



Topical Report on Security and Safety Integration

Prepared for the:
Safety and Security Interface Technology Initiative

September 11, 2006



Topical Report on Security and Safety Integration

Prepared for the:
Safety and Security Interface Technology Initiative

EFCOG Approval:

David B. Amerine _____
Chairman, Energy Facility Contractors Group

Working Group Concurrence:

Paula A. Ostby
Chairman, Safety Analysis Working Group

Mark S. Strauch
Chairman, Security Working Group

Advocates:

Chief Health, Safety and Security Officer (HS-1)
Associate Administrator for Defense Nuclear Security (NA-70)
Office of Safeguards and Security, Emergency Management (EM-3.1)
Central Technical Authorities

Users:

Site Managers
Site Security Personnel
Site Safety Personnel
Facility Operations Managers

Expectations:

This document is the result of collaboration between safety and security professionals both within DOE and the contractor organizations from across the complex. Working as the Safety and Security Interface Technology Initiative, the intent of this effort is that the technical report be promulgated by EFCOG, with endorsement from the above advocates and input from the user community. Comments or questions on this report may be sent to Bob.Lowrie@wsms.com.

Executive Summary

The purpose of this topical report is to describe a process developed to facilitate integration of security and safety elements satisfying the current Design Basis Threat (DBT) expectations as well as safety basis objectives. These issues were initially discussed during the NNSA Safety and Security Summit (August 2005) and formally discussed during meetings sponsored by the EFCOG Safety Analysis Working Group (SAWG) in February 2006. The proposed process described in this technical report is the result of a series of core working team meetings in Germantown, MD in early March 2006 and in Idaho Falls, ID in mid-July 2006.

The interest and participation in process development by both security and safety professionals have been exemplary from the outset. Approximately 30 individuals from seven DOE sites and DOE-HQ attended the February SAWG meetings. Participants included DOE-HQ, DOE Site Office, contractor, and subcontractor personnel involved in implementing security or safety within the complex. The March and July core team meetings allowed a smaller working team to develop the concepts from the February EFCOG meetings into the report contained herein.

Process Summary

A cost effective, comprehensive process has been developed to simultaneously satisfy DBT and safety basis objectives for security systems. This approach is intended to facilitate sites meeting the defined dates to satisfy the DBT. An integrated project team approach has been proposed that contains multiple interrelated elements/processes: training, alternative analysis, document integration, configuration control, etc. Section 5 of the report lays out the overall process.

A key element of this process leading to cost savings for individual facilities is the toolbox approach that makes systems and key information transportable between facilities and sites and accessible by multiple DOE sites for review and use. The toolbox is populated with pertinent Security Information Data Set (SIDS) information that includes safety basis and security data for various security systems, including system evaluation and approval documentation. These data may be used as part of the information set required to obtain approval to deploy similar security systems at several sites.

For this process to be successful, safety and security professionals from around the complex and at DOE-HQ need to understand the parameters under which their counterparts work and possess a contextual understanding of the terms of art used by their counterparts.

Topical Report Elements

The key elements of the topical report are addressed below.

Drivers and End State

The key concepts and regulatory requirements to be considered to successfully deploy new or modified security systems at DOE nuclear facilities are identified and discussed. All requirements must be satisfied to successfully meet the objectives of the proposed process. The desired end state for this process includes successful implementation in the field,

handling of related documentation, and the concept of a portable database or toolbox containing pertinent security and safety basis information suitable for multi-site use.

Establish Terminology/Concept Crosswalk

Effective communication between the security and safety basis professionals is needed for this process to be successful. In some cases the same or similar words have very different meanings depending on the venue. The reverse is also true; different terms can have the same or similar meanings. To help address this concern, a process to inform and familiarize Subject Matter Experts (SMEs) from each discipline is proposed. Some of the more important terms and concepts requiring clarification are included in a crosswalk matrix in Appendix A of this report.

Awareness Training on Project Approach, Selection of Tools, and Terminology

This element focuses on ideas and concepts related to training that would serve to enhance the understanding of procedures and programs on the various security systems and upgrades. The principal intent is to devise training that can be transported between multiple sites.

Integrated Project Approach to Safely Deploy Security Systems

To cost effectively deploy a new or upgraded security system, an integrated project approach is recommended. This section adapts this approach to security systems and presents a process flow that starts with the DBT, evaluates a series of candidate security systems, prepares security and safety basis documentation as required by the Nuclear Safety Rule (10CFR830 Part B), and selects and procures the optimal system or systems. Preparation of the Project Execution Plan is a key component of this approach.

Alternative Analysis Process for System Selection

The alternative analysis process is an integral element in the proposed Integrated Project Approach. This section describes this process in detail showing how an optimal security system is selected to satisfy both security and safety basis objectives. Representatives from Security, Safety Basis, and DOE are part of the project team that exercises this process and selects the optimal system or systems.

Security System Toolbox: Development, Data Capture, and Data Sharing

This section presents a concept with the potential for universal application at DOE sites. The intent is to identify and provide information to the end users or sites that facilitates the deployment of security systems that meet safety basis requirements. Important data covering the security system, security analyses, and safety basis information can be captured in a data base (toolbox) and shared among the DOE sites that are required to meet the DBT. It is recognized that classification considerations with this toolbox will have to be managed based on a need to know. The ultimate goal is development of a “system in a box” concept, whereby individual sites can access the database and select security systems that have already been tested, evaluated, and approved for use within the DOE Complex. Thus, the new analysis may be limited to the site or installation specific evaluations to assure that the specific installation/use is within the approved criteria and standards. This concept has the potential to greatly simplify the security system approval process.

Safety Basis and Security Document Integration

This section summarizes the documentation objectives associated with both safety basis and security. Clearly, a new or upgraded security system should be accurately reflected in both sets of documents. DOE approvals will also be necessary in some instances for both document sets. This section addresses the documentation implications in both venues. The Major Modification concept and its application in this arena are also discussed in some detail. However, the safety driven activities for major modifications and new projects are being developed in DOE-STD-1189, *Integration of Safety into the Design Process*.

Post-Installation Readiness

After installation of new or upgraded security systems, an appropriate level of review needs to be conducted to ensure that system operability and safety requirements have been met, and that design objectives have been satisfied. A graded approach should be used to the extent practical. This section also recommends using existing readiness review processes rather than creating new ones.

Configuration Control

The need for configuration control of security systems is apparent. The concept presented in this section assumes separate paths (one for the safety basis process and one for the security process) that interface at opportune points. The Unreviewed Safety Question (USQ) process is required for security system changes to evaluate changes to the safety basis, as well as the DOE approval requirements on the safety basis documentation changes. A security change control process, which defines the DOE approval requirements, is required to evaluate changes in the security venue, whether the change was driven by security, safety, or operational requirements. This may be performed as part of the Site Safeguards and Security Plan (SSSP) configuration control.

Review Process for Improvements and Lessons Learned

The concepts presented in this topical report are intended to be “living processes” that are expected to be improved and updated over time. This section provides the framework for periodic reviews of the processes to incorporate lessons learned from, for example, external and internal assessments as well as process reviews.

Topical Report on Security and Safety Integration

Table of Contents

Section	Title	Page Number
Executive Summary		iii
Acronyms and Abbreviations		vii
1.	Introduction	1
2.	Drivers and End State.....	1
3.	Establish Terminology/Concept Crosswalk	3
4.	Awareness Training on Project Approach, Selection of Tools, and Terminology	5
5.	Integrated Project Approach to Safely Deploy Security Systems	6
6.	Alternative Analysis Process for System Selection	11
7.	Security Systems Toolbox: Development, Data Capture, Data Sharing....	14
7.1.	Develop Initial Data Sets.....	14
7.2.	Near-Term Systems Being Developed	16
7.3.	Data Sharing	16
7.4.	Standing Data Base	17
7.5.	Lead Site Concept	17
8.	Safety Basis and Security Documentation Integration.....	18
8.1	Discussion of Drivers and Their Implications.....	18
8.1.1	Safety Basis Implications	18
8.1.2	Security Implications.....	19
8.1.3	Safety Change Implications to Security	19
8.2	Major Modification and USQ Considerations.....	20
8.3	Hazard and Accident Analysis Process	21
8.4	Derivation of Controls.....	21
8.5	Security Information Protection	22
9.	Post-Installation Readiness.....	22
10.	Configuration Control	22
11.	Review Process for Improvements and Lessons Learned	23
12.	Summary	25
Appendix A	Security/Safety Crosswalk	26
Appendix B	Graded Safeguards (reference DOE M 470.4-6, Nuclear Material Control and Accountability)	36
Appendix C	Evaluation Criteria – Examples	37

Acronyms and Abbreviations

AEC/FEC	Area Emergency Coordinator/Facility Emergency Coordinator
AEGL	Acute Exposure Guideline Level
ALs	Administrative Limits
ASA	Auditable Safety Analysis
CAS	Central Alarm Station
CDC	Center for Disease Control
CFR	Code of Federal Regulations
CSDR	Conceptual Safety Design Report
DBT	Design Basis Threat
DNFSB	Defense Nuclear Facilities Safety Board
DOE	Department of Energy
DOE-HQ	Department of Energy Headquarters
DSA	Documented Safety Analysis
EDO	Emergency Duty Officer
EFCOG	Energy Facility Contractors Group
EPA	Environmental Protection Agency
EPIP	Emergency Planning Implementation Procedure
EPHA	Emergency Preparedness Hazard Assessment
ERPG	Emergency Response Planning Guideline
ES&H	Environment, Safety, and Health
ESE	DOE Office of Energy, Science, and Environment
FDAR	Facility Data and Approval Record
FSP	Facility Security Plan
GE	General Emergency
HASP	Health and Safety Plan
HAZOP	Hazard and Operations Analysis
HC	DOE-STD-1027 Hazard Category
HHS	Health and Human Services
IPT	Integrated Project Team
INL	Idaho National Laboratory
JCO	Justification for Continued Operation
LCO	Limiting Condition for Operation
MSP	Modified Security Plan
NNSA	National Nuclear Security Administration
NNSA-HQ	National Nuclear Security Administration Headquarters
NPH	Natural Phenomena Hazard
PAC	Protective Action Criteria
PC	Performance Category (PC-2 or PC-3 as designated in DOE-G-420.1-2 <i>Guide for the Mitigation of Natural Phenomena Hazards for DOE Nuclear Facilities and Nonnuclear Facilities</i>)
PDSA	Preliminary Documented Safety Analysis
PSEAG	Physical Security Equipment Action Group
PSO	Program Secretarial Office

Acronyms and Abbreviations (continued)

SAE	Site Area Emergency
S&S	Safeguards and Security
SAWG	Safety Analysis Working Group
SB	Safety Basis
SER	Safety Evaluation Report
SIDS	Security Information Data Set
SME	Subject Matter Expert
SNM	Special Nuclear Material
SSC	Structure, System, and Component
SSMR	Safeguards and Security Management Report
SSSP	Site Safeguards and Security Plan
TEEL	Temporary Emergency Exposure Limit
TSR	Technical Safety Requirements
TSWG	Technical Support Working Group
USQ	Unreviewed Safety Question
VA	Vulnerability Analysis
VAR	Vulnerability Analysis Report

1. Introduction

The scope of this effort is identified as: “Develop an integrated process involving both safety basis and security allowing achievement of Design Basis Threat (DBT) objectives while ensuring safety is appropriately considered.” This report was developed as a starting point for building a bridge between the requirements and practices within the security and safety disciplines. This report is not intended to be the final solution, but a catalyst facilitating communication and allowing the sites and facilities to meet the short-term DBT requirements and schedule. However, successful implementation has the potential of making this process a long-term solution for these facilities across the complex. This report proposes practices that are expected to reduce the cost of implementing the DBT evaluations and shorten scheduled implementation.

In addition to establishing a database and framework for sharing data on security system design and implementation, this process addresses the separation of requirements and interfaces between safety and security needs. This interface is partly met by defining when safety requirements provide the primary constraint and when security requirements provide the primary constraint [described in Section 3 of this report]. Key to the success of this process is early and open discussions between safety and security professionals [as discussed in Section 8 of this topical report].

