).

   a. Once mission need is approved (Critical Decision-0), the site security program representative should begin to plan for the role of security within the project. This represents a critical point for determining and defining the security involvement in the project.

Table V-1. Overarching Areas of Consideration.*

Initiation Phase (Pre-Conceptual Planning)	Definition Phase (Conceptual Design)	Execution Phase I (Preliminary Design Phase)	Execution Phase II (Final Design Phase and Construction)	Transition/Closeout Phase/Operational Phase
Safeguards and security program planning and management integrates physical protection, protective force, information security, (technical surveillance countermeasures), personnel security, and nuclear material control & accountability. Identify safeguards and security Representative for project.	Identify general safeguards and security requirements: - Threat assessment - materials control and accountability - Physical Security - Information Security - Personnel Security - Cyber Security - Barriers, access controls, explosives, communications	Conduct vulnerability assessments	Construct/order necessary safeguards and security components supporting the project.	Have approved security plans: e.g. facility data and approval record, materials control and accountability, site security plan, and site safeguards and security plan
Identify major safeguards and security assets associated with the project: Matter (information): - classified - unclassified controlled Accountable Material: - nuclear - radiological - classified parts Type of safeguards and security function: - classified information, - classified parts - nuclear material processing, - nuclear /radiological material storage, clear/ radiological	Look at safeguards and security programs/projects impacting the new projects or identify the impacts this project may have on existing programs or operations. Formulate data for conduct of vulnerability assessments in conformance with DOE M 470.4-1	Prepare system configuration. Identify specific safeguards and security requirements. materials control and accountability; Physical security Info security Personnel security, Cyber security	Prepare training documents (operations & maintenance) based on final installed system. Begin training as necessary for the various topical areas as identified.	Complete safeguards and security professionals training.
Assess application of design basis threat	Identify types of safeguards and security costs associated with each Phase and Critical Decision.	Identify resources needed.	Finalize organizational structure.	Conduct and complete an operations readiness review for security.
Formulate costs.	Identify safeguards and security risks to the project.	Refine cost estimates	Prepare safeguards and security plans/procedures.	

***Consistent with DOE O 413.3A**

(1) During conceptual design, the site security program representative should evaluate the security risk of the proposed facility and document the security requirements (e.g. physical security devices and systems, nuclear materials safeguards, information security and any specialized security equipment) that result from this evaluation.

(2) The site security program representative should summarize alternative protection and control strategies and provide the Federal project director with estimated ranges for capital and operating costs of alternatives which meet security policy requirements.

b. This should occur with most topical security areas to ensure that alternatives for protection and control of security risks are evaluated for effectiveness and for long-term costs.

c. This information should be incorporated into the conceptual design and cost estimates, to be used to evaluate the project alternatives for Critical Decision-1.

d. For facilities that will be security categories I or II as related to material inventories, roll-up capabilities, and are not hazard classification categories (see DOE M 470.4-6); contain classified information and/or materials; and/or are DOE 'mission critical' facilities, a vulnerability assessment should be conducted for Critical Decision-1 to assess security risks.

e. This vulnerability assessment should be a preliminary assessment based upon the conceptual design of the facility's proposed security features. The vulnerability assessment is performed either by certified vulnerability assessment analysts from the site or outside contracting companies that have this expertise. This vulnerability assessment will make recommendations concerning upgrades of the physical security, protective force, and/or administrative controls for the proposed facility, based on the identified security risk. These recommendations are then incorporated into the conceptual design and are factors in evaluating the proposed alternatives for Critical Decision-1.

f. At the conclusion of conceptual design (Critical Decision-1), the Federal project director should know the impact of incorporating adequate safeguards and security elements into the project (e.g., security's impact on the project will be significant, minimal, or serve in an advisory role ensuring safeguards and security departmental requirements are identified).

3. EXECUTION PHASE I (PRELIMINARY DESIGN PHASE). Once Critical Decision-1 has been obtained and project engineering and design funds authorized, the preliminary design phase commences.

a. The integrated project team should closely monitor the preliminary design efforts to ensure that all project requirements are being incorporated.

b. The site security program representative should stay involved by assisting in refining security strategies, defining security system performance requirements, evaluating the responses to the preliminary vulnerability assessment results, determining office, alarm station, and other infrastructure requirements; and preparing mature cost estimates.

(1) Prior to Critical Decision-2 if a vulnerability assessment was necessary, then an update to the vulnerability assessment should be done.

(2) If at all possible, the same team of certified security analysts should perform a vulnerability assessment on the preliminary design documents.

