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

ADMIN CHANGE

DOE G 413.3-3A

Chg 1: 10-22-2015

SUBJECT: ADMINISTRATIVE CHANGE TO DOE G 413.3-3A, *SAFEGUARDS AND SECURITY FOR PROGRAM AND PROJECT MANAGEMENT*

1. EXPLANATION OF CHANGES. These Administrative Changes are limited to changing the Office of Primary Interest (OPI) to the Office of Project Management Oversight and Assessments.

2. LOCATIONS OF CHANGES:

Page	Paragraph	Changed	To
Title		INITIATED BY: Office of Management	INITIATED BY: Office of Project Management Oversight & Assessments
i(andii)	3	The Department of Energy, Office of Acquisition and Project Management, Attention: MA-63, 1000 Independence Avenue, SW, Washington, DC 20585.	The Department of Energy, Office of Project Management Oversight & Assessments, 1000 Independence Avenue, SW, Washington, DC 20585.

NOT MEASUREMENT SENSITIVE

DOE G 413.3-3A
Approved: 08-15-2013
Chg 1 (Admin Chg) 10-22-2015

SAFEGUARDS AND SECURITY FOR PROGRAM AND PROJECT MANAGEMENT

[This Guide describes suggested non-mandatory 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 Project Management Oversight & Assessments

FOREWORD

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

This Guide is intended to provide a methodology for implementing the safeguards and security requirements of DOE O 413.3B, *Program and Project Management for the Acquisition of Capital* Assets, dated 11-29-2010. DOE Guides are not requirement documents and should not be construed as requirements. Guides are part of the DOE Directives Program and provide suggested ways of implementing Orders, Manuals, and other regulatory documents.

Beneficial comments (recommendations, additions, and deletions) and any pertinent data that may improve this document should be sent to: The Department of Energy, Office of Project Management Oversight & Assessments, 1000 Independence Avenue, SW, Washington, DC 20585.

CONTENTS

SECTION I. INTRODUCTION

1. GOAL. To ensure that safeguards and security requirements are identified and integrated into a capital asset project early in its development timeline and that their implementation and effectiveness are assessed throughout the project life cycle. Protection strategies should consider potential threats to assist early on during the asset design process. Establishing and integrating safeguards and security requirements early in the project is necessary for efficient project planning and cost estimating to avoid scope creep later in the project which leads to cost and schedule overruns. Good front end planning is a fundamental principle of good project management that enhances the probability of completing projects within the initially approved project baseline. The initial identification of safeguards and security requirements and the requirements of other critical disciplines (e.g., safety), and the integration with other project functional and physical requirements is critical to the development of the best overall cost effective acquisition strategy 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. Provide safeguards and security guidance to Federal Project Directors and Federal Program/Site Office Managers (and to 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. Define the project's safeguard and security related features and functions, as developed or required by the security program and security policies, early enough to minimize impact on operations;

   c. Identify the function of the federal site security program representative who serves as the security design point of contact for security features and is a member of the integrated project team during the entire project cycle.

   d. Facilitate communication and interaction between the site security professionals; classification and Unclassified Controlled Nuclear Information (UCNI) officials; the integrated project team; and the members of the project design team.

   e. This guide applies to the DOE elements specified in DOE O 413.3B, including the National Nuclear Security Administration (NNSA), which fund, direct, and manage acquisition projects as defined by such Order.

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 it is new or a modification to an existing facility.

This Guide provides suggested approaches for implementing security provisions within the security functional areas as specified in DOE O 413.3B, *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 series. This Guide provides explanations and examples for implementing requirements of DOE O 413.3B and specific to compliance with safeguard and security requirements provisions, including requirements to identify classification and controlled unclassified information.

Except for requirements established by a regulation, contract, or DOE policy 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 not, however, create an inference of compliance with the related requirements. Alternative methods of program implementation 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 recommended or optional implementation guidance that could be used to meet the requirements of the DOE O 413.3B. This Guide is applicable to all DOE activities that are subject to the requirements of DOE O 413.3B.