This process does not add any requirements to the existing DOE regulations for security or safety. This process is intended to be a guide facilitating implementation of these requirements.

2. Drivers and End State

The key concept to consider in assuring that both the security requirements and safety requirements are satisfied for any security installation at a facility meeting the DBT is that the approach: 1) encompass all threats against which security systems are required to be designed and 2) be employed in an effective manner to assure neutralization and protect the national security. The process outlined herein, while having attributes helpful for long term application, was developed to concentrate on implementation of needed security features to meet the near-term DBT needs.

The key regulatory drivers to be considered are:

- (1) *Design Basis Threat Policy* (DOE Order 470.3A) – This DOE order identifies and characterizes the potential adversary threats to the DOE programs and facilities that could adversely impact national security, the health and safety of employees, the public, or the environment. This security directive is available from the Office of Security to cleared personnel with a need-to-know.
- (2) *Safeguards and Security Program* (DOE Order 470.4 and associated manuals) – This DOE order establishes the roles and responsibilities for the DOE Safeguards and Security (S&S) Program. The S&S Program consists of six key elements: 1) Program Planning and Management (DOE M 470.4-1 chg 1, 3-7-06), 2) Physical Protection (DOE M 470.4-2 chg 1, 3-7-06), 3) Protective Force (DOE M 470.4-3 chg 1, 3-7-06), 4) Information Security (DOE M 470.4-4, 8-26-05), 5) Personnel Security (DOE M 470.4-5, 8-26-05), and 6) Nuclear Material Control and Accountability

- (DOE M 470.4-6, 8-26-05). Specific security program requirements for each of the key elements are contained in the respective manuals (listed above). Effective security programs are developed and implemented utilizing all the requirements contained in the six manuals.
- (3) *Salient Consideration Memorandum* – Salient Considerations of the Design Basis Threat Annex Special Evaluation Team, dated June 25, 2004 from William J. Desmond, Administrator for Defense Nuclear Security/Co-Chair, Annex Special Evaluation Team NNSA, and Larry D. Wilcher, Director, Security Policy Staff/Co-Chair, Annex Special Evaluation Team Office of Security.
 - (4) *Nuclear Safety Management Rule* (10CFR830) – This rule covers all actions that affect, or may affect, the safety of DOE nuclear facilities. The need to achieve a security posture in response to the DBT does not eliminate the need to comply with federal regulations as set forth in the Nuclear Safety Rule. Rather, the need is to concentrate on deploying the needed security elements while maintaining compliance with 10CFR830.
 - (5) *Facility Safety* (DOE Order 420.1 and Guides) – This DOE directive and the associated guides establish facility programmatic safety requirements for DOE (ESE and NNSA) for nuclear and explosive safety design criteria, fire protection, criticality safety, Natural Phenomena Hazards (NPH) mitigation, and the System Engineer Program. There are specific requirements for design considerations in the associated guides and standards that need to be addressed while making modifications in response to the DBT. Although all changes must be assessed against their potential impact on the facility Safety Basis, an example with the most significant impact would be the requirements invoked if the new or upgraded security system results in a major modification to the facility under 10CFR830.
 - (6) *Integration of Safety into the Design Process* (DOE-STD-1189-2006) – This standard is being developed for issue along with the revision to DOE-O-413.3 *Program and Project Management for the Acquisition of Capital Assets*. This Standard provides expectations for incorporating Safety-in-Design for facilities whose intended purposes involve the handling of hazardous materials, both radiological and chemical, to provide adequate protection for the public, workers, and the environment.
 - (7) *Worker Safety and Health Program Rule* (10CFR851) - This new rule may have an impact on the selection and implementation of security elements and therefore, must be part of the decision process. It establishes requirements for a worker safety and health program, including fire protection that reduces or prevents occupational injuries, illnesses, and accidental losses by workers with safe and healthful workplaces at DOE sites. Implementation details of this new rule should be assessed as this process moves forward. As the impact of the rule is determined, the results should be integrated into this process.

The expectations or end state resulting from this topical report and associated implementation program elements include:

- (1) A recommended process for handling the documentation of the security and safety disciplines, including an appropriate change control process and participation by all

stakeholders in the facility that may be impacted by the change (e.g., facility operations personnel, Documented Safety Analysis (DSA) developers, and facility management).

- (2) A means to package security systems with sufficient information to help expedite the flow of that system through the process. In addition, a means to share successes (including all lessons learned) among sites, to include information and safety basis to the extent such information is transportable.
- (3) Identification of key security systems and associated essential security elements being installed, and an arrangement for the sites installing these systems to host an appropriate team to review a specific system and determine what information is exportable.
- (4) Identification of the security system essential elements and appropriate controls required for testing of these essential elements in the facility.

For this process to work effectively, it should be applicable to all facilities and have implementation feedback as an integral part of the overall process. Accordingly, this process requires input and participation from both safety and security professionals and the associated decision makers at each participating site.

The expectation for the solution reached for each site recognizes that assuring adequate safety and security is the goal and that 100% assurance in either case is not practicable. Risk of an accident or security breach will never be zero. Therefore, the focus is on providing adequate and appropriate protection in these areas with consideration of other project elements, such as cost, schedule, operability, mission, etc. Thus, the final solution balances each of these parameters to reach the appropriate solution for the facility under consideration. The evaluation process is typically addressed using a systems engineering approach such as that discussed in Section 6 of this report.

3. Establish Terminology/Concept Crosswalk

To effectively integrate the safety and security processes as outlined in this topical report, there is a need for a common understanding of the requirements, concepts, and terms on which each group relies. This report is intended to inform and familiarize security professionals and safety professionals with the regulations, requirements, and issues governing the functions of their counterparts. It is not the intent of this section to complete this familiarization process, but to highlight some of the differences that may exist between the two disciplines, and thus provide a starting point from which communication can be initiated and integrated solutions identified.

The inherent differences in requirements and expectations result in two different sets of terms, regulations, and goals for success that if understood, allow success in both venues and satisfy all acceptance criteria. At the top level, the acceptance criteria for a facility or project requires that both safety and security requirements be satisfied. Neither set of regulations takes precedence over the other within the scope of the applicable regulatory requirements. However, there are conditions for which individual regulations do not apply. For example, DOE-STD-3009, CN3 excludes sabotage and terrorism from the scope of the hazard and accident analysis performed in support of the facility nuclear safety basis. Although acts of

sabotage and terrorism are excluded from the hazard and accident analysis scope, this does not preclude the need to analyze and describe security systems and associated accident conditions in the safety basis for the facility. On the other side, a threat (perceived or real) in which security personnel are alerted changes the relative significance of the criteria. In this case the ES&H requirements are not applicable if they are in conflict with the security response. Protection of the material is the highest priority and provides the greatest safety for all.

There are three key differences that need to be addressed to provide an appropriate platform within which security and safety issues can be integrated.

- Definition of success (goals)
- Regulations and expectations
- Terms and definitions

The definition of success within the Environment, Safety & Health (ES&H) discipline is to assure that the complete spectrum of potential accidents that could expose members of the public, onsite workers, facility workers, and the environment to hazardous materials has been evaluated and appropriate protection provided. The definition of success within the security discipline is to develop protection strategies for threat level 1 through 4 facilities that achieve acceptable protection system levels. These two definitions of success often lead to conflicts that must be resolved for the project to successfully move forward. The most obvious point of confrontation between these venues is personnel evacuation in the event of an off-normal condition. For example, life safety considerations in the event of a facility fire require the workers to promptly and completely evacuate the facility, however, security considerations (SNM accountability for example) may present barriers that prevent workers from immediately or completely vacating the facility. Project success requires that both of these competing sets of requirements and expectations be met. This may drive solutions that are non-traditional to fully satisfy both sets of requirements. A key factor in successful resolution of this conflict is the integration achieved through the alternative analysis.

The implementation requirements (regulations) that drive the key actions for both security and safety derive from the following regulations:

- 10CFR830 (*Nuclear Safety Management*) and associated safe harbor programs within the Rule
- 10CFR851 (*Worker Safety and Health Program*)
- DOE-O-470.3 (*Design Basis Threat Policy*) and associated manuals and guides
- DOE-O-470.4 (*Safeguards and Security Program*) and associated manuals
- Adversary Capabilities List (ACL) - *Terrorist Adversary Capabilities List*, dated February 18, 2004, from Linton Brooks, Under Secretary for NNSA and Robert Card, Under Secretary for Energy, Science, and Environment
- Salient Consideration Memorandum - *Salient Considerations of the Design Basis Threat Annex Special Evaluation Team*, dated June 25, 2004 from William J. Desmond, Administrator for Defense Nuclear Security/Co-Chair, Annex Special Evaluation Team NNSA, and Larry D. Wilcher, Director, Security Policy Staff/Co-Chair, Annex Special Evaluation Team Office of Security

- *Vulnerability Assessment Process Guide*, dated September 30, 2004, from Marshall O. Combs, Director, Office of Security, Office of Security and Safety Performance Assurance

To facilitate this understanding a crosswalk between the security and safety terms and expectations has been initiated. This initial crosswalk of terms and concepts is provided in Appendix A. As there is not a one-for-one alignment of terms and concepts, the appendix can not provide a clean roadmap between the two disciplines. However, the concepts have been generally arranged to facilitate an understanding of the differences.

4. Awareness Training on Project Approach, Selection of Tools, and Terminology

To effectively transport the selected security concepts among the various sites, a consistent approach to training and terminology is needed. As this consistency should be developed along with the security system, the purpose of this section is to establish the overall approach to developing the training and consistent terminology for the system. This discussion focuses on ideas and concepts that would enhance the portability of training procedures and programs for the various proposed security systems to multiple DOE sites. For example, in some cases, security has requested that security systems be operationally tested at the vendor site prior to shipping and onsite deployment. During this functional checkout period, security and safety professionals may be required to observe all aspects of operation and testing for these systems before the systems are released for shipment to the applicable site. Additionally, vendor training provided at the factory for some security systems may be required to familiarize site maintenance personnel, systems engineers, and safety analysts with the maintenance and operation of the systems, in addition to the provided support of any setup testing on site.

Integrated Safety Management System principles should be incorporated in project execution planning and in establishing scope and technical requirements for the security system using a tailored approach. A needs and impact analysis should be conducted to determine the basis for the design and development of the training program. Additionally, it is recommended that training procedures associated with the security systems be developed in time to support all associated internal and external reviews.

Project interfaces need to be established, implemented, and maintained among the organizations and disciplines participating in the design and implementation process. Interface controls include communications, identification of responsibilities and written procedures. The vendor may be required to provide design review/support personnel to interface with facility system engineers and facility safety personnel in a capacity to answer any questions/concerns about the equipment and how facility personnel and/or the facility safety basis may be affected.

Consideration should be given to having the security system vendors observe and monitor (where permissible) the final installation and onsite shakedown testing of these systems. This vendor support provides an opportunity to comment on such concerns as location-specific maintenance that may be required due to environmental or operating conditions. The vendor may also assist in assessing implementation-specific parameters and acceptance

criteria for the system during the test period. Note that this may require some vendors to be cleared.

Procedures should incorporate appropriate and pertinent information from source documents, such as facility design documents, safety basis documents, and vendor technical manuals. Prior to approval for the first deployment of any selected security system, all associated facility operational and maintenance procedures should be completed and be available to accompany future deployments at other sites. Modifications to these procedures should be made at each site prior to approval for deployment, incorporating installation-specific revisions to the base procedures.

5. Integrated Project Approach to Safely Deploy Security Systems

Prior to selection of new or upgraded security systems to meet the DBT, an integrated evaluation of available alternatives should be performed. The integrated evaluation is to ensure integration of safety, security, operations, and governmental policy. The integrated evaluation involves establishing a project management team structure with participation from appropriate security, safety, and operations representatives. Figure 5-1 provides a process flowchart to effectively deploy new or upgraded security systems to meet the DBT, while ensuring compliance with applicable safety requirements. The process begins with recognition of a change in security protection requirements, such as a change in the DBT or with the results of an ongoing SSSP review. Security personnel then perform a vulnerability analysis (VA) of the DBT changes. The VA can be in the form of computer simulation, field exercises, or other approved means, consistent with the methodology described in the *VA Process Guide*.

