INSPECTORS GUIDE

Protection Program Management

SSA

Office of Security and Safety Performance Assurance

Office of Security Evaluations
Office of Independent Oversight

March 2006

PROTECTION PROGRAM MANAGEMENT

INSPECTORS GUIDE

March 2006

U.S. Department of Energy
Office of Safeguards and
Security Evaluations
19901 Germantown Road
Germantown, Maryland 20874

Preface

As part of an effort to enhance the appraisal process, the Office of Independent Oversight (SP-40) and the Office of Security Evaluations (SP-41) have prepared a series of documents that collectively provide comprehensive guidance and tools for the evaluation of safeguards and security program effectiveness across the U.S. Department of Energy (DOE) complex. The SP-40 Appraisal Process Protocol describes the philosophy, scope, and general procedures applicable to all independent oversight appraisal activities. The SP-41 Safeguards and Security Appraisal Process Guide describes specific procedures used by SP-41 in planning, conducting, and following up safeguards and security inspections. This Protection Program Management Inspectors Guide, as one in a series of topical inspectors' guides, provides detailed information and tools to assist inspectors assigned to evaluate protection program management in DOE.

Although this inspection guide is designed specifically for the SP-41 inspector, it is made available to the field through the DOE homepage and may be useful to field element and facility contractor personnel who conduct surveys or self-assessments of the protection program management topic.

SP-41 anticipates making periodic revisions to this guide in response to changes in DOE program direction and guidance, insights gained from independent oversight activities, and feedback from customers and constituents. Therefore, users of this process guide are invited to submit comments and recommendations to SP-41.

This page intentionally left blank.

Contents

Contents (Continued)

Acronyms

ACL	Adversary Capabilities List
B&R	Budget and Reporting
BA	Budget Authority
BO	Budget Outlay
CAP	Corrective Action Plan
CD	Critical Decision
CFO	Chief Financial Officer
CMPC	Classified Matter Protection and Control
CPE	Critical Protection Element
COTR	Contracting Officer's Technical Representative
CSO	Cognizant Secretarial Officer
DBT	Design Basis Threat
DOE	U.S. Department of Energy
FV&A	Foreign Visits and Assignments
GPP	General Plant Projects
HRP	Human Reliability Program
ISSM	Integrated Safeguards and Security Management
JCATS	Joint Conflict and Tactical Simulation
JTS	Joint Tactical Simulation
M&O	Management and Operations
MC&A	Material Control and Accountability
QRB	Quality Review Board
SNM	Special Nuclear Material
SP-60	Office of Security Policy
S&S	Safeguards and Security
SSD	Safeguards and Security Director
SSIMS	Safeguards and Security Information Management System
SSSP	Site Safeguards and Security Plan
TSCM	Technical Surveillance Countermeasures
VA	Vulnerability Assessment
WMD	Weapons of Mass Destruction

This page intentionally left blank.

Section 1

INTRODUCTION

Contents

Purpose

The Protection Program Management Inspectors Guide provides the inspector with a set of detailed tools and references that can be used to plan, conduct, and close out an inspection of the overall management of the protection program. These tools serve to promote consistency, assure thoroughness, and enhance the quality of the inspection process.

The information in the guide is intended for inspectors who are familiar with conducting inspections of the protection program management (PPM) topic at U.S. Department of Energy (DOE) facilities as well as for experienced inspectors who might be less familiar with the PPM topic or with DOE practices. For the experienced PPM inspector, the information is organized for easy reference and can serve as a reminder when conducting inspection activities. For inspectors who are less familiar with DOE or the PPM topic, the information can serve as a valuable tool for gaining familiarity with the PPM topic in the DOE environment. With the assistance of an experienced PPM inspector, the tools and reference material in this guide should support effective and efficient data collection.

Organization

This introductory section describes the inspection tools and outlines their use. Sections 2 through 6 provide detailed guidance for inspecting each major PPM subtopic:

- Section 2 - Planning Process
- Section 3 - Organization and Staffing
- Section 4 - Budget Process
- Section 5 - Program Direction
- Section 6 - Control Systems.