SECTION II. ROLES AND RESPONSIBILITIES[1]

1. UNDER SECRETARIES.

   a. Receive Acquisition Executive (AE) authority from the Secretarial Acquisition Executive (SAE), as appropriate (see DOE O 413.3B for more details on delegation of authority to Acquisition Executives).

   b. Under DOE O 470.4B, the Associate Administrator for Defense Nuclear Security, the Under Secretary of Science, and the Under Secretary for Energy are designated as the DOE cognizant security officer for the organizations under the purview of their Offices, and may delegate this authority officially in writing as appropriate to carry out the associated responsibilities.

   c. Hold accountability for project-related site environment, safety and health, and safeguards and security.

2. 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. Oversees the project line management organization, including 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 the project security management documents as stipulated in the Project Execution plan.

3. FEDERAL PROJECT DIRECTOR.

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

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

---

[1] Safeguard and security provisions from DOE O 413.3B, *Program and Project Management for the Acquisition of Capital Assets*, Appendix B, dated 11-29-2010; and DOE O 470.4B, Admin Chg. 1, *Safeguard and Security Program*, dated 2-15-2013.

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

d. Assures safeguards and security requirements are integrated into the project documents.

e. Approves changes within control ranges set in the safeguards and security aspects of the project execution plan.

4. FEDERAL SITE SECURITY PROGRAM REPRESENTATIVES.

a. Represent the security interests of the site and are the points of contact for resolving security issues on the integrated project team (IPT).

b. Responsible for ensuring that safeguards and security concerns and criteria are identified, to include oversight of reviews for the safeguard and security of classified and controlled unclassified information (see DOE O 470.4B, Appendix A; DOE O 475.2A, *Identifying Classified Information*; DOE O 471.1B, *Identification and Protection of Unclassified Controlled Nuclear Information*, for requirements).

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

d. Participate/lead in facility security vulnerability assessments and/or security risk analysis in coordination with specialized security vulnerability analysts from contractor staff and consultants, as required.

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

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

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

h. Validate/approve the System Requirements Documents for Safeguards and Security to ensure that all requirements are identified and addressed.

5. OTHER INTEGRATED PROJECT TEAM MEMBERS

a. IPT members represent their disciplines and work to ensure that design and construction incorporate the security area concerns and requirements.

b. Ensure that reviews for classified and controlled unclassified information are conducted by appropriate authorities in accordance with Departmental regulations and directives.

6. 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. Throughout the life cycle of the project ensure that plans developed in previous phase(s) are periodically updated based on increased planning maturity.

7. SITE CONTRACTOR SECURITY REPRESENTATIVE

a. Works with the site project manager to ensure that security requirements and issues are being properly represented and resolved.

8. SITE CONTRACTOR EMERGENCY MANAGEMENT REPRESENTATIVE.

a. Works with the site project manager to ensure that security requirements and issues, and potential interfaces with emergency management assets are being properly represented and resolved.

9. HQ SECURITY PROGRAM OFFICES.

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

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

c. Review and concur on the safeguard and security aspects of the Project Execution Plan.

SECTION III. SAFEGUARDS AND SECURITY PROGRAM BACKGROUND

All DOE facilities should be evaluated for potential risks to employees, the public, and the environment. DOE O 470.4B, Admin Chg. 1, *Safeguard and Security* Program, dated 2-15-2013; DOE O 470.3B, *Graded Security Protection (GSP) Policy*, dated 8-12-2008; and successor Orders/Policies, contain requirements for determining the level of protection, based on facility functions and potential security risks and graded security protection policy requirements. This also includes Cyber Security under the provisions of DOE O 205.2B, *Department of Energy Cyber Security Program*, dated 3-11-2013, and DOE O 150.1, *Continuity Program*, dated 5-08-2008.

A preliminary safeguards and 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 reviews, should be factored early into the conceptual design before establishing the project cost range at Critical Decision-1, requesting funding authorization for design, and establishing the project performance baseline at Critical Decision-2. The last is especially important when the project will involve construction of a protected area, material access area, and/or special designated security areas due to the substantial scope and cost associated with these types of facilities.