DOE M 470.4-1 chg 1, *Safeguards and Security Program Planning and Management*, Part 1, Section E – “Vulnerability Assessment Program,” outlines the general requirements to conduct a VA and contains information about planning assumptions, threats, targets, modeling, performance testing, results, quality assurance, figures of merit, critical system elements, VA reports, system effectiveness, training and certification. Additional VA Program requirements are contained in:

- 1) DOE O 470.3A, *Design Basis Threat Policy*;
- 2) Adversary Capabilities List, February 2004;
- 3) VA Process Guide, 9-30-04;
- 4) Salient Considerations Memorandum, 6-25-04;
- 5) DOE Manuals 470.4-2 *Physical Protection*, 470.4-3 *Protective Force*, and 470.4-6 *Nuclear Material Control and Accountability*;
- 6) *Consolidated Guidance Concerning the Required Format and Content for the Design Basis Threat Implementation Plans and Quarterly Updates*, dated February 1, 2005, from Glenn S. Podonsky, Director Office of Security and Safety Performance Assurance;
- 7) *2004 Design Basis Threat Implementation Plan Vulnerability Assessment Requirements*, dated November 16, 2005, from CDR Robert F. Brese, USN, Acting Director, Office of Security Oversight;
- 8) *Modified Probability of Hit/Kill Tables*, dated December 16, 2005, from the Office of the Associate Administrator for Defense Nuclear Security (NA-70); and

- 9) *Establishment of Force-on-Force Performance Test Working Group*, dated May 16, 2005, from Glenn S. Podonsky, Director, Office of Security and Safety Performance Assurance and William J. Desmond, Associate Administrator for Defense Nuclear Security.

The VA Process Guide provides the VA Analyst with the minimum process requirements/expectations (at the macro level). The VA Process table of contents includes: 1) Threat Characterization, 2) Target Determination, 3) Scope Definition, 4) Facility/Site Characterization, 5) PF Characterization, 6) Pathway Analysis, 7) Scenario Development, 8) Neutralization Methodology, 9) System Effectiveness Methodology, 10) Upgrade Analysis, 11) Implementation, etc.

When the VA identifies a shortfall in protection measures, an analysis of possible upgrades to the security system is required. The upgrade may require deployment of new or upgraded security systems. To ensure that safety considerations of the upgrade are properly analyzed, a project team approach is applied. The shortfall in the protection measures is defined by the VA process in the form of a “problem statement” that the project team uses as the basis for identifying the most effective (from both a safety and security perspective) option for satisfying the problem statement. The security representatives on the integrated project team provides a briefing of the problem statement at the site and the known list of available technologies to the integrated project team (IPT).

If no known options are available a market search is conducted for technologies that may address the shortfall. If no options are identified to meet the objective, a development effort is required. The IPT would bring in the appropriate system development subject matter experts (SMEs) to design a concept that would meet the DBT for the application under consideration. Since no other alternative was defined in the initial assessment, once developed, the solution becomes the single solution and the IPT can proceed to the “Selection of Security Systems” block in Figure 5-1.

If there is only one option available to address the shortfall, the IPT can proceed to the “Selection of Security System(s)” block in Figure 5-1 and then submit the selection to DOE for approval of the selected security system.

If multiple options are available a formal alternatives analysis may be performed using a formal method, such as Kepner Tregoe and/or pairwise comparison. [Section 6 of this report has more details on performing an alternatives analysis.] The alternatives analysis should result in a recommended security system or upgrade. DOE approval of the recommendation should be documented through a formal security evaluation report as noted in Section 8 of this report.

After selection of the system upgrade, a project execution plan should be developed (or refined if one was generated earlier) to procure, analyze, design, train, test, and deploy the new or upgraded security system. A change control process should be applied to the new or upgraded security system selection. [See Section 10 of this report for guidance on application of the change control process.] Change control includes application of the USQ process to address the impact on safety and a security change control process to determine the depth of analysis required and the DOE approval requirements for the modification. It is recognized that the security change control process may need to be developed further at some sites.

In concert with the change control process, DOE and the contractor determine if the new or upgraded security system could be a 10CFR830 major modification to a nuclear facility. [See Section 8.2 of this report for more information on major modifications and the USQ process.] If DOE and the contractor determine that the new or upgraded security system results in a major modification to a nuclear facility, then a Preliminary Documented Safety Analysis (PDSA) is required and must be approved by DOE prior to procurement. The PDSA and its precursor document (Conceptual Safety Design Report) are expected to be developed in concert with the design of the new or upgraded security system. The PDSA and CSDR define the safety features and the safety classification of those key features. Additionally, they establish design requirements associated with the safety functions, such that the system is designed and procured to the appropriate standards. These documents and specific implementation requirements will be more fully described in DOE-STD-1189 *Integration of Safety into the Design Process* planned for RevCom in October 2006.

DOE documents approval of the PDSA through a Safety Evaluation Report (SER), allowing procurement to proceed. DOE may approve limited procurement and construction as described in DOE-G-421.1-2, *Implementation Guide for use in Developing Documented Safety Analysis to meet Subpart B of 10CFR830*. As the security system is being installed, a DSA and Technical Safety Requirements (TSR) for operation will be prepared. Prior to deployment of the security system, DOE must approve modifications to the facility DSA and TSR with an SER and any changes to security plans with a formal security evaluation report. [Section 8 addresses the concept of a security evaluation report.] Once the system is installed, training is complete, and the DSA and TSR changes approved, an integrated readiness review following the tenets of DOE Order 425.1B, *Startup and Restart of Nuclear Facilities* should be performed. The purpose of the readiness process is to ensure personnel, procedures, and equipment are ready to effectively and safely deploy the security system. [See Section 9 of this report for more information on the readiness process.] The results of the security and safety evaluations should be posted within the data system toolbox to allow for portability to other sites. [Section 7 provides the conceptual basis for the security information data set (SIDS) supporting this portability between sites.]

A strong corporate culture and infrastructure supporting integration of security and safety disciplines are fundamental to a successful execution of a security project. Additionally, a clearly articulated management commitment to integration of the two disciplines is needed to ensure the easiest, quickest, and most successful implementation of the near-term DBT requirements.

Quality assurance requirements driven by the safety requirements may also be a factor in system selection and implementation. For example, security technologies that rely on software or firmware for safe/reliable implementation of the technology often have specific requirements that need to be addressed early in the technology development process. In these cases, quality assurance professionals need to be integrated into the team early in the planning process. Software verification and validation driven by the software quality assurance requirements of DOE-N-203.1, *Software Quality Assurance* may be a major factor in the project schedule and cost, and need to be addressed early. These software quality assurance requirements may also be a factor in the technology selected.

The standard project management process and principles should be used, but with assurances of involvement of a multi-disciplined team approach. It is important that the IPT include DOE representation from both disciplines. Key steps to ensure success include:

- Select a project manager to lead the effort
- Define clear lines of authority and responsibility
- Provide necessary resources (staff and funding)
- Use an integrated team approach, inclusive of applicable disciplines (e.g., facility operations, physical security, emergency response, protective force, risk management, legal, security and safety basis subject matter experts, and other safety and health disciplines)
- Identify and observe applicable rules, regulations, and requirements
- Use evaluative system engineering tools (e.g., alternate analysis/pair-wise comparisons) for optimizing both security and safety options
- Prepare a final report summarizing the selection process, clearly explaining the rationale, results, and conclusions
- Develop security system specifications (e.g., failure data, safety controls, capabilities, inherent hazards, and functional and operational requirements) supporting both design and safety analysis processes
- Develop and adhere to a realistic and achievable schedule with logic ties and deliverables

As this process matures, a plan for the most effective implementation of each of these steps should be developed and documented.

The successful application of the integrated project management process is likely to result in conflicting requirements/desires, necessitating the need to strike a rational balance between safety and security expectations. In these cases, productive communication between the stakeholders, including all applicable disciplines within the contractor and DOE organizations, is essential.

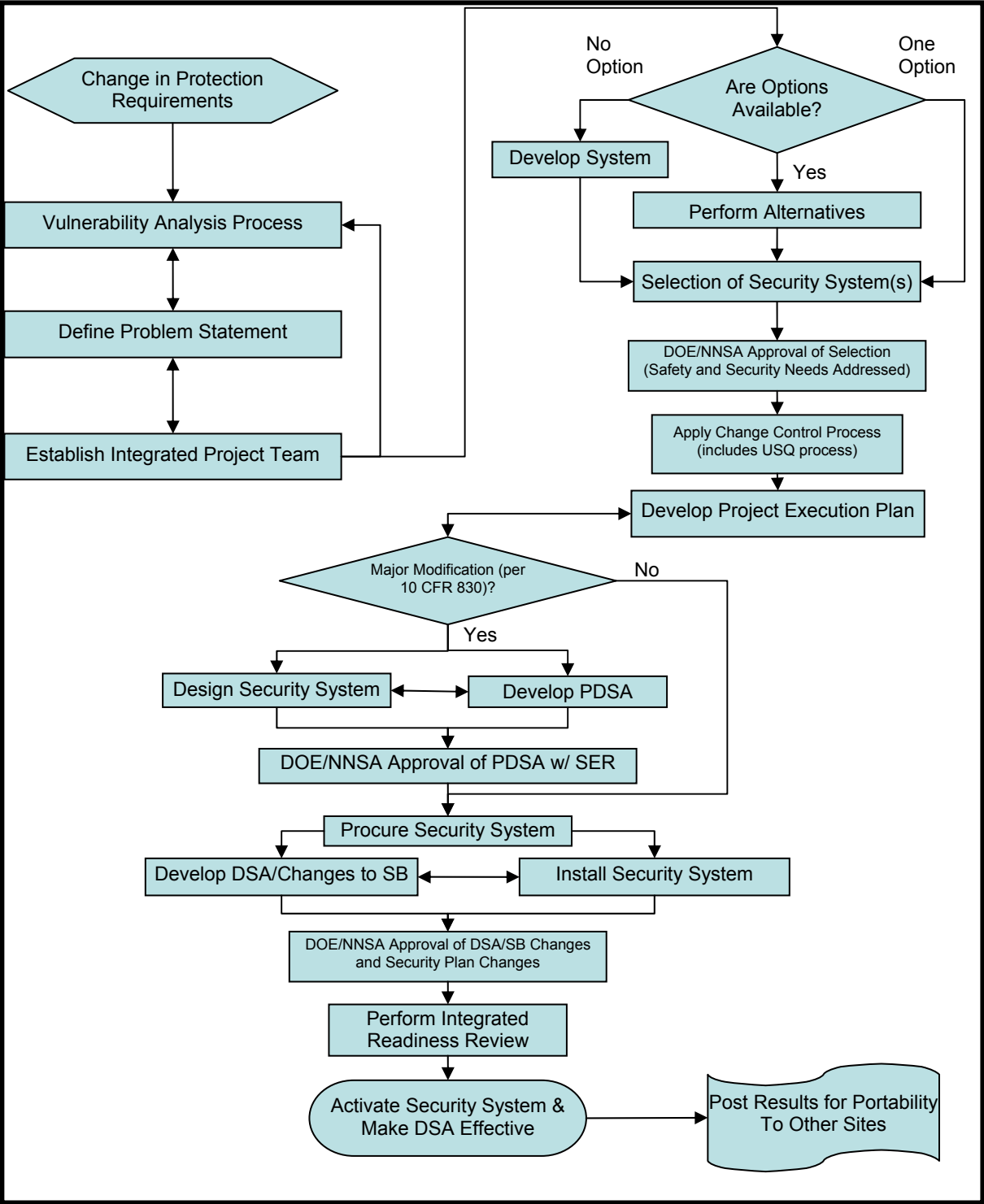


Figure 5-1

Security System Deployment Process Diagram

6. Alternative Analysis Process for System Selection

As described in Section 5 above, a key step for integration of safety and security, as well as selecting security technology, is to clearly identify the problem statement and the objective of the upgrade. This objective needs to be clearly stated and communicated among all IPT members. The objective is the compass for the IPT when evaluating potential alternatives. An alternative analysis approach is summarized below and presented graphically in Figure 6-1.