(3) This should offer an opportunity to easily compare results from the preliminary vulnerability assessment with this assessment. As before, the results of this assessment are to be incorporated, based on the identified security risk, into the facility design.

c. Depending on the scope of and risk of assets associated with the project, the resources necessary to conduct vulnerability assessments and security technology option analyses might be significant.

d. Risks may be identified in the course of the vulnerability assessment or the security technology option analysis and captured in the risk register, which is part of the risk management plan. Additionally, security designs and associated electrical; communications; heating; ventilation; and air conditioning; and other appropriate support infrastructures for the security features of the project should be integrated into the overall project design and engineering package.

e. Where possible, industry standards should be used to plan for future growth or technological changes in the security systems.

f. When developing the project schedule, the need for and timing of construction personnel with security clearances should be ascertained. The Federal project director should ensure that sufficient time exists for the acquisition of services requiring security clearances.

4. EXECUTION PHASE II (FINAL DESIGN PHASE AND CONSTRUCTION). After Critical Decision-2 has been obtained, the final design phase continues toward conclusion.

a. Site security program representative should stay engaged in monitoring and providing assistance to the design team during final design.

b. At the conclusion of final design, all project requirements should be satisfied by the facility design and/or proposed operational features. Site security program representative of the integrated project team should ensure approval of the selected security system design by both contractor and field office managers.

c. Testing requirements and acceptance criteria are prepared for security systems and for system components, and acceptance tests, based upon required performance levels, should be specified for all security-relevant systems in the proposed contract documents for construction.

d. Upon approval of Critical Decision-3 and the start of construction, security should provide support to construction activities of necessary security initiatives, begin safeguards and security-identified training objectives, finalize organizational structure, and prepare appropriate security plans and procedures necessary to support the project.

e. The scheduling of system operations and maintenance training should take place along with acceptance plan preparation and approval by the Federal project director.

f. The acceptance plan includes the supporting operations and maintenance manuals and procedures. Project activities that are in progress in parallel with construction include final preparation of plans and procedures for facility operations. This includes acceptance testing of systems as construction is completed and the facility is transferred from the project to operations.

5. TRANSITION/CLOSEOUT PHASE/OPERATION PHASE.

a. During the Transition/Close-out, all security system documentation is reviewed and an acceptance determination made by the Federal project director. System component and complete system acceptance testing is evaluated against the test and acceptance plan. For security, efforts leading to Critical Decision-4 should represent an approved security plan, procedures, trained security professionals on-hand, and a successful Operational Readiness Review.

b. Prior to Critical Decision-4, the final update of the Vulnerability Assessment should be required, with a resulting Final Vulnerability Assessment Report. This report should document the proposed security systems and features, as well as demonstrate how the facility design, construction, and operations satisfy security requirements.

c. At Critical Decision-4, the project is completed, and there is transition to the operations program/project manager for assumption of responsibility for operations and maintenance. The facility/site Management and Operations Group takes over the responsibility for the management, operation, and associated support including security.

SAFEGUARDS AND SECURITY PROJECT CHECKLIST

While Table V-1 gives the basics of Safeguards and Security, the following checklist gives the Federal project director more detail of how to integrate the safeguards and security disciplines into the critical decision phases of a project.

As used in this attachment, "security" refers to both safeguards and security as it is applicable to the project or facility regardless of the type of building, structure, or facility and whether new or a modification. *These lists are not meant to be all-inclusive.* It is suggested that they be used in conjunction with other tools and techniques such as, but not limited to, lessons learned, brain-storming, scenario planning, similar projects, and subject matter experts.

1. INITIATION PHASE (PRE-CONCEPTUAL PLANNING):

   a. Safeguards and security point of contact is designated by Federal program/site office manager as a member of the integrated project team as appropriate and inform on the parameters of the potential project or mission need.

      (1) New facility or retrofit.

      (2) Type of facility (e.g., research, production, administrative/computing facility, nuclear and/or radiological material storage, processing with or without classified parts).

      (3) Population of the facility (e.g., numbers and origin).

      (4) Potential locations for the facility.

      (5) Existing facility or infrastructure upgrade project (e.g., fire safety upgrade, security systems upgrade, adding classified capabilities to a formally unclassified facility).

   b. Begin identification of potential security-related assets associated with the project.

      (1) Special nuclear materials, other nuclear material, radiological material, biological assets (virus samples, etc.), chemical inventories, classified and/or unclassified controlled information or parts, critical assets, high cost or unique items, high availability items [fire station, emergency operations center, etc.].

      (2) Potential physical size and location of the project.

      (3) Potential for hazardous materials.