An appropriate security plan should be completed and approved prior to the start of construction (including site preparation), consistent with DOE O 470.4B, *Safeguards and Security Program*, Admin Chg.1. 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 470.3B, *Graded Security Protection (GSP) Policy*. 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 requiring high physical protection the Federal Project Director should make reference to the GSP Policy because additional performance-based security measures may necessitate a security vulnerability assessment/security assessment to be performed by the site to determine what additional security measures are necessary to achieve an integrated protection system consisting of detection, assessment, communication, response, interruption, and neutralization.

The DOE O 470.3B establishes minimum design principles based on vulnerability assessments. Adherence to this directive should provide reasonable assurance that safeguards and security designs embody 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 by the requirements of DOE O 473.3, *Protection Program Operations*, dated 6-27-2011.

The type of security area established depends on the nature of the security interests to be protected. The following list of security areas is based on the restrictive nature for the security interests protected:

- general access area
- property protection area,
- limited area,
- protected area,
- material access area, and
- special designated security areas.

The general access area (to 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. Physical protection strategies for the physical protection of DOE facilities must be developed, documented, and implemented consistent with both the Graded Security Protection Policy, formerly the Design Basis Threat Policy; and the overall National policy to protect against radiological, chemical, or biological sabotage (specifically to DOE described in DOE O 470.3B, *Graded Security Protection (GSP) Policy*, dated 8-12-2008).

The following DOE Directives describe DOE policy and procedures to implement various aspects of safeguards and security which should apply to the protection of capital asset projects:

- DOE O 470.3B, *Graded Security Program (GSP) Policy*, dated 8-12-2008;
- DOE O 470.4B, Admin Chg. 1, *Safeguards and Security Program*, dated 2-15-2013;
- DOE O 474.2, Admin Chg. 2, *Nuclear Material Control and Accountability*, dated 11-19-2012;
- DOE O 473.3, *Protection Program Operations*, dated 6-29-2011; and
- DOE O 471.6, Chg. 1, *Information Security*, dated 11-23-2012.

Requirements for identifying and protecting classified and controlled unclassified information are specified in the following references:

- 10 CFR Part 1045, *Nuclear Classification and Declassification*. It establishes the Government-wide policies and procedures for implementing sections 141 and 142

of the Atomic Energy Act of 1954 for classifying and declassifying Restricted Data (RD) and Formerly Restricted Data (FRD) and implements the requirements of Executive Order 13526 concerning National Security Information (NSI) that affects the public.

- Executive Order 13526, *Classified National Security Information*. It prescribes the Government-wide system for classifying, safeguarding, and declassifying NSI.

- 32 CFR Part 2001, *Classified National Security Information.* Implements the requirements prescribed in Executive Order 13526 for classifying, safeguarding, and declassifying NSI.

- DOE O 475.2A, *Identifying Classified Information,* dated 2-01-2011. It establishes requirements for managing the DOE program including details for classifying and declassifying information, documents, and material classified under the Atomic Energy Act (RD, FRD, and Trans Classified Foreign Nuclear Information) or Executive Order 13526 (National Security Information), so that it can be protected against unauthorized dissemination.

- 10 CFR Part 1017, *Identification and Protection of Unclassified Controlled Nuclear Information.* It establishes Government-wide policies and procedures for implementing the requirements of Section 148 of the Atomic Energy Act of 1954 concerning the identification and protection of certain unclassified but sensitive Government information concerning atomic energy defense programs.

- DOE O 471.1B, *Identification and Protection of Unclassified Controlled Nuclear Information,* dated 3-01-2010. It establishes the requirements for managing the DOE program for indentifying and protecting UCNI.

- DOE Order 471.3, Admin. Chg. 1, *Identifying and Protecting Official Use Only Information,* dated 1-13-2011, and DOE M 471.3, Admin. Chg. 1, *Manual for Identifying and Protecting Official Use Only Information,* dated 1-13-2011. They establish the requirements for the DOE program to identify certain unclassified information as Official Use Only and to identify, mark, and protect documents containing such information.