Once the objective is identified, the project team establishes minimum acceptable requirements for all impacted stakeholders. For example, input may be from a safety, security, operations, maintenance, or any other perspective deemed important enough by the project team to eliminate a particular security technology from further consideration. Such requirements are referred to as “Musts” and are simple statements that when applied to a particular security technology a “Yes” or “No” answer may be obtained. The intent is to reduce the list of potential alternatives to only those that are credible as early on in the evaluation process as possible. Documentation of which specific security technologies failed to meet any of the “Must” criteria is key to developing a defensible selection process. The “Must” designation is a key factor in assuring that all discipline requirements are addressed early in the system selection process.

After the “Musts” are developed, the project team establishes desirability criteria for the security technology to meet the objective. These desired attributes are known as “Wants” and some potential alternatives will meet these better than others. As with the “Musts,” these “Wants” should include input from all stakeholders. They may be from a safety, security, or any other perspective deemed important by the project team. Rationale for the “Wants” along with creation of a “dictionary” provides a mutually agreed upon definition of the “Want” and helps to maintain consistency in terms will be valuable in making and documenting a defensible selection process. An example set of “Musts” and “Wants” is provided in Appendix C.

Once the “Wants” are established, the project team develops a weighting system to determine the relative importance of each “Want.” This allows potential alternatives to be compared to one another, or “scored,” on the basis of how well they meet established “Wants.” The weighting system may be an overall comparison or a pair-wise comparison of all “Wants.” Typically, an overall comparison is used for small numbers of “Wants” and a pair-wise comparison for larger numbers. In the end, the project team needs to choose which system works best for their project.

After a clear objective is defined and “Musts” and “Wants” are established, a list of potential security technologies is developed. Typically, this is done by a small group of SMEs who are very conversant in the available choices. This process should be approached in a brainstorming spirit. That is, SMEs should not be allowed to immediately exclude or drop possible alternatives based on their subjective experiences or opinions. This exercise should be conducted with the attitude of, “What are all of the security technologies available, even those that have only a small potential of meeting the overall objective?”

Each of the possible alternatives is then evaluated against each of the “Must” criteria. As previously indicated, these criteria are a simple “Yes or No”. Alternatives that fail any single

“Must” criteria are removed from further consideration. Documentation of the alternative and the specific criteria that failed is critical to the integrity of the selection process and later questions regarding the adequacy of the evaluation.

All alternatives passing the “Must” evaluation are scored using the weighted “Wants” criteria. All alternatives are then ranked according to their weighted score. From this, a short list of the top scoring alternatives is developed. Only those alternatives with similar scores are considered. For example, if the top three scoring alternatives are separated by five points, but the third and fourth are separated by eight points, only the top three alternatives are included on the short list. More or fewer alternatives go onto the short list according to the similarities in scoring. Note that it may be important to look at attractive attributes of the second tier of candidates to see if modifications may be appropriate in the selected system that would have changed the outcome of the ranking process. Vendors may be willing to “improve” their design to accommodate the enhanced system configuration.

Relative risks of each alternative on the short list should be reviewed. The risks considered should include all aspects of each alternative. Examples may include: impact to facilities, ease of acquisition or installation, experience base, reliabilities, maintainability, etc. A preferred security technology can then be selected if the ranking and risk consideration reveal a single best alternative.

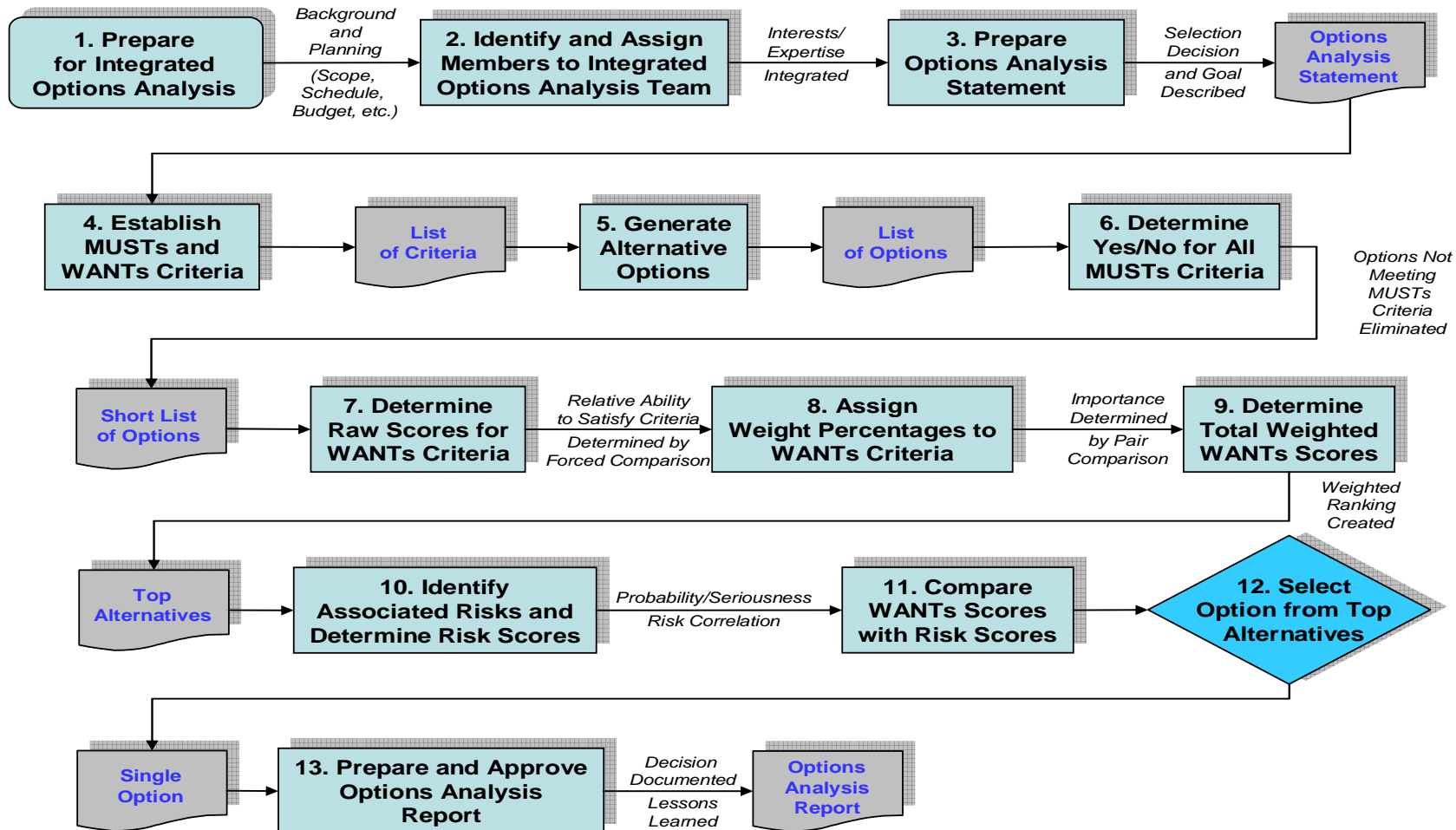
If the short list of the highest ranked alternatives and risks are considered similar, additional “Want” criteria should be developed. The additional criteria are weighted as necessary. However, in many cases, all additional criteria are considered equally important. Once the alternatives on the short list have been scored using the additional “Want” criteria, a final selection can be made.

A thorough, but concise, final report on the selection process should be prepared. The purpose of this document is to provide an easily understood explanation of the selection of a particular alternative from a number of viable alternatives. Professional judgment and opinions are valid justifications in the selections process so long as the logic and rationale are included to explain the thought process. The final documentation should include dictionaries or other documentation generated to build the decision making framework as appendices.

Note on the Alternative Analysis Process

As a side benefit, the establishment and weighting of “Wants” by the project team will also serve as a “team building” exercise if all parties are able to participate equally in deciding which “Wants” are most important. This process allows team members to both be heard and see other perspectives. It emphasizes competing objectives and focuses on the importance of collective consensus decisions to achieve the best solution. An independent facilitator is important during these deliberations to guard against “group think” and to ensure that opposing views are heard and dispositioned. It is important to assure that the SMEs are solicited and heard by the team. Note that it may be important for the independent facilitator to allow the discussion of the importance of the individual “Wants” to be in the team meeting, but have the actual weighting to be performed independently, with only the facilitator knowing the actual final weighting factors. This helps to assure the validity of the outcome of the evaluation. Most important, issues that cannot be resolved should be elevated to senior management for resolution.

Figure 6-1 Integrated Options Analysis Process



7. Security Systems Toolbox: Development, Data Capture, Data Sharing

The intent of the tool box process is to identify and provide information to sites within the complex to expedite procurement and deployment of security systems that meet applicable security and safety requirements. This process ensures that the following are accomplished:

- (1) identify data elements needed to develop a package of security system options
- (2) capture key decisions and relevant data used to approve a system
- (3) define information to be supplied by vendors/system developer
- (4) identify how DOE can pre-approve key features of security systems and make sure those features are portable to multiple sites with minimal additional evaluation
- (5) capture and/or update performance data for the security technology

However, it is noted that site-specific or implementation-specific evaluations will always be required to assure that there are no interface issues at the site where the system is deployed. To develop the appropriate security system toolbox, the approach is developed in the following subsections.

7.1. Develop Initial Data Sets

The initial data sets should come from reviewing the key security systems currently being implemented at various sites. Once that initial data set is captured, emphasis shifts to a team approach to identifying upcoming safety systems. For review of ongoing security systems, a lead/host site should be designated to establish security and safety analysis input information. [See section 7.5 for a discussion of the Lead Site concept.] Examples of analysis input information include the following:

- Control derivation
- Hazard and accident analysis basis
- Test and failure data
- Alternative analysis reports
- Product specifications
- Performance specifications
- Procurement specifications
- Design and installation packages
- Failure Modes and Effects Analysis (FMEA)
- Reliability and maintainability data, including maintenance requirements and plans
- Analysis of Inadvertent Discharge
- Software Quality Assurance (including Verification and Validation)
- Application considerations (i.e., new facility vs. existing facility; interior or exterior; delay or denial; etc.)
- Readiness process
- Training for both safety and security needs

- Equivalency analysis for vendor modifications and updates
- System Engineer documentation on systems and specifications
- Associated structural analysis for mounted designs
- Security evaluation results (e.g. Site Assistance Visits, Inspection and Evaluation results, etc.)
- Credited controls

A determination as to whether the system deployment would constitute a 10CFR830 major modification determination would be required. This would include impacts or design changes to existing facility systems to include safety significant or safety class systems, impacts to existing Technical Safety Requirements (TSRs), safety class/safety significant control treatment, and quality requirements (including software). The initial systems to be addressed in this process include:

- (1) Dillon Aero, 7.62 AP, mobile and fixed platforms
- (2) ROWS, 5.56 or 7.62 AP, mobile and fixed platforms
- (3) MK-19, 40 mm
- (4) Secure transport vehicles
- (5) Inert Gas Systems
- (6) Fixed Foam Systems
- (7) Generic Command and Control System

Additional systems and technologies are being assessed and can be added as appropriate. This includes systems and technologies that are ready for deployment and those being developed. Specificity for these elements is required as this process moves toward implementation.

In order to standardize and optimize the data capture performed by these security system review teams, a checklist should be developed as an aid. Potential ideas for the generic checklist of desired data elements include:

- (a) Identify what data are portable
- (b) Structural impacts and loadings, PC-2 or PC-3 design
- (c) Accidental Discharge Analysis
- (d) Hazard analysis
- (e) White papers
- (f) Development of positive USQ, evaluation of the safety of the situation, and addendum to DSA
- (g) Training Programs – Standardized Training
- (h) Software Quality Assurance

For cases where a site hosts discussions on a particular system, the team sharing the data prepares and disseminates what they learned from the process in a final report. These reports will be used to populate the standing data base described below. Team reports and documents issued should prescribe processes and methodologies used, specify requirements,

or establish design when items, services, and processes that are not currently in use in the complex are identified.