      (4) Potential impacts to protective force size and posture.

      (5) Potential interfaces with emergency management/response assets due to nature of the facility.

(6) Impacts on existing security infrastructure/operations.

(7) Assess the design basis threat guidance for application to the project.

c. Establish relationships with other team members or disciplines involved.

(1) Operations.

(2) Safety (i.e. life safety; environment, safety and health; and nuclear safety).

(3) Engineering.

(4) Information/cyber security technologies/technical surveillance countermeasures.

(5) Budget [i.e. review (of) security costs].

d. Rough out timeline for major security related milestones and associated resources.

(1) Conduct of vulnerability assessments.

(2) Security system design initiated and completed.

(3) Security documentation prepared, updated and completed (e.g., vulnerability assessment, security plan, materials control and accountability plan, security clearances).

(4) Security tests (all safeguards and security functions).

(5) Security operational readiness review.

2. DEFINITION PHASE (CONCEPTUAL DESIGN):

a. Confirm the parameters of the project and mission need.

(1) New facility or retrofit.

(2) Type of facility (e.g. research, production, administrative/computing facility).

(3) Population of the facility.

(4) Potential locations for the facility.

(5) Existing facility or infrastructure upgrade project (e.g. fire safety upgrade, security systems upgrade, adding classified capabilities to a formally unclassified facility, electrical power distribution and communications).

(6) Potential initial registration or revision/update to the Safeguards and Security Information Management System.

(7) Validate the application of the design basis threat to the facility and its operation.

(8) Perform vulnerability analyses against the facility configuration.

b. Confirm security related assets identified in initiation phase and identify any new security-related assets.

(1) Special nuclear materials, other nuclear material, radiological material, biological assets (virus samples, etc.), classified and/or unclassified controlled information or parts, critical assets, high cost or unique items, high availability items (fire station, emergency operations center, etc.).

(2) Potential physical size and location of the project.

(3) Potential for hazardous materials.

(4) Potential impacts to safeguards and security staffing.

(a) protective force size and posture.

(b) materials control and accountability staffing.

(c) information security staffing.

(5) Potential interfaces with emergency management/response assets due to nature of the facility.

c. Integration with existing security infrastructure/operations.

(1) Finalize security-related functional and operational requirements for inclusion in overall project functional and operational requirements document.

(a) Identify general safeguards and security requirements, to include barriers, explosives, security communications, protective force support, entry/access controls, intrusion detection/surveillance systems, and materials control and accountability systems.

(b) Identify operational and infrastructure support needed for safeguards and security features.

(2) Identify safeguards and security-related disciplines necessary to consult on the project (e.g., physical security, information security, materials control

and accountability, operations security, protective force, personnel security, etc.).

(3) Continue sharing information with other team members or disciplines involved especially in regard to the overlap of design requirements that are known or evolving.

(a) Operations.

(b) Safety (i.e. life safety; environment, safety and health; and nuclear safety).

(c) Engineering.

(d) Information/cyber security technologies/technical surveillance countermeasures.

(e) Project management with other members integrated project team.

(f) Emergency management.

(4) Begin to finalize timeline for major security-related milestones and associated resources.

(a) Conduct of computer-based vulnerability assessments of the system and its components.

(b) Security system design initiated and completed.

(c) Security documentation updated and completed.

(d) Security performance/acceptance tests.

(e) Security operational readiness review.

(f) System operations and training documentation.

(g) System source code documentation.

(5) Begin to develop/review security-related costs and resources.

(a) Direct project related.

(b) Security operations.

(c) Project support related.

3. EXECUTION PHASE I (PRELIMINARY DESIGN PHASE):

a. Conduct security-related assessments based on the confirmed parameters of the project and mission need.

(1) New facility or retrofit.

(2) Type of facility (e.g. research, production, administrative/computing facility).

(3) Population of the facility.

(4) Potential locations for the facility.

(5) Existing facility or infrastructure upgrade project (e.g., fire safety upgrade, security systems upgrade, and adding classified capabilities to a formerly unclassified facility).

b. Conduct security-related assessments based on the design basis threat, security policies, and the confirmed security-related assets.

(1) Special nuclear materials, other nuclear material, radiological material, biological assets (virus samples, etc.), classified and/or unclassified controlled information or parts, critical assets, high cost or unique items, high availability items (fire station, emergency operations center, etc.).

(2) Potential physical size and location of the project.

(3) Potential for hazardous materials.

(4) Potential impacts to protective force size and posture.

(5) Potential interfaces with emergency management/response assets due to nature of the facility.

(6) Impacts on existing security infrastructure/operations.