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

- Intelligence Community Standard (ICS) 705-1, *Physical and Technical Security Standards for Sensitive Compartmented Information Facilities,* dated 9-17-2010

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, 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.[2]

   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 officially designated DOE cognizant security office and should be consistent with security policies.

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

   c. The approach should provide a security solution that maintains compliance with safeguard and security requirements, or includes approved deviation from; and provides effective security, while minimizing security's impact on project cost, potential safety concerns, and operational impacts. The approach should also consider interim and/or temporary safeguards and security measures that should be implemented during the execution phase of the project.

   d. Technologies should be used in lieu of staff to perform routine security functions whenever possible and feasible. The design features should accomplish the majority of the tasks.

   e. The application of these approaches should include cost to benefit analyses, and documented returns on investment and break even points where possible.

---

[2] Interagency Security Committee (ISC) Standard, *Physical Security Criteria for Federal Facilities*; ISC Standard, *Facility Security Level Determinations for Federal Facilities.*

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

   a. Successful design accounts for all requirements within the area's applicability and expected environmental conditions for the system to operate. For example, DOE nuclear safety directives do not address malevolent acts, sabotage, or terrorist activities, while security requirements are focused primarily on such actions. Another example, while security may address the guns/gates/guards needed to meet physical protection standards, the requirements for identifying classified and controlled unclassified information and documents is found in other regulations and DOE directives and are listed in Section III. For cyber security requirements the applicable DOE directive is DOE O 205.1B, *Department of Energy Cyber Security Program.*

   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 unauthorized 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 evaluation of operational implications and estimated life-cycle costs of security considerations of proposed alternatives and 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 (see DOE G 413.3-4, *Technology Readiness Assessment Guide,* for managing technology risk in projects). 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 need to request technical assistance from their officially designated DOE cognizant security office. 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.

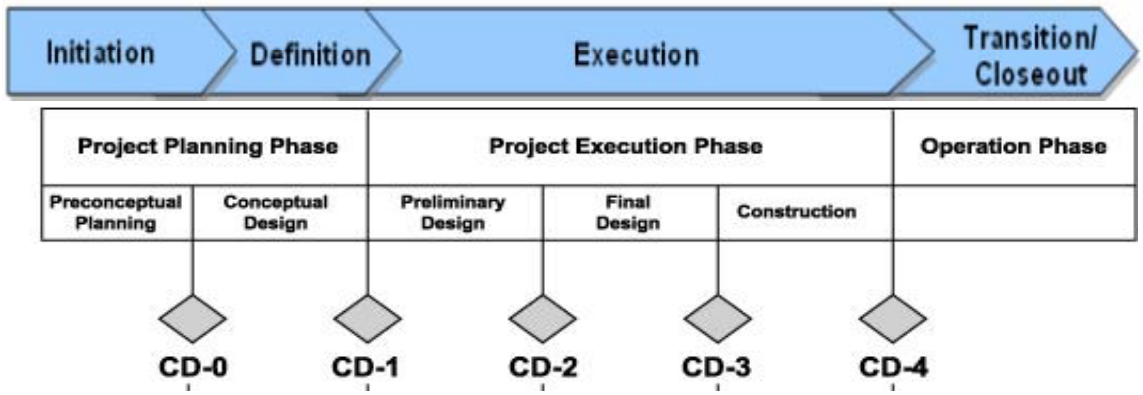

Figure V-1 Typical DOE Project Timeline

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

   For all projects, an early evaluation of probable security concerns and vulnerabilities should be made by the federal program/site office manager. The site security office and contractor's security office should develop functional design requirements to meet safeguard and security, and cyber security requirements using the Graded Security Protection Policy (DOE O 470.3B or successor documents) and applicable DOE safeguards and security, and cyber security requirements. 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 Appendix B, Section 1, Chapter VII of DOE O 470.4B, *Safeguards and Security Program.* This action should identify the scope of the access authorizations required for project personnel and the need for identifying procedures for submitting the necessary changes to the Facility Data and Approval Record.