An important aspect of maintaining the integrity of the database is independent peer review of the information placed into the database. To achieve this review and assure that the security system (and associated information) has the best portability to other DOE sites, it is recommended that entries receive an independent SME review, preferably from other sites. It is expected that this peer review may require personnel outside of DOE to achieve an appropriate level of scrutiny (e.g., Department of Defense). This peer review would require both safety and security professionals on the team. Thus, the review may have to be driven at the Central Technical Authority and Chief of Defense Nuclear Security Safety level of DOE to assure that appropriate SMEs are brought into the process.

7.2. Near-Term Systems Being Developed

As the focus is on the near-term deployment, the initial evaluation is based on anticipated security systems that can be fielded between now and 2008. This initial listing allows the team to determine any additional key security systems that may be used in meeting the current DBT, as well as driving security upgrades. A key element of this evaluation is to determine which systems have the potential to be extended to other sites. An inventory of emerging security systems should be generated to ensure this common approach is applied early in the conceptual phase. By applying a standard approach and leveraging lessons learned from previously installed systems, it may be possible to shorten the design/approval cycle for the emergent projects. The inventory of emerging projects should be compiled from the upgrade actions defined in the various DBT Implementation Plans from the Office of Defense Nuclear Security and the Office of Energy, Science, and Environment. To ensure completeness, the effort should be coordinated with the Security Technology Deployment Programs of the Office of Security Technology and Assistance (HS-80) and the Office of Defense Nuclear Security (NA-70). When appropriate, interfaces with the Physical Security Equipment Action Group (PSEAG) and the Technical Support Working Group (TSWG) may improve collection of system performance and safety data.

As an added benefit, the database can also be used as a tool for security system developers to both review data for existing systems (including installed and available), as well as a guide for the data requirements and expectations for developing systems.

7.3. Data Sharing

Once the data is gathered, it is important to share that information with both the security and safety personnel at other sites to ensure viable options are known, and options that failed are not repeated. The intent is that this information be placed on a controlled, electronically accessible platform that would allow personnel at the various sites to access the information as needed, but within the limitations driven by the security classification of the information.

To assure that the data is appropriate for use, a configuration management program needs to be implemented for the database. This should include a peer review of the information before it is available for use within the database.

It is expected that two levels of information will be provided in the database. First would be the primary data set that has the key verified information for the security technology. The

second is a set of supporting or lower tier information that is available for consideration by a reviewer, but not as formal as the primary approved data set. This may include comments, test results, USQDs, etc.

7.4. Standing Data Base

To be of use, data must be made available to multiple sites. This requires the creation and maintenance of an accessible data base at the classification level required to contain useful information and on an electronically accessible platform that is available to all sites. The scope of that data base should include the essential elements for key security systems currently deployed, security systems being developed (HQ point of contact), security systems being considered at various sites, and insights in development of DBT accident base case concepts that would envelop a variety of scenarios.

A targeted information checklist should be jointly developed by security, safety, and operations personnel for use in site data gathering and retrieval visits. This list can be refined as teams begin working together. Elements to be considered for this checklist include:

- systems characteristics
- key features for safety
- derivation of administrative controls
- issues found during approval process
- options reviewed that were not of value
- system owner (i.e., host site)

Key issues that will need to be resolved include the host platform and location for the database, configuration control of the database, and classification level of the database. These issues should be jointly resolved with the safety team and the Security Directors.

7.5. Lead Site Concept

Based on the implementation schedule and limited resources to develop needed security technology, the team proposes the use of a “Lead Site” or “Host Site” approach to deploying security technologies and developing the information required for the safe deployment of the technology at the applicable DOE sites. The “Lead Site” would be the site that identifies the need for the technology and starts the development of the technology. Thus, a single site would be identified as the lead for a particular security technology and as host, solicit input and direct interaction from other sites with interest in the same security technology. This approach allows the combined resources of several sites to share information and build the needed security and safety information in the database that is intended to facilitate implementation of the technology at other DOE sites. This approach is expected to limit the analysis and development efforts to only that required for the specific deployment at the other sites and not force a total duplication of efforts. Key in this effort would be the joint effort in developing the procurement specification and essential elements of the technology. Additionally, the required safety controls in many cases may be directly transportable to the other sites that deploy the technology. To assure that this development effort is managed appropriately, NNSA/DOE-HQ would coordinate and manage this development effort.

8. Safety Basis and Security Documentation Integration

8.1 Discussion of Drivers and Their Implications

The selection or upgrade of a security system to meet the DBT involves identification of practical alternative systems that not only satisfy the security needs, but also consider characteristics such as operational efficiency, cost, and safety (exclusive of malevolent acts). As outlined in Section 6, this selection should be based on a disciplined documented analysis.

The security system selection process includes a security evaluation process to determine that the appropriate system is developed and deployed. Once a system selection has been made, it is necessary for DOE security offices to approve the choice. Approval may be accomplished by a security evaluation or other appropriate DOE approval mechanism. This DOE security approval mechanism is the security equivalent to the SER providing DOE authorization (or conditional approval) to proceed with the security system procurement, installation, and deployment. Once approved by DOE, the security upgrades are identified in the Site Safeguards and Security Plan (SSSP) and the Design Basis Threat Implementation Plan.

It is also necessary to perform an Unreviewed Safety Question (USQ) determination to assess the potential safety basis impacts of the proposed system. If required (i.e., positive USQ), DOE approval of changes to the facility safety basis must be sought. This is done through modifications to a facility DSA and TSRs, the approval for which is documented in a DOE-issued Safety Evaluation Report. Note that, as presented previously, if the change constitutes a 10CFR830 major modification, then a PDSA is required before the project can proceed with procurement and final design.

8.1.1 Safety Basis Implications

10CFR830 requires that facility hazards be analyzed and that hazard controls be implemented so that adequate protection is achieved for the public, workers and the environment. When a security system is put into place in a facility, accidental or unintended discharge could present a hazard to workers and/or the public.

Accidental or inadvertent discharge must be addressed for all credible scenarios. These events could be caused by human error, faulty security system design, or internal or external hazards. Examples of accident initiators that could actuate the security system and exacerbate accident consequences include facility events (e.g., fires) and natural phenomena hazards (e.g., seismic).

Moreover, accidental discharges could initiate accidents such as hazardous material releases, fires, nuclear criticality, leaks, or damage to safety SSCs or process systems. Depending on the characteristics of the security system and the facility, the installation could be considered a major modification of the facility. In that case, 10 CFR 830 would require the preparation of a PDSA and application of the nuclear safety design criteria of DOE O 420.1B, *Facility Safety*.

Installation of a new system would trigger a comprehensive change control process. To address the impact on safety, the change would involve entering the USQ determination process and the modification of the facility's safety basis to include consideration of the

safety aspects of the new system. If the USQ determination is negative, DOE approval of the change would not be necessary for the safety review. If the security review is also negative, DOE approval of the change would not be necessary. However, it is recommended that a security configuration control process be employed for those systems deemed critical to the security posture (see Section 8.1.2). This would include the essential elements of those systems.

Similarly, a security system deployed outside of a nuclear facility that had the potential of affecting facility safety as a result of unintended actuation would also trigger the USQ process. This would also require an analysis of those potential effects and the identification of safety controls that might prevent or mitigate the event.

8.1.2 Security Implications

The new or upgraded security system may also have implications in the security venue. A process involving change control, vulnerability analysis/evaluation, etc. culminating in DOE approval must be followed. It is essential that the security and safety basis processes be coordinated to ensure safe and secure operation of the proposed change without delays caused by the opposite review and documentation approval process. Implementation of the new or upgraded security system will require changes to facility specific security plans. An evaluation of impact to the existing physical security and/or administrative controls specified in the security plan must be completed. If an impact exists, then a revision to the security plan must be completed and submitted for DOE approval. DOE evaluates the acceptability of the revised control set and approve with or without conditions of approval. The basis for DOE acceptance of the physical and administrative controls should be formally documented in a formal security evaluation report. This security evaluation should document the review activities (i.e., facility walkthroughs, documents reviews, interviews, etc.), basis for recommended approval and/or basis for conditions of approval, criteria for acceptance, and the evaluation.

8.1.3 Safety Change Implications to Security

As security upgrades may impact safety authorization, any new or upgraded safety system may have implications in the security venue. A process involving change control, vulnerability analysis/evaluation, etc. culminating in DOE approval must be followed. It is essential that the security and safety basis processes be coordinated to ensure safe and secure operation of the proposed change without delays caused by the opposite review and documentation approval process. Implementation of the new or upgraded safety system may require changes to facility specific security plans. An evaluation of impact to the existing security physical and/or administrative controls specified in the security plan must be completed. If an impact exists, then a revision to the security plan is required to be submitted for DOE approval. DOE evaluates the acceptability of the revised control set and approve with or without conditions of approval.

8.2 Major Modification¹ and USQ Considerations

In some cases the new or upgraded security system (i.e., change) may be considered a major modification in accordance with the Nuclear Safety Rule, 10CFR830. In these cases, the addition of the system potentially results in a significant change to the safety basis for the facility or facilities in which the system or upgrade will be installed. The implication of classification as a major modification is that a PDSA must be prepared and approved (through an SER) before the installation of the new system may proceed. The PDSA must show how the nuclear safety design requirements of DOE O 420.1B will be satisfied. This would include a description of the system and its installation, a hazard analysis and (if warranted) identification of safety controls, and classification of safety controls as Safety Class or Safety Significant, if appropriate according to the criteria for those designations. Upon installation, the facility safety basis would need to be modified to account for the new system and its safety controls.

Some of the issues that would need to be addressed are the controls indigenous to the security system, controls that may be required because of facility-specific conditions, design of the installation regarding seismic and fire hazards to the system that could affect inadvertent actuation, etc.

The PDSA requires DOE approval prior to procurement and installation of systems and components. Creation of the PDSA requires significant interaction among the safety basis project team and security to ensure proper integration and coordination. More definitive guidance on the treatment of major modifications is being developed as part of DOE-STD-1189 "Integration of Safety into the Design Process," which is planned for RevCom in October 2006.

The determination of whether or not a major modification is appropriate to characterize the change is typically a challenge requiring the involvement of DOE. The USQ process is helpful in answering this question. If the USQ determination is positive, then discussions with DOE should commence and a consensus reached as to whether declaration of a major modifications and preparation of a PDSA are necessary. The comprehensive change control process is then followed to ensure integration and updates to both the safety and security bases. The completed PDSA would be submitted to and approved by DOE.

If a PDSA is not necessary to properly address the proposed change, a comprehensive change control process would still be followed including updates to both the safety and security bases. In this case, since a PDSA is not necessary, procurement and design activities could proceed after DOE approval, based on a safety analysis that demonstrates adequate safety for the installation.

There is also the possibility that a USQ determination of a proposed change could be negative, that is, there is no USQ. This could be the case when there is an existing security system, and the proposed change does not present new safety issues that were not previously considered for the initial installation. In this case, the change could be made on the contractor's authority. However, both the safety and security documentation needs to be updated to reflect the changes.

¹ Major modification will be clarified by DOE-STD-1189, *Integration of Safety into the Design Process*, scheduled for REVCOM in October 2006.

8.3 Hazard and Accident Analysis Process

DOE-STD-3009, *Preparation Guide for U.S. Department of Energy Nonreactor Nuclear Facility Documented Safety Analysis* provides appropriate guidance for hazard and accident analysis involved in assessing a security system deployment.