  The subtopic sections are further divided into several sub-elements to assist the reader in understanding subtopic organization.

- Section 7 - Integration: contains guidelines concerning the interaction between PPM subtopics and other topic areas.
- Section 8 - Analyzing Data and Interpreting Results: contains guidelines on how to organize and analyze information collected during data collection activities. These guidelines include likely impacts of particular information on other topics or subtopics, the impact of other topic results on PPM, and a discussion on interpreting the significance of potential deficiencies.

The Inspection Tool Kit in Appendix A provides a series of data collection and analysis tools and worksheets to aid inspectors.

General Considerations

Use of This Guide

The tools contained in this guide are intended to be used at the discretion of the inspector. Typically, inspectors select the tools that are applicable and most suitable on a facility-specific and inspection-specific basis. Although the guidelines presented here cover a variety of inspection activities, they do not and cannot address all protection program variations, systems, and procedures used at all DOE facilities. The tools might have to be modified or adapted to meet inspection-specific needs, and, in some instances, the inspectors might have to design new activities and new tools to collect information not specifically covered in this guide.

Baseline Orders

The primary Departmental order that provides detailed policy, standards, and guidance concerning the management of the protection program is DOE Order 470.1, *Safeguards and Security Program.* The information in this guide does not repeat all applicable DOE orders or manuals. Rather, it is intended to complement these documents by providing practical guidance for planning, collecting, and analyzing inspection data.

Conditions of Use

One significant consideration in developing inspectors guides is to provide a repository for the collective knowledge of the most experienced Office of Independent Oversight (SP-40) inspectors. Such knowledge can be enhanced and updated as inspection methods improve and SP-40 inspection experience accumulates. This is particularly true for the evolving PPM topic. Every attempt has been made here to develop specific guidelines that are useful to both new and experienced inspectors. In addition to functioning as guidelines for collecting information, the inspection tools provide guidelines for prioritizing and selecting activities, and analyzing and interpreting results.

Characterization of the Protection Program Management Topic

The purpose of the protection program is to ensure that DOE security interests are provided the appropriate degree of protection from theft, sabotage, and other hostile acts that might cause adverse impacts on national security or the health and safety of DOE and contractor employees, the public, or the environment. How the protection program and program elements are managed to achieve this purpose is the essence of PPM. PPM is a process in which activities relating to

planning, organization and staffing, budget, direction, and control are conducted continuously. Generally speaking, the PPM topic examines management as a circular control process in which managers affect the outcome of the work process by setting standards and expectations, allocating resources to accomplish the work, examining the outcome of the process, and modifying guidance and/or resources as is prudent. PPM inspections examine the effectiveness of this process.

One or more of the five subtopics (i.e., Planning Process, Organization and Staffing, Budget Process, Program Direction, and Control Systems) will be the subject of inspection activities, depending upon the focus and goals of the inspection. Because of the relationship among subtopics, at least some elements of each are typically inspected. Data collected for one subtopic often includes data relevant to other subtopics. When examining the Planning subtopic, planning activities are reviewed to discern management's ability to integrate Department security requirements into the site mission. For example, in response to modifications to the Design Basis Threat (DBT), data collection under the Budget subtopic will reflect site efforts to address the resources necessary to meet implementation deadlines. Likewise, the same DBT requirements will be mirrored in organization and staffing. Similarly, if new equipment and procedures are introduced, the inspection process will find modifications in control systems as self-inspections and survey programs are adapted to those elements considered essential to the security system. In another example, inspection of the Program Direction subtopic might indicate incentives and awards for timely execution of system modifications. This final example illustrates how each subtopic can stand on its own merit, even though an examination of only one subtopic would be insufficient to adequately describe the overall effectiveness of PPM at a facility.