Table V-1. Overarching Areas of Consideration.*

Initiation Phase (Pre-Conceptual Planning)	**Definition Phase (Conceptual Design)** (Prior to CD-1)	**Execution Phase I (Preliminary Design Phase)** (Prior To CD-2)	**Execution Phase II (Final Design Phase and Construction)** (Prior to CD-3)	**Transition/Closeout Phase/Operational Phase**
Safeguards and security program planning and management integrate physical protection, protective force, information security, technical security programs, personnel security, and nuclear material control & accountability. Develop functional design requirements to meet safeguard and security and cyber security requirements using the Graded Security Protection Policy. 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 preliminary security vulnerability assessment/ security assessments.	Construct/order necessary safeguards and security components supporting the project as per Acquisition Plan. Submit final Security Vulnerability Assessment / Security Assessment Report.	Have approved security plans: e.g. facility data and approval record, materials control and accountability, site security & emergency mngt. plan, or site safeguards and security and emergency mngt. plan.
Identify major safeguards and security assets associated with the project. Information and Matter: - classified; - unclassified controlled; Accountable Material: - nuclear; - radiological; - classified parts; Type of Safeguards and Security Function: - classified & controlled unclassified information; - classified & controlled unclassified parts; - nuclear material processing; - nuclear radiological material storage.	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 preliminary security vulnerability assessment/security assessment for the selected project alternative after CD-1 in conformance with DOE O 470.4B and DOE O 413.3B.	Prepare system configuration. Identify specific safeguards and security requirements such as: materials control and accountability; physical security; information security; personnel security; cyber security. Obtain approval for any deviations from Departmental security requirements.	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 and emergency management professional training.
Assess application of Graded Security Protection (GSP) Policy.	Identify types of safeguards and security range of costs associated with each Phase and Critical Decision.	Identify resources needed.	Finalize organizational structure.	Conduct and complete an operations readiness review for security.
Formulate order of magnitude range of costs.	Identify safeguards and security risks to the project alternatives.	Refine cost and schedule estimates to support CD-2.	Prepare safeguards and security plans/procedures.	Submit Lessons Learned Report

***Consistent with DOE O 413.3B, DOE O 470.4B, DOE O 473.3, DOE O 474.2, DOE O 471.6, & DOE O 205.1B CD = Critical Decision**

Note to Figure V-1 – Information, documents, or material generated at any phase of the project should be reviewed by appropriate officials (e.g., Derivative Classifiers, UCNI Reviewing Officials) in accordance with applicable departmental directives and regulations when it has the potential to contain classified or controlled unclassified information as part of information security.

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.

(1) Prior to beginning conceptual design, the site security program representative should develop a functional design document based on DOE safeguard and security and cyber security orders. This document should provide the baseline for conceptual design alternatives.

(2) 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.

(3) The site security program representative should summarize requirements associated with safeguard and security assets being protected/affected by the project. The site security program representative and the Federal Project Director working with the Contractor Project Manager should review and concur with the alternative protection and control strategies, along with estimate ranges for capital and operating costs of alternatives which meet security policy requirements.

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

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

b. For facilities that will handle, store, or process categories I or II quantities of Special Nuclear Materials, or where roll up quantities to a Category I quantity is credible, or as defined by their program office as “mission critical” an identification of general safeguard and security requirements for the recommended alternative should be performed prior to CD-1 (this should be followed by a preliminary security vulnerability assessment/security assessment prior to CD-2).

c. The identification of general safeguard and security requirements should be based upon the conceptual design of the facility and uses staffing and operational assumptions. It may make recommendations regarding changes to the physical security, protective force, material control and accountability, or other administrative/engineered controls for the proposed facility in order to mitigate potential risks to Departmentally approved ranges of risks. These recommendations should be considered and incorporated, where applicable into the conceptual design for the facility at CD-1. The identification of the safeguards and security requirements for the selected alternative at CD-1 should have assessed the potential risks to Departmental assets, if the facility were built to this design. This process should be conducted with the assistance of trained security analysts familiar with DOE requirements.

d. At the conclusion of conceptual design (CD-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 CD-1 has been obtained, 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 and validating the security system performance requirements; evaluating the responses to the safeguard and security requirements; determining the physical security, alarm station, material control and accountability, administrative/engineered controls, and other infrastructure requirements for the proposed facility; and preparing more mature cost estimates.