One of the first steps is to decide what type of safety evaluation is to be performed. The site practice for hazard analysis (“What-If”, HAZOP, etc.) should be used to assess this change. Obtaining concurrence from DOE on the selected approach is suggested. It is also important to determine the extent of facility involvement in the proposed change. For example, does the change apply to a single facility or multiple facilities up to and including the entire site or the complex? Prior to any meetings to discuss the impacts of the change, discussions should be held with security professionals and SMEs to accurately define the proposed change, identify any inherent safety features of the system, and identify key installation requirements.

Analysis sessions are held with the project team, including, as appropriate, nuclear criticality safety, facility safety, facility operations, fire protection, and security personnel familiar with the system. The project team would follow the selected hazard analysis approach to address the hazards and potential accident scenarios resulting from the new or upgraded security systems. There are typically several sessions with the project team to cover a comprehensive set of internal and external initiating events. Planned activities associated with the security system, both internal and external to impacted facilities, should also be considered. Inherent safety features associated with the new or upgraded security system are also considered to ensure that a comprehensive analysis/evaluation is performed. The session outcome is a formal document presenting the process, discussing the resulting hazards and accident scenarios including estimated frequencies and consequences to workers and the public. A set of recommended safety controls appropriate for preventing/mitigating event consequences is also provided and is the key result of the analysis. The specific controls provided with the security system could receive special designation in this document, if appropriate.

8.4 Derivation of Controls

With respect to the proposed change and within the context of the safety basis process, it may be necessary to designate specific controls (engineered or administrative) in the safety basis to prevent or mitigate the event of concern (e.g., accidental discharge). The controls could be specific safety SSCs consisting of passive and/or active features ensuring safe operation and preventing inadvertent actuations. Some of these controls will probably be inherent with the design and installation of the proposed security system. Acceptable controls may include safety management program elements ensuring safety during routine activities, as well as training exercises with the security system. The control set or sets would flow directly from the hazards and accident analysis process into the safety basis (i.e., the DSA and TSRs). If the controls are passive or active they would be included in the TSRs as Design Features, Limiting Conditions for Operation (LCOs), or Administrative Controls. If safety management programs suffice, then the programs would be summarized and the salient features emphasized in the TSRs.

8.5 Security Information Protection

It is very likely that some of the security system information necessary for the safety basis documents (DSA and TSRs) would be classified with access provided on a “need to know” basis. This could be accomplished by having a classified addendum to both the DSA and the TSR documents. The DSA addendum might have the elements of the system description that need protection. The TSR addendum might have the elements of the hazard control set that would be the responsibility of the security element to implement. The list of “need to know” personnel, however, include the Facility Manager and designees. It is ultimately the Facility Manager’s responsibility to ensure that operations are conducted according to the facility safety basis and also to be aware of any proposed changes to the safety basis, as reflected in the classified addendum.

9. Post-Installation Readiness

After installation of physical security systems, an appropriate level of review needs to be conducted to ensure that the security features will be available when needed and ready to function as designed. In addition, the review needs to ensure the safety features related to the security system are installed, ready to operate, and available when called on. The level of review can be graded based on the significance of the installation as long as the review covers these key features. Use of existing readiness review processes in place at the site is encouraged.

Essential elements associated with security systems require routine testing of the system to ensure operability. Security system testing requirements should be identified during the system selection process and documented in the Project Execution Plan. Additionally the testing requirements are documented in the SSSP and in a formal Performance Assurance Program Plan as required by DOE security directives.

In addition to reviewing physical security systems, when the safety controls related to security are administrative in nature, the review needs to ensure appropriate procedures, training, and other activities are in place and effective.

DOE-O-425.1 C, *Start and Restart of Nuclear Facilities* is applicable for new nuclear facilities and modifications following shut down of a HC-1 or HC-2 nuclear facility. The requirements of this order specify a readiness review process that must, in all cases, demonstrate that it is safe to start (or restart) the applicable facility. It is also required for new HC-3 nuclear facilities. The order should be reviewed for applicability when deploying security technologies and for modifications within a nuclear facility.

10. Configuration Control

Configuration (change) control for security systems should be managed by a rigorous process that includes determination of approval authority. Over the past decade a safety basis configuration control process has matured, covering structures, systems, and components and associated technical basis documents and administrative procedures. A configuration control process to manage security approvals and changes initiated to meet the DBT are also required.

Engineered systems for security projects/changes should be treated like any other project or change, including designation of a design authority representative and/or system engineer. SME reviews are applied when necessary using a graded approach and facility operational safety reviews (or equivalent) include representatives from security.

All facility changes (including security-related changes) affecting Hazard Category 1, 2, and 3 nuclear facilities must be subject to the USQ process. Changes to security plans or facility changes that affect security should be subject to an evaluation process to determine approval authority for the change. Configuration control for security changes should be owned by the line organization with DOE providing formal approvals in a form of documents similar to the SERs used for safety basis documents. The rigor of the change control process may be linked to the security designation for the facility (Threat Level 1 - 4). A listing could be posted on a master list (possibly web-based) to identify the latest approval and effective documents.

While configuration control applies in a graded manner to aspects of change to nuclear facilities, it is the implementation procedures that actually flow down the process by triggering change packages and multi-discipline safety and technical reviews (including security and safety representatives). Figure 10-1 depicts application of the USQ and Security Change Evaluation processes within the configuration control program. Authority to proceed with changes is contingent on execution of both the USQ and Security Change Evaluation processes. These processes include DOE approval if the change could place a facility or activity outside its safety basis or Security Plan.

11. Review Process for Improvements and Lessons Learned

The intent is to assess this process against the transfer of information for security system deployment between Y-12 and INL. This assessment will be used to benchmark the process presented in this report. Follow-on implementation will provide additional feedback to the process as well as populate the security system database/toolbox. The intent is that while the database is populated, the participants provide feedback that facilitates continuous improvement in the process. It is proposed that an annual integrated review be held with interested participants from both the security and safety disciplines to overview the current process and assure that it is providing the intended benefit to the sites. As this review depends on DOE's implementation of these recommendations, it is suggested that the scope of the reviews be defined along with the implementation program(s).

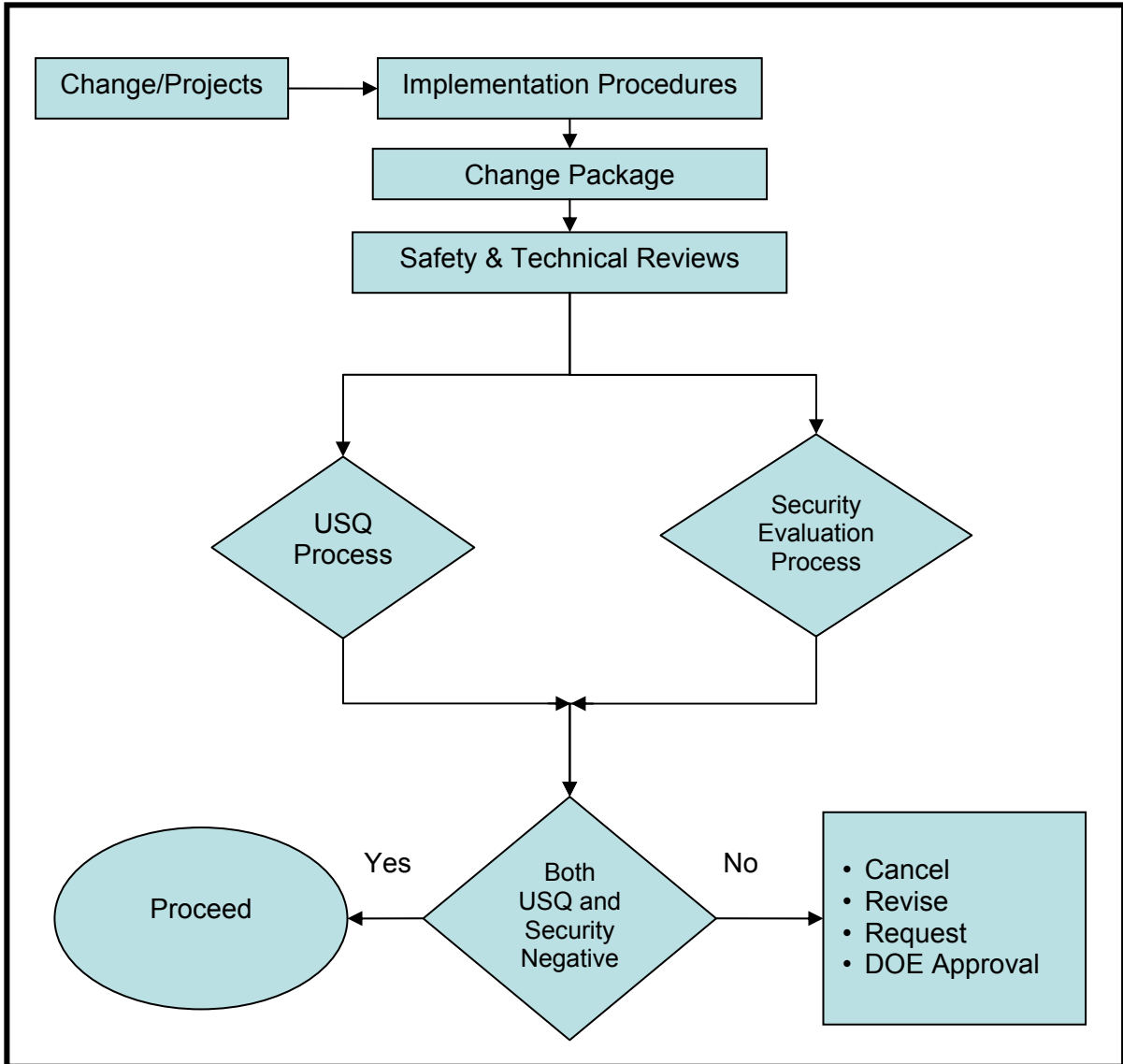


Figure 10-1 Security and Safety Change Process

12. Summary

A cost effective, comprehensive process has been developed to simultaneously satisfy DBT and safety basis objectives for security systems. This approach is intended to facilitate sites meeting the defined dates to satisfy the DBT. An integrated project team approach has been proposed that contains multiple interrelated elements/processes: training, alternate analysis, document integration, configuration control, etc. Figure 5-1 (Security System Deployment Process Diagram) lays out the overall process. A key element of this process leading to cost savings for individual facilities is the toolbox approach that makes systems and key information transportable between facilities and sites and accessible by multiple DOE sites for review and use. The toolbox will be populated with pertinent Security Information Data Set (SIDS) information that includes safety basis and security data for various security systems, including system evaluation and approval documentation. These data may be used as part of the information set required to obtain approval to deploy similar security systems at several sites.

For this process to be successful, safety and security professionals from around the complex and at DOE-HQ need to actively seek to understand the parameters under which their counterparts work and possess a contextual understanding of the terms of art used by their counterparts.