(7) Associated security risks.

c. Conduct reviews of overall project documentation for:

(1) General and specific security requirements inclusion in engineering and design packages (e.g., physical security, barriers, explosives, security communications, protective force support, entry/access controls, intrusion detection/surveillance systems, materials control and accountability systems, classified and/or unclassified, unclassified controlled information systems, cyber systems).

(2) Operational and infrastructure support needed for security features.

(3) Interfaces and impacts to and from other sections of the engineering and design package (e.g. safety systems, general and specific layouts, operational descriptions, etc.).

d. Provide tasking, as required, to security-related disciplines to consult on the project (e.g., physical security, information security, materials control and accountability, operations security, protective force, personnel security, etc.).

(1) Begin development of security-related training strategies.

(2) Begin development of security-related operational strategies.

(3) Interface with safety and operational training development.

e. Continue sharing information with other team members or disciplines involved especially in regard to the overlap of design requirements that are known or evolving.

(1) Operations.

(2) Safety (i.e. life safety; environment, safety and health; and nuclear safety).

(3) Engineering.

(4) Training.

(5) Information/cyber security technologies/technical surveillance countermeasures.

(6) Budget [i.e. review (of) security costs].

f. Execute and review/complete major security-related milestones.

(1) Conduct of vulnerability assessments.

(2) Security system design, including key technologies.

(3) Security documentation.

(4) Security performance tests.

(5) Security operational readiness review.

g. Review/Finalize security-related costs and resources.

(1) Direct project related.

(2) Security operations and staffing.

(3) Project support related.

4. EXECUTION PHASE II (FINAL DESIGN PHASE AND CONSTRUCTION):

a. Monitor construction and change control.

(1) Document reviews.

(2) Project meeting attendance.

(3) Construction site walkthroughs.

(4) Participation/observation in security related acceptance testing.

b. Continue security related assessments based on the design basis threat, security policies, and the confirmed security-related.

(1) Special nuclear materials, other nuclear material, radiological material, biological assets (virus samples, etc.), classified and/or unclassified controlled information or parts, critical assets, high cost or unique items, high availability items (fire station, emergency operations center, etc.).

(2) Potential physical size and location of the project.

(3) Potential for hazardous materials.

(4) Potential impacts to protective force size and posture.

(5) Potential interfaces with emergency management/response assets due to nature of the facility.

(6) Impacts on existing security infrastructure/operations.

(7) Associated security risks.

c. Continue reviews of overall project documentation and construction for:

(1) General and specific security requirements inclusion in engineering and design packages (e.g. barriers, explosives, security communications, protective force support, entry/access controls, and intrusion detection/surveillance systems).

(2) Operational and infrastructure support needed for security features.

(3) Interfaces and impacts to and from other sections of the engineering and design package (e.g., safety systems, general and specific layouts, operational descriptions, etc.).

d. Provide tasking, as required, to security-related disciplines to consult on the project (e.g., physical security, information security, materials control and accountability, operations security, protective force, personnel security, etc.).

(1) Begin development of security-related training strategies.

(2) Begin development of security-related operational strategies.

(3) Interface with safety and operational training development.

e. Continue sharing information with other team members or disciplines involved especially in regard to the overlap of design requirements that are known or evolving.

(1) Operations.

(2) Safety (i.e. life safety; environment, safety and health; and nuclear safety).

(3) Engineering.

(4) Training.

(5) Information/cyber security technologies/technical surveillance countermeasures.

(6) Budget (i.e. review of security costs).

f. Update and/or complete documentation and analysis necessary to support major security-related milestones.

(1) Conduct of vulnerability assessments.

(2) Staffing plans.

(3) Security System installation, including security technology.

(4) Security documentation updated and completed.

(a) Security plans, including site security plan, site safeguards and security plan, materials control and accountability.

(b) Security procedures.

(c) Operations/maintenance plans.

(d) Proposed operation/maintenance budgets.

(5) Security function and performance tests (all safeguards and security functions).

(6) Security operational readiness review.

(7) Documentation in support of the Safeguards and Security Information Management System data registration.

g. Review/finalize security related costs and resources.

(1) Direct project related.

(2) Security operations.

(3) Project support related.

5. TRANSITION/CLOSEOUT PHASE/OPERATIONAL PHASE:

a. Monitor construction closeout and change control.

b. Transition security to an operational status.

c. Continue security-related assessments based on the design basis threat, security policies, and the confirmed security-related assets.

(1) Special nuclear materials, other nuclear material, radiological material, biological assets (virus samples, etc.), classified and/or unclassified controlled information or parts, critical assets, high cost or unique items, high availability items (fire station, emergency operations center, etc.).