(1) Prior to Critical Decision-2 (CD-2), conduct a preliminary security vulnerability assessment/security assessment; if necessary (see DOE O 413.3B and DOE STD 1192-2010, *Vulnerability Assessment Standard*, dated February 2010).

(2) If at all possible, the same team of security analysts should perform a preliminary security vulnerability assessment/security assessment on the preliminary design documents. Due to the complex nature of these assessments, it is suggested that the resulting preliminary security vulnerability assessment be peer reviewed by an independent team of experienced analyst prior to CD-2.

(3) This should offer an opportunity to easily compare results from the identification of the safeguard and security requirements with the preliminary security vulnerability assessment prior to CD-2 and reconcile

differences. As indicated before, the results of this assessment are to be incorporated, based on the identified security risks, into the facility design.

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

c. Risks may be identified in the course of the preliminary security 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. These vulnerability assessments should add separate assessments from the counterintelligence, telecommunications, or cyber security programs which normally are not included in the security vulnerability assessments, or security vulnerability technology option analysis, which could add additional equipment and infrastructure support requirements.

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

e. 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.

f. Risks identified during the security vulnerability assessments should be included in the project risk management plan and accounted for in the project cost estimates to include cost and schedule contingency allowances for safeguard and security elements of the project.

g. At CD-2, the project should include all safeguard and security elements that would impact the project scope, cost and schedule performance baseline.

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

a. The site security program representative should stay engaged in monitoring and providing assistance to the design team during final design. Engagement should include: reviewing design documents against the functional requirements document and the security vulnerability assessment; ensuring the infrastructure is in place to support safeguard and security requirements; being involved in cost/benefit tradeoffs discussions/decisions, and in conduct of limited scope security vulnerability assessments of proposed design changes.

b. Prior to CD-3 finalize the security vulnerability assessment/security assessment report. At the conclusion of final design, all project requirements should be satisfied by the facility design and/or proposed operational features. The 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 (CD-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.

g. The site security program representative should continue to monitor and evaluate the impact of design or concept of operation changes that occur during construction, or be satisfied by an approved deviation. The impact of these changes should be reported to the Federal Project Director and reported in the appropriate document of record.

5. TRANSITION/CLOSEOUT PHASE/OPERATION PHASE.

a. During the Transition/Close-out phase, 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 (CD-4) should represent an approved security plan, procedures, trained security professionals on-hand, and a successful Operational Readiness Review.

b. Prior to CD-4, the final update of the Security Vulnerability Assessment/Security Assessment should be prepared, with a resulting Final Security Vulnerability Assessment/Security Assessment Report. This report should document the installed security systems and features, as well as demonstrate how the facility

design, construction, and operations satisfy security requirements, or can be accomplished by an approved deviation from Departmental security requirements.

c. CD-4 is the achievement of the project completion criteria defined in the Project Execution Plan at which the operations organizations assume responsibility for starting 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. Security assessments should include reviews for the protection of classified information and unclassified controlled nuclear information as required in the Directives cited in Section III of this Guide. *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 – PRE CD-0):

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

      (1) Classification as new facility or retrofit.

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

      (3) Estimate of population for 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 controlled unclassified information or parts, sensitive compartmented information, 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 and fire department response assets due to nature of the facility.

(6) Impacts on existing security infrastructure/operations.

(7) Assess the graded security protection (GSP) policy and other Departmental security directives for application to the project.

c. Establish relationships with other team members or disciplines involved to ensure programmatic integration.

(1) Operations.

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

(3) Engineering.

(4) Information/cyber security technologies/Technical Security Program.

(5) Classified design. Plan to minimize/segregate the classified portion of the design and train the project team in the plan. The goal is to minimize the cost of the design effort.

(6) Emergency Management.

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

Note: See Appendix F, DOE G 413.3-18A, *Integrated Project Team Guide for Formation and Implementation,* for special considerations for nuclear projects. The need for classified and controlled unclassified information reviews should be considered.

d. Preliminary schedule for major security related milestones and associated resources.