Appendix A Security/Safety Crosswalk

Safety	Security
Hazard identification, analysis, and classification:	
<p>Hazard Analysis and Facility Hazard Categorization: Facilities and facility segments are classified and/or categorized based on hazard inventories, criticality, and risk of accidental release to workers or the public to provide a basis for the determination of safety documentation requirements, level and sophistication of safety analysis, and structural design requirements.</p> <p>Hazard categorization is considered for both radiological and toxicological hazards. Nuclear hazard categorization is performed in accordance with DOE-STD-1027 and chemical hazard categorization is performed in accordance with 29CFR1910.119.</p> <p>Facility hazard operations can be generally grouped into three categories:</p> <ul style="list-style-type: none"> • Radiological Operations • Chemical Operations • Other Industrial Operations 	<p>Design Basis Threat guidance is issued by the Director of Security Affairs in conjunction with local threat guidance and vulnerability analysis for use by managing contractors in the design and implementation of physical protection program planning.</p> <p>Protection programs are tailored to address site and facility specific characteristics and requirements, current technology, ongoing programs, operational needs, and to achieve acceptable protection levels that reduce inherent risks on a cost-effective basis. Protection planning documents are developed per DOE requirements, in conjunction with facility managers, to address physical protection measures and support needed for the protection of security interests and response to a security incident.</p> <p>A protection strategy meeting DOE requirements is developed for all security interests so that security programs provide a high degree of assurance of the capability to deter, detect, assess, delay, prevent, and/or inhibit unauthorized access to nuclear weapons, nuclear test devices, or completed nuclear assemblies, Category II or greater quantities of SNM, and vital equipment.</p> <p>Target Characterization Sabotage of radiological, chemical or biological materials – acute dose delivered in the 24-hour period after the intake (reduce these values by a factor of 7 for alpha emitting radionuclides for bone marrow, gastrointestinal tract and lung): ≥ 200 radiation absorbed dose (rad) to the bone marrow; ≥ 500 rad to the gastrointestinal tract; ≥ 1000 rad to the lung; or, ≥ 3000 rad whole body dose delivered in a one-hour period.</p>

Safety	Security
<p>Nuclear Facility Hazard Categories These categories and associated analyses are derived from DOE-STD-1027, <i>Hazard Categorization and Accident Analysis Techniques for Compliance with DOE Order 5480.23 Nuclear Safety Analysis Reports</i> as defined by quantities of material or potential consequence to a receptor.</p> <p>HC-1, 2, 3 Nuclear Operations involving hazardous materials that present a potential significant risk to workers or the public. These are defined in DOE-STD-1027 as follows:</p> <p>HC-3 DEFINITION - Hazard Analysis shows the potential for only significant localized consequences.</p> <p>INTERPRETATION - Facilities with quantities of hazardous radioactive materials which meet or exceed values defined in the standard.</p> <p>HC-2 DEFINITION - Hazard Analysis shows the potential for significant on-site consequences.</p> <p>INTERPRETATION - Facilities with the potential for nuclear criticality events or with sufficient quantities of hazardous material and energy, which would require on-site emergency planning activities.</p> <p>HC-1 DEFINITION - Hazard Analysis shows the potential for significant off-site consequences.</p> <p>INTERPRETATION - Category A reactors and facilities designated by PSO.</p>	<p>Special Nuclear Material (SNM): Plutonium, uranium-233, uranium enriched in the isotope 233 or in the isotope 235, and any other material which the NRC, pursuant to the provisions of Section 51 of the Atomic Energy Act determines to be: 1) SNM, but does not include source material; or 2) any material artificially enriched by any of the foregoing, but does not include source material.</p> <p>SNM Categories (I, II, III, IV) See Appendix B</p> <p>attractiveness level — (A, B, C, D, E) categorization of SNM material types and compositions which reflect the difficulty of processing and handling required to convert material to a nuclear explosive device</p> <p>Threat Level 1 through 4</p> <p>Graded Protection Concept: A fundamental principle of the Department's security program is a graded approach to the protection of national security assets. This approach applies to and is embodied in the relevant threat considerations for Departmental national security assets. The Department intends that the highest level of protection be given to security interests where loss, theft, compromise, or unauthorized use would adversely affect the national security or the health and safety of employees, the public, and the environment. The graded protection approach categorizes all Departmental assets into one of four "Threat Levels" based on the general consequence of loss, destruction, or impact to public health and safety at a facility or the program, project, or activity conducted. Threat Levels 1-3 facilities and assets must meet performance-based standards; Threat Level 4 facilities and assets must meet compliance based standards.</p> <p>Threat Level 1: Theft or Sabotage (including unauthorized nuclear detonation) of Nuclear Weapons, Nuclear Test Devices, Nuclear Weapon Components, and Category I Quantities of SNM</p> <p>Threat Level 2: Sabotage of Radiological, Biological, or Chemical Materials</p> <p>Threat Level 3: Theft, Sabotage (including disruption of mission) or Espionage at Critical Facilities or Activities</p> <p>Threat Level 4: Theft, Sabotage or Espionage at Non-Critical Facilities or Activities</p>

Safety	Security
<p>Radiological Operations involving radioactive materials that do not present a significant hazard, but do involve quantities above a minimum level of concern. Radiological facilities are also called Below HC-3 Nuclear Facilities by the Rule. Radiological Facilities are those facilities that do not meet or exceed the hazard category 3 threshold quantity values published in DOE-STD-1027-92 but still contain some quantity of radioactive material (above those discussed in Appendix B to 40 CFR 302).</p> <p>Radiological operations require safety documents to be developed (some sites still use DOE-EM-STD-5502-94 to guide management of these facilities).</p> <p>Radiological facilities shall develop an auditable (defendable) safety analysis (similar to a SAR but with much reduced content and requirements). An auditable safety analysis (ASA):</p> <ul style="list-style-type: none"> A. Provides systematic identification of hazards within a given DOE operation; and B. Describes and analyzes the adequacy of measures taken to eliminate, control, or mitigate identified hazards. <p>Radiological facilities with hazardous waste activities require the development and maintenance of a HASP.</p>	<p>Radiological Sabotage Targets: Radiological sabotage targets are those that would result in unacceptable consequences for the safety of the public, employees, or the environment from a deliberate dispersal of radiological material.</p>
<p>Chemical Operations involving chemical hazards in forms or quantities beyond common industrial settings. Chemical hazards are subdivided further into High Hazard Chemical and Low Hazard Chemical for flexibility in implementing requirements.</p> <p>Chemical hazards within a nuclear facility are required to be addressed within the DSA. If the hazard is significant to workers or the public, the required controls would be identified as safety significant. Some sites require safety basis documentation for chemically hazardous facilities regardless of the radiological inventory. These non-nuclear facilities often have a configuration control program that provides the same level of rigor as the USQ provides for nuclear facilities.</p>	<p>Chemical Sabotage Targets: Chemical sabotage targets are those that would result in unacceptable consequences for the safety of the public, employees, or the environment from a deliberate dispersal of chemicals. Security confirms that security protection is comparable to that provided by the commercial sector for similar material.</p>

Safety	Security
<p>The facility Emergency Preparedness Hazard Assessment (EPHA) provides a screening process to identify those quantities of chemicals that are significant from an emergency response standpoint. Concentrations at the site boundary are compared to the Emergency Response Planning Guide (ERPG-2) concentrations to determine if the results are acceptable.</p>	<p>Chemical Sabotage Targets (continued)</p>
<p>Definitions:</p> <p>acute exposure guideline level (AEGL) - EPA threshold exposure limits intended to describe the risk to humans resulting from once-in-a-lifetime (or rare) exposure to airborne chemicals. Acute exposures are single, non-repetitive exposures for not more than 8 hours. Exposure levels are applicable to the general population (including children and susceptible individuals).</p> <p>emergency response planning guideline (ERPG) - An estimate of the concentration ranges above which one could reasonably anticipate observing adverse effects. ERPG values are the preferred guidelines when dealing with chemical exposures.</p> <ul style="list-style-type: none"> • ERPG-2 - the maximum airborne concentration below which it is believed that nearly all individuals could be exposed for up to one hour without experiencing or developing irreversible or other serious health effects or symptoms that could impair their abilities to take protective action • ERPG-3 - the maximum airborne concentration below which it is believed that nearly all individuals could be exposed for up to one hour without experiencing or developing life-threatening health effects 	

Safety	Security
<p>temporary emergency exposure limit (TEEL) that have no AEGL or ERPG. Definitions for TEELs are based on those for AEGLs/ERPGs. For application of TEELs, the concentration at the receptor should be calculated as the peak 15-minute time-weighted average. TEELs may be downloaded from the DOE Chemical Safety web site (www.eh.doe.gov/chem_safety/teel.html).</p> <ul style="list-style-type: none"> • TEEL -2 - the maximum concentration in air below which it is believed nearly all individuals could be exposed without experiencing or developing irreversible or other serious health effects or symptoms that could impair their abilities to take protective action • TEEL -3 - the maximum concentration in air below which it is believed nearly all individuals could be exposed without experiencing or developing life-threatening health effects 	<p>Chemical Sabotage Targets (continued)</p>
<p>Other Industrial Operations involving hazardous materials routinely encountered in public or common industrial settings.</p> <p>hazardous material - any solid, liquid, or gaseous material that is toxic, flammable, radioactive, corrosive, chemically reactive, or unstable upon prolonged storage, in quantities that could pose a threat to life, property, or the environment</p>	<p>Biological Sabotage Targets: Biological sabotage targets are those that would result in unacceptable consequences for the safety of the public, employees, or the environment from a deliberate dispersal of biological material. (1) Biological Sabotage Target Characterization: Biological sabotage targets are defined in Department of Health and Human Services (HHS), Office of Health and Safety publication “Biosafety in Microbiological and Biomedical Laboratories,” 4th Edition.</p> <p>Biological Sabotage Target Characterization Considerations: The VA Confirm that security protection is in accordance with the requirements as designated in 7 CFR 331, 9 CFR 121, and 42 CFR 73 and classified by the Center for Disease Control (CDC) as requiring Biosafety Level 4 or greater facilities per biosafety procedures specified in HHS publication “Biosafety in Microbiological and Biomedical Laboratories,” 4th Edition, April 1999.</p>

Safety	Security
<p>Operational Control For Off Normal Conditions:</p> <p>Emergency Duty Officer (EDO)</p> <p>Until the site level emergency response facilities are activated, the EDO is responsible for categorizing operational emergencies and further classifying emergencies for the general site (that portion of the site that is not within a facility or operational area boundary), in coordination with the Incident Commander. For an Onsite Transfer of hazardous materials, the EDO is also responsible for categorizing and classifying transportation accidents that occur within the facility boundary, in coordination with the AEC/FEC and in accordance with this procedure and facility classification procedures. If the event is safeguards and security related and involves the general site, the EDO determines the emergency categorization/classification level based on the event and security phase declaration made by the senior Law Enforcement Division Supervisor on duty.</p>	<p>NOTE: SECON is another threat condition not necessarily associated with an onsite emergency or event. It is included here because there are some additional actions driven by SECON conditions.</p> <p>Homeland Security Threat Conditions (known in DOE as Security Conditions [SECONs]) are established based on the analysis of a continuous and timely flow of integrated all-source threat assessments and reporting provided to Executive Branch decision-makers.</p> <p>SECON 1, SEVERE CONDITION (RED) SECON 2, HIGH CONDITION (ORANGE). SECON 3, ELEVATED CONDITION (YELLOW). SECON 4, GUARDED CONDITION (BLUE). SECON 5, LOW CONDITION (GREEN).</p>
<p>Emergency Classification - Classifies an Operational Emergency involving a hazardous material release by the degree of severity, depending on the actual or potential consequence of the emergency. Classification levels are Alert, Site Area Emergency (SAE), and General Emergency (GE)</p> <ul style="list-style-type: none"> • ALERT Emergency classification level triggered by an event that is predicted, in progress or has occurred that results in <ul style="list-style-type: none"> - Actual or potential substantial reduction in the level of control over hazardous materials (radiological and non-radiological) where the radiation dose from any release to the environment of radioactive material or a concentration in air of other hazardous material is expected to exceed the applicable protective action criteria (PAC) at or beyond 30 meters from the point of release. The PAC is not expected to be exceeded at or beyond the facility boundary. - Actual or potential substantial degradation in the level of safety or security of a nuclear weapon, component, or test device that would not pose an immediate threat to workers or the public. - Actual or potential substantial degradation in the level of safety or security of a facility or process that could, with further degradation, produce a Site Area Emergency or General Emergency. 	<p>Safeguards and Security Phase Declarations: System used by the protective force security contractor, to categorize security related events. The level of the security event is then used as an EAL to declare the corresponding emergency classification at a particular facility.</p> <ul style="list-style-type: none"> • SECURITY ALERT - Event requiring management attention and increased security vigilance (no EAL). • PHASE I - A potential threat has been identified that warrants increased management awareness and requires heightened capability to implement security response actions (no EAL). • PHASE II - A known threat has been identified that requires heightened capability to implement security response actions (EAL). • PHASE III - A major verified security incident is in progress or has occurred that requires the immediate implementation of security response actions (EAL). • PHASE IV - A major verified security incident is in progress or has occurred that requires special operations procedures (EAL).