Inspection Goals

The primary inspection goal is to determine with reasonable certainty whether the protection program is adequately managed, meets standards established by DOE policy, and efficiently provides appropriate protection to DOE security interests. In other words, the inspection must determine to what degree management is able to accomplish its mission. To do this, it is necessary to determine whether the five management subsystems (subtopics) are functional and integrated into an effective management system for the development and implementation of an effective protection program. While emerging Departmental site-specific concerns may be identified and included as unique elements of inspections, the primary goal always remains the same: to determine whether the inspected management system is effective.

Compliance vs. Performance

While a PPM inspection includes compliance and performance activities, significantly greater emphasis is placed on the performance aspect, since performance is conclusive in determining the adequacy of a management system. Even when dealing with policy requirements for which a compliance approach might seem appropriate, the SP-40 approach should go beyond strict compliance and determine the performance aspects of these requirements. When possible and appropriate, data collection activities for the PPM topic should be performance-oriented.

Inspection Planning Goals

The ultimate goal of planning is to anticipate and provide for actions necessary to conduct the highest quality inspection possible with the resources available. This broad goal is broken down into several narrower goals, namely to:

- Understand the character of and gain an appreciation for the inspected, superior, and subordinate protection program organizations; their mission, size, and management relationships; and the environment in which the total management system operates

- Determine the specific areas of focus for inspection activities

- Identify Headquarters elements where data gathering is required prior to the conduct phase of the inspection (including interviews, when appropriate)

- Produce the topic inspection plan and other necessary documents

- Determine specific follow-up requirements to be accomplished prior to the conduct phase of the inspection, and by which member of the inspection team.

Planning Decisions

Based on analysis of the information gained from the document review, discussion with other topic teams, and discussion with the points of contact, the topic team must make a number of decisions, including:

- Scope and emphasis of inspection activities

- Data required

- Data collection methods and tools to employ

- Headquarters program or other offices to be contacted for possible interview prior to the onsite data gathering

- Unique document review requirements

- Logistics, administrative, and personnel support required, and their sources

- Tentative assignment of each team member's data collection responsibilities

- Tentative schedule for data collection activities.

Once these decisions have been made, the detailed planning of data collection activities can proceed.

Using the Topic-Specific Tools

Sections 2 through 6, organized around the PPM subtopics, provide topic-specific information intended to help inspectors collect and analyze inspection data. Each subtopic section is further divided into the following standard format:

- References
- General Information
- Common Deficiencies/Potential Concerns
- Planning Activities
- Data Collection Activities.

References

The References section identifies appropriate DOE orders, policy memoranda, and other relevant documentation. The references provide the bases for evaluating the inspected program and for assigning findings. Refer to the applicable order/manual during interviews and tours of facilities to ensure that all relevant information is collected.

General Information

The General Information section defines the scope of the subtopic. It includes background information, guidelines, and commonly used terms intended to help inspectors focus on the unique features and problems associated with the subtopic. It also identifies the different approaches that a facility might use to accomplish an objective and provides typical examples.

Common Deficiencies/ Potential Concerns

This section addresses potential deficiencies or concerns that have been noted on previous inspections. Accompanying each common deficiency or potential concern is a short discussion providing more detail. Information in this section is intended to help the inspector further focus inspection activities and identify site-specific symptoms that might indicate whether a particular deficiency is likely to be present. By reviewing the list of common deficiencies and potential concerns prior to gathering data, inspectors can be alert for these deficiencies and concerns during interviews, tours, and other data-gathering activities.

Planning Activities

This section identifies activities normally conducted during inspection planning. These planning activities include reviews of general documents and interviews with the site and facility safeguards and security management and protective force managers. The detailed information in the planning activities section is intended to help ensure systematic data collection and to ensure that critical elements are not overlooked.

Data Collection Activities

This section identifies activities and outlines a methodology that inspectors may choose to follow during data collection. The information is intended to be reasonably comprehensive, although it is recognized that it will not address every conceivable variation. Typically, these activities are organized by functional element or by the type of information being gathered, and include steps that may be followed to gain the desired data for further analysis. The activities listed in this section are those most often conducted and reflect considerable SP-40 data collection experience and expertise. Each activity is identified by an alphabetical letter for easy reference.