(1) Development of a safeguard and security functional requirements document to assist in concept development.

(2) Conduct of security vulnerability assessments/security assessments.

(3) Security system design initiated and completed.

(4) Security documentation prepared, updated to include any deviations from Departmental security requirements, and completed (e.g., security vulnerability assessment/security assessment; security plan; materials control and accountability plan; security clearances; Technical Security Program documentation, if applicable).

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

(6) Security operational readiness review.

2. DEFINITION PHASE (CONCEPTUAL DESIGN – PRE CD-1):

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

(1) New facility or retrofit.

(2) Type of facility (e.g. research, production, sensitive compartmented information, 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 formerly unclassified facility, electrical power distribution and communications).

(6) Perform alternative analysis and ensure security risks for the recommended alternative are identified in the Risk Management Plan for the project.

(7) Validate the application of the GSP policy and other Departmental security directives to the facility and its operation.

(8) Develop an understanding of the facility's concept of operations.

(9) Identify general safeguards and security requirements for the recommended alternative prior to CD-1 based on the proposed 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 controlled unclassified information or parts, sensitive compartmented information, 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) Complete plan to minimize/segregate the classified portion of the design and training of the project team on the plan. Goal is to reduce design costs.

(5) Perform a red/black analysis of the major process equipment (gloveboxes, etc.) to assist design with equipment spacing requirements (classified process additional spacing requirements are often not factored in).

(6) Potential impacts to safeguards and security staffing.

(a) Protective force size and posture.

(b) Materials control and accountability staffing.

(c) Information security staffing.

(d) Testing and maintenance or Performance Assurance Program resources if the project is for a facility that requires a facility clearance.

(e) Additions to infrastructure and maintenance.

(7) Potential interfaces with emergency management/response and fire department 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.

Note: Cyber security is not a security organization function. This function is primarily handled by the Chief Information Officer organization. This should be coordinated with an information technology representative rather than a security representative.

(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 security programs.

(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 preliminary computer-based security vulnerability assessments/security assessment of the system and its components, if necessary.

(b) Security system design initiated and completed.

(c) Security documentation updated and completed.

(d) Finalize the Security Vulnerability Assessment/Security Assessment Report.

(e) Security performance/acceptance tests.

(f) Security operational readiness review.

(g) System operations and training documentation.

(h) 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 – PRE CD-2):

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) Concept of facility operations.

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

b. Conduct security-related assessments based on the GSP policy, other Departmental security directives, and the confirmed security-related assets.

(1) Special nuclear materials, other nuclear material, radiological material, biological assets (virus samples, etc.), classified and/or controlled unclassified information or parts, sensitive compartmented information, 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 and fire department 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, sensitive compartmented information, controlled unclassified information, Controlled Unclassified Nuclear 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.).

(4) Perform a Red/Black analysis of the minor security process equipment (instruments, etc.) to assist design with cable tray and conduit space requirements. Note: Projects historically have not factored additional spacing needed when a project has Red and Black cable trays and conduit.

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 security programs.

(6) Emergency Management.

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

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

(1) Conduct of security vulnerability assessments/security assessments.

(2) Security system design, including key technologies.

(3) Security documentation.

(4) Security performance/functional 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 – POST CD-2):

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.

(5) Conduct impact on design changes. Analyses should include cost, risk/protection effectiveness, and operability factors.

b. Continue security related assessments based on the GSP policy, other security directives, and the confirmed security-related assets.

(1) Special nuclear materials, other nuclear material, radiological material, biological assets (virus samples, etc.), classified and/or controlled unclassified information or parts, sensitive compartmented information, 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 and fire department 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.).

(4) Verify the Red/Black analysis of security process equipment as significant design modifications are approved (check for additional space requirements). Note: Projects historically have not factored the additional spacing requirements needed when a project has Red and Black cable trays and conduit.

d. Provide tasking, as required, to security-related disciplines to consult on the, project (e.g., physical security, information security, material controls 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.