Safety	Security
<p>Emergency Classification (Continued)</p> <ul style="list-style-type: none"> • SITE AREA EMERGENCY (SAE) Emergency classification level triggered by an event that is predicted, in progress, or has occurred that results in one or more of the following situations. <ul style="list-style-type: none"> - Actual or potential major failure of functions necessary for the protection of workers or the public. The radiation dose from any release of radioactive material or concentration in air from any release of other hazardous material is expected to exceed the applicable PAC beyond the facility boundary. The PAC is not expected to be exceeded at or beyond the site boundary. - Actual or potential threat to the integrity of a nuclear weapon, component, or test device that may adversely impact the health and safety of workers in the immediate area, but not the public. - Actual or potential major degradation in the level of safety or security of a facility or process that could, with further degradation, produce a General Emergency. 	<p>Safeguards and Security Phase Declarations (continued)</p> <p>NOTE: Security system alarms report separately to the following alarm stations (not facility control rooms). Specific actions are to be taken immediately by protective force personnel in response to security alarms received by the Central Alarm Station (CAS) or Secondary Alarm Station (SAS).</p> <p>Central Alarm Station - A Central Alarm Station (CAS) is used in protection of Category I and Category II quantities of SNM.</p> <p>Secondary Alarm Stations - Facilities with Category I or II quantities of SNM must have a SAS. Used as an alternative alarm annunciation point to the CAS, the SAS must be maintained at a location continuously manned, such that a response can be initiated in the event a CAS is unable to perform its intended function</p>
<p>Emergency Classification (Continued)</p> <ul style="list-style-type: none"> • GENERAL EMERGENCY(GE) Emergency classification level triggered by an event that is predicted, in progress, or has occurred that results in one or more of the following situations. <ul style="list-style-type: none"> - Actual or imminent catastrophic reduction of facility safety or security systems with potential for the release of large quantities of hazardous materials (radiological or non-radiological) to the environment. The radiation dose from any release of radioactive material or a concentration in air from any release of other hazardous material is expected to exceed the applicable Protective Action Guide or Emergency Response Planning Guideline at or beyond the site boundary. - Actual or likely catastrophic failures in safety or security systems threatening the integrity of a nuclear weapon, component or test device that may adversely impact the health and safety of workers and the public. 	

Safety	Security
<p>Safety Documents</p> <p>Facility Category and Facility Classification results are documented in Safety Basis (SB) documents such as a Documented Safety Analysis (DSA) or other appropriate safety documents. 10CFR830 Subpart B Table 2 provides a listing of the safe harbors within the rule for developing the safety basis for a facility.</p> <p>Documented Safety Analysis (DSA) - a documented analysis of the extent to which a nuclear facility can be operated safely with respect to workers, the public, and the environment, including a description of the conditions, safety boundaries, and hazard controls that provide the basis for ensuring safety. DSAs are prepared using one of the safe harbor methodologies in 10 CFR 830, Subpart B or an approved alternative.</p> <p>Emergency Plan - a clear and concise description of the overall emergency organization, designation of responsibilities, and procedures involved in coping with any or all aspects of an operational emergency</p> <p>Safety Basis – the documented safety analysis and hazard controls that provide reasonable assurance that a DOE nuclear facility can be operated safely in a manner that adequately protects workers, the public, and the environment. The Safety Basis (SB) is described in documents such as the facility Documented Safety Analysis (DSA) Auditable Safety Analysis (ASA), and Administrative Limits (ALs). Safety Basis documents are approved by DOE.</p> <p>Technical Safety Requirements (TSRs) - Provisions relating to organization and management, procedures, record keeping, assessment, and reporting necessary to ensure safe operation of a facility. With respect to nuclear facilities <i>administrative controls</i> means the section of the Technical Safety Requirements (TSRs) containing provisions for safe operation of a facility including (1) requirements for reporting violations of TSRs, (2) staffing requirements important to safe operations, and (3) commitments to the safety management programs and procedures identified in the Documented Safety Analysis as necessary elements of the facility safety basis provisions.</p>	<p>Safeguards and Security Planning Documents</p> <p>Facility Data and Approval Record (FDAR) A determination must be made by DOE that a facility is eligible to receive, process, use, or store classified material, nuclear materials, or DOE property of significant monetary value. Facility approval is based on the determination that satisfactory S&S measures are in place.</p> <p>Site Safeguards and Security Plan</p> <p><i>Part I, the Safeguards and Security Management Report (SSMR)</i> is the principal written record of the protection program. It provides information for managers to evaluate protection program elements and resources for compliance and improvement, allows for cost benefit analysis and comparison, and provides an information baseline to show integration of complex-wide S&S interests.</p> <p><i>Part II, the Vulnerability Analysis Report (VAR)</i>, provides the results of vulnerability analysis and risk assessments. A vulnerability assessment is conducted to support requirements for protection against theft or diversion of SNM, industrial sabotage, and radiological/chemical/biological sabotage. The VAR documents the analysis results and provides the technical basis for the preparation of the SSMR for a facility.</p> <p>Facility Security Plan (FSP) A facility specific document that describes the protection measures for facility security interests. FSPs are required for applicable facilities, which due to the limited scope of security interests do not require a SSMR.</p>

Safety	Security
<p>Safety Basis Documents (continued) Temporary/Transitory Facility Hazards , are handled either by modifying the DSA, developing a Justification for Continued Operation (JCO), or developing a temporary supplement to the DSA. These could include a discovery condition where the equipment is potentially not covered by the safety basis, short-duration storage of hazardous materials or weapons devices, or special process testing within the facility.</p> <p>A JCO may be used to provide an interim Safety Basis for operation either for a discovery situation where a Potential Inadequacy in the Safety Analysis (PISA) is declared. For discovery situations, JCOs can provide an interim Safety Basis for continued operation when a PISA is declared.</p> <p>For proposed activities, a temporary supplement to the safety basis may be prepared for one-time short term (months rather than years) operations such as short campaigns, special tests, extended outages, etc.. The supplement is expected to cover the six basic topics of a “Safe Harbor” DSA (applicable to the scope of the activity) and satisfy general Rule requirements for a DSA. The combination of the DSA and supplement must be complete as they relate to Rule requirements.</p> <p>Both the JCO and temporary supplement to the safety basis specify closure requirements so that when the short-term operation is completed, or the USQE is finished and approved, these documents can be retired, the Safety Basis returned to normal, and operational constraints removed without the need for further approvals. These documents are part of the Safety Basis and USQ review of proposed activities and/or discoveries must consider any active JCOs or supplements to the safety basis in determining whether a USQ exists.</p>	<p>Safeguards and Security Planning Documents (contd) Modified Security Plan (MSP) A MSP is required for any activity that deviates or modifies the security measures outlined in existing facility SSMR, VAR, FSP, or deviation documents. A MSP is not required if the activity is prescribed by procedure (e.g., normal maintenance) or is an emergency (e.g., unforeseen and requires immediate action to correct). All Level II and III MSPs require the approval of S&S.</p> <p>Deviations (e.g., variances, waivers, and exceptions) from DOE security orders are prepared and submitted in accordance with applicable site procedures.</p>
<p>Temporary storage or use of hazardous materials or weapons devices, or special process testing within the facility, will be covered by specific updates (as an addendum) to the EPHA and associated EPIP. To avoid duplication of effort, test plans or other controlling safety basis documents for such hazards may be configured to serve as temporary addenda to the site or facility EPHA and emergency plans as applicable.</p>	

Safety	Security
Miscellaneous Other Items to Consider as Differences	
<p>Training The central training authority for safety resides at the site.</p>	<p>Training The central training authority for security is centrally maintained at the National Training Center in Albuquerque, NM.</p>
<p>Scope The scope of safety analysis and documentation is limited to operational concerns and does not include malevolent acts. Specific evaluation of malevolent acts is thus not part of safety documentation.</p>	<p>Scope Malevolent acts are the focus of security evaluations. However, this does not exclude consideration of personnel safety. To the extent practicable the public and operations personnel should be protected from harm. Care should be taken in selecting security systems that are appropriate for the risk (i.e., the most robust security system is not required for all situations).</p>
<p>Configuration Controls The Unreviewed Safety Question (USQ) process is required to be used to protect the nuclear safety basis for the facility. This program is a key element of the configuration control program. The USQ process is defined as: The mechanism for keeping a safety basis current by reviewing potential unreviewed safety questions, reporting unreviewed safety questions to DOE, and obtaining approval from DOE prior to taking any action that involves an unreviewed safety question. Note that this process includes all changes in the facility process changes or security changes.</p>	<p>Configuration Controls A mechanism needs to be defined that allows security questions to be raised to the security signature authority for approval.</p>

Appendix B Graded Safeguards (reference DOE M 470.4-6, Nuclear Material Control and Accountability)

	Attractiveness Level	Pu/U-233 Category (kg)				Contained U-235/Separated Np-237/Separated Am-241 and -243 Category (kg)				All E Materials Category IV
		I	II	III	IV ¹	I	II	III	IV ¹	
WEAPONS Assembled weapons and test devices	A	All	N/A	N/A	N/A	All	N/A	N/A	N/A	N/A
PURE PRODUCTS Pits, major components, button ingots, recastable metal, directly convertible materials	B	≥2	≥0.4<2	≥0.2<0.4	<0.2	≥5	≥1<5	≥0.4<1	<0.4	N/A
HIGH-GRADE MATERIALS Carbides, oxides, nitrates, solutions (≥25 g/L) etc.; fuel elements and assemblies; alloys and mixtures; UF ₄ or UF ₆ (≥ 50% enriched)	C	≥6	≥2<6	≥0.4<2	<0.4	≥20	≥6<20	≥2<6	<2	N/A
LOW-GRADE MATERIALS Solutions (1 to 25 g/L), process residues requiring extensive reprocessing; moderately irradiated material; Pu-238 (except waste); UF ₄ or UF ₆ (≥ 20% < 50% enriched)	D	N/A	≥16	≥3<16	<3	N/A	≥50	≥8<50	<8	N/A
ALL OTHER MATERIALS Highly irradiated forms, solutions (<1 g/L), uranium containing <20% U-235 or <10% U-233 ² (any form, any quantity)	E	N/A	N/A	N/A	Reportable Quantities	N/A	N/A	N/A	Reportable Quantities	Reportable Quantities

¹The lower limit for Category IV is equal to reportable quantities in this Manual.

²The total quantity of U-233 = [Contained U-233 + Contained U-235]. The category is determined by using the Pu/U-233 side of this table.

Appendix C Evaluation Criteria – Examples

No.	Objective	MUST	WANT
1	Effective to enable recapture of defined locations in specified time limit	√	
2	Capable of creating a person-sized breach (i.e., at least 4 ft diameter hole) and multiple assault entry points	√	
3	System(s) remotely activated without jeopardizing Protective Force	√	
4	Positive safety: firing requires 3 separate actions	√	
5	Positive safety: verification of defined locations status by operations under normal conditions (engineered systems)	√	
6	Single insider cannot defeat system(s)	√	
7	No single point failure for engineered systems	√	
8	Reliability high (engineered system(s) must be testable)	√	
9	System(s) deployment will not cause a significant accident initiation	√	
10	Proven technology	√	
11	System(s) will not hinder Protective Force recapture operations	√	
12	Cost less than \$3M for each system(s) or method to be used	√	
13	Accidental firing not credible (e.g., power surges, lightning, etc.)	√	
14	Active engineered system(s) must have 2-person activation	√	

Appendix C Evaluation Criteria – Examples (continued)

No.	Objective	MUST	WANT
A	System(s) is difficult to defeat or counter (intentionally or unintentionally)		√
B	Greater expectation of Protective Force Survivability		√
C	Installation, training, and maintenance is simple		√
D	Initial installation of system(s) causes minimal impacts to ongoing operations		√
E	Deployment impacts to SNM storage minimal (criticality)		√
F	Collateral damage to structure, personnel, public, environment, and mission minimal		√
G	Fire and other hazards are minimal		√
H	System(s) firing and deployment time simple and minimized		√
I	Will breach most defined locations		√
J	Impacts from engineering design configuration is minimal to current authorization basis		√