(2) Potential physical size and location of the project.

(3) Potential for hazardous materials.

(4) Potential impacts to protective force size and posture.

(5) Potential interfaces with emergency management/response assets due to nature of the facility.

(6) Impacts on existing security infrastructure/operations.

(7) Associated security risks.

d. Review final project documentation and construction (As-built) and assist in the development of punch lists for:

(1) General and specific security requirements inclusion in engineering and design packages (e.g., barriers, explosives, security communications, protective force support, entry/access controls, intrusion detection/surveillance systems).

(2) Operational and infrastructure support needed for security features.

(3) Interfaces and impacts to and from other sections of the engineering and design package (e.g., safety systems, general and specific layouts, operational descriptions, etc.).

e. Provide tasking, as required, to security related disciplines to consult on the project (e.g., physical security, information security, materials control and accountability, operations security, protective force, etc.).

(1) Finalize/conduct security-related training.

(2) Finalize/conduct security-related operational procedures.

(3) Interface with safety and operational training development.

(4) Interface with safety and operational procedures.

(5) Continue sharing information with other team members or disciplines involved especially in regard to the overlap of design requirements that are known or evolving.

(6) Operations.

(7) Safety (i.e. life safety; environment, safety and health; and nuclear safety).

(8) Engineering.

(9) Training.

(10) Information/cyber security technologies/technical surveillance countermeasures.

(11) Budget [i.e. review (of) security costs].

f. Update documentation and analysis necessary to support major security-related milestones.

(1) Conducting of vulnerability assessments.

(2) Staffing plans.

(3) Security system installation.

(4) Security documentation updated and completed.

(a) Security plans.

(b) Security procedures.

(c) Maintenance and test plans/procedures.

(d) Proposed operational budgets.

(5) Security functional, performance/acceptance tests.

(6) Security operational readiness review.

g. Conduct/oversee security-related operational acceptance tests and performance-related tests.

h. Finalize security-related costs, resources and reports.

(1) Direct project related.

(2) Security operations.

(3) Project support related.

(4) Safeguards and Security Information Management System.

REFERENCES

1. LEGISLATION

   a. 42 U.S.C. §§ 2011, et seq., Atomic Energy Act of 1954, as amended.

   b. 42 U.S.C. §§ 7101 to 7352, Department of Energy Organization Act, as amended.

   c. 42 U.S.C. 7144a, Establishment of Security, Counterintelligence, and Intelligence Policies.

2. REGULATIONS.

   a. 41 CFR 102-74, Facility Management.

   b. 48 CFR 952.204-2, Security Requirements.

3. DEPARTMENT DIRECTIVES.

   a. DOE P 205.1, *Departmental Cyber Security Management Policy*, dated 5-8-01.

   b. DOE M 205.1-3, *Telecommunications Security Manual*, dated 4-17-06.

   c. DOE M 205.1-4, *National Security System Manual*, dated 3-8-07.

   d. DOE O 205.1A, *Department Of Energy Cyber Security Management*, dated 12-4-06.

      NOTE: Although separate from the safeguards and security information security program, the Department's cyber security program operates under the same basic protection principles. The cyber security program (including both classified and unclassified cyber security) is administered by the Department's Chief Information Officer.

   e. DOE O 413.3A, *Program and Project Management for the Acquisition of Capital Asset*s, dated 7-28-06.

   f. DOE P 470.1, *Integrated Safeguards and Security Management* (ISSM) Policy, dated 5-8-01.

   g. DOE O 471.1A, *Identification and Protection of Unclassified Controlled Nuclear Information*, dated 6-30-00.

   h. DOE M 471.1-1, Chg. 1, *Identification and Protection of Unclassified Controlled Nuclear Information Manual*, dated 10-23-01.

   i. DOE O 470.4A, *Safeguards and Security Program*, dated 5-25-07.

   j. DOE M 470.4 Series of Manuals.

k. Director, Central Intelligence Directives 6/9, Physical Security Standards for Sensitive Compartmented Information Facilities, 11-18-02.

4. OTHER FEDERAL DIRECTIVES.

a. 4-010-01, Unified Facilities Criteria, Department of Defense Minimum Antiterrorism Standards for Buildings.

b. U.S. Army Corps of Engineers, Technical Manual 5-853-4, Electronic Security Systems; CEGS 13720 series guides, and the PROSPECT Program.

c. General Services Administration Office of Government Policy, Federal Real Property Council Security Resource Guide.

d. Department of Justice Vulnerability Assessment of Federal Buildings.