(4) Develop a plan and conduct training to ensure efficient and complete startup and turnover of the integrated safeguard and security (S&S) systems. The plan should include interaction with the various DOE S&S personnel since they will be involved with the acceptance/approval of the S&S systems.

(5) Prior to the installation of classified equipment, train the appropriate construction personnel on the classification sensitivities.

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 security programs.

(6) Emergency Management.

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

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

(1) Finalize security vulnerability assessment/security assessment report, if required.

(2) Staffing plans.

(3) Security System installation, including security technology.

(4) Security documentation updated and completed.

(a) Security plans; including site security plan; performance assurance program 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 - PRE CD-4:

a. Monitor construction closeout and change control.

b. Transition security to an operational status.

c. Continue security-related assessments based on the GSP policy, other security directives, and the confirmed security-related assets.

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

(2) Physical size and location of the project.

(3) Hazardous materials.

(4) Impacts to protective force size and posture.

(5) Interfaces with emergency management/response and fire department 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, cyber security, 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) Emergency Management.

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

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

(1) Updates to security vulnerability assessment/security assessment report.

(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) Facility registration activities, e.g., Facility Data and Approval Record changes.

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. 10 CFR Part 1045, Nuclear Classification and Declassification.

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

   c. 32 CFR Part 2001, Classified National Security Information.

   d. 41 CFR 102-74, Facility Management.

   e. 48 CFR 952.204-2, Security Requirements.

3. EXECUTIVE ORDERS.

   a. Executive Order 13526, Classified National Security Information.

4. DEPARTMENT DIRECTIVES.

   a. DOE P 205.1, *Departmental Cyber Security Management Policy*, dated 5-08-2001.

   b. DOE P 470.1A, *Safeguards and Security Program*, dated 12-29-2010.

   c. DOE O 150.1, *Continuity Program*, dated 5-08-2011.

   d. DOE O 205.2B, *Department of Energy Cyber Security Program*, dated 3-11-2013.

      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 251.1C, *Departmental Directives Program*, 01-15-2009.

f. DOE O 413.3B, *Program and Project Management for the Acquisition of Capital Assets*, dated 11-29-2010.

g. DOE O 470.4B, Admin. Chg. 1, *Safeguards and Security Program*, dated 2-15-2013.

h. DOE O 470.3B, *Graded Security Protection (GSP) Policy*, dated 8-12-2008.

i. DOE O 471.1B, *Identification and Protection of Unclassified Controlled Nuclear Information*, dated 3-01-2010.

j. DOE O 471.3, Admin. Chg. 1, *Identifying and Protecting Official Use Only Information*, dated 1-13-2011.

k. DOE O 471.6, Chg.1, *Information Security*, dated 11-23-2012.

l. DOE O 472.2, *Personnel Security*, dated 6-27-2011.

m. DOE O 473.3, *Protection Program Operations*, dated 6-29-2011.

n. DOE O 474.2, Admin. Chg. 2, *Nuclear Material Control and Accountability*, dated 11-19-2012.

o. DOE O 475.2A, *Identifying Classified Information*, dated 2-01-2011.

p. DOE STD 1192-2010, *Vulnerability Assessment Standard*, dated February 2010.

q. DOE M 205.1-3, Chg. 1, *Telecommunications Security Manual*, dated 12-20-2012.

r. DOE M 471.3, Admin. Chg. 1, *Manual for Identifying and Protecting Official Use Only Information*, dated 1-13-2011.

5. 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*.

c. U.S. Army Corps of Engineers, CEGS 13720, *Electronic Security System*, dated 11-01-1998.

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

e. Director for Central Intelligence Directive 6/9, Physical Security Standards for Sensitive Compartmented Information Facilities.

f. Department of Justice, Vulnerability Assessment of Federal Buildings.

g. Intelligence Community Standard (ICS) 705-1, Physical and Technical Security Standards for Sensitive Compartmented Information Facilities, dated 9-17-2010.

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

i. ISC Standard, Facility Security Level Determinations for Federal Facilities.

j. ISC Report, The Design Basis Threat (DBT).