Validation

Validation is the procedure inspectors use to verify the accuracy of the information they have obtained during data collection activities. Validation is one of the most important activities of the onsite inspection. Since validation requires acknowledgement from the organization being inspected, it compels both the inspectors and the inspected to review, discuss, and verify collected information on a daily basis. Validation authenticates inspection results from the very first day of data collection and greatly contributes to the quality of the inspection report.

The validation process ensures that site representatives understand what was observed and understand any potential problems and impacts as defined by SP-40. Validation is also designed to ensure that all information collected by the inspectors is factually precise. It is confined to facts, not conclusions. Further, it affords the inspected organization the opportunity to acknowledge the accuracy of the information collected, provide additional detail, request that further data be collected, or provide mitigation. Although actual (or even potential) ratings are not discussed, the validation process ensures that information included in the report supports ratings with precise facts that are not a surprise to site representatives.

There are on-the-spot validations, daily validations, and a summary validation. *On-the-spot validations* verify information at the time it is collected and are particularly important for summarizing such situations as interviews with higher-level management and staff, since it is frequently difficult to go back for validation later in the inspection process. *Daily validations* are normally conducted at the end of the day during the onsite phase of the inspection. Even if the points of contact accompany the inspectors on every inspection activity and validate observations on the spot, a daily validation meeting with more-senior site representatives

(when available) is still recommended. A *summary validation* is usually conducted at the end of the data collection phase of the inspection. Ideally, the summary validation is conducted at the working level and is attended by both members of the inspection topic team as well as site program representatives. During the summary validation, significant information, including items validated previously, is revalidated. Whether done formally or not, it is important here, too, that no information should come as a surprise to the inspected facility. The summary validation is the final validation activity before data analysis and the preparation of the SP-40 inspection report.

Experience in the PPM topic has proven that the primary methods of data collection, namely interviews and document reviews, make it difficult to complete on-the-spot validations for data collected. Interviews are typically sequential and seek similar information from various managers at multiple levels of management. Typically, during the first few days of data collection, there is not enough information collected to allow substantial on-the-spot or daily validations of an issue or a deficiency. During this period, validation normally consists of confirming the accuracy of collected data. In addition, the daily validation during the first few days typically consists as much of asking questions for clarification as attempting to validate an issue or confirm a developing deficiency. For the PPM topic, actual validation of facts to support an issue or a deficiency normally takes place later in the data collection process during daily validation sessions and, subsequently, during the summary validation.

Experience has also shown that if PPM inspectors attempt to validate information during the first few interviews on issues they are attempting to develop, it may be difficult to obtain information on these same issues in subsequent interviews. It is usually advantageous to wait until issues are more fully developed before beginning the process of validating issues or deficiencies that are developed during the course of the data collection. Also, the PPM team typically needs data from other topic teams for conducting meaningful validations, and this data is not usually available during the first part of the inspection. The PPM team should consider all of these factors during data collection and validation activities.

Using the Tools in Each Inspection Phase

The inspection tools are intended for use in all phases of the inspection, including planning, conduct of the inspection, and closure.

In the **planning phase**, inspectors:

- Use the General Information section under each subtopic to characterize the program and focus the inspection.

- Perform the activities identified under Planning Activities to gather the information necessary to further characterize the program and focus inspection activities. Frequently, photocopies of the applicable tools (see Appendix A, Inspection Tool Kit) are needed during interviews, so that the inspector can make notes in the margins or highlight sections for future discussion in more detail.

- Review the Common Deficiencies/Potential Concerns subheading in each section to help focus inspection activities, to determine whether any of the deficiencies are apparent, and to identify site-specific features that might indicate that more emphasis should be placed on selected areas or activities.

- Review Section 8, Analyzing Data and Interpreting Results, to provide additional focus to assure that data collection requirements are adequately planned for and to help provide a basis for assigning tasks to individual inspectors.

- Assign specific tasks to individual inspectors (or small teams of inspectors) by selecting specific items from the Data Collection Activities subheading in the section of interest. The assignments should be made to optimize efficiency and to ensure that all high-priority activities are accomplished.

- Take into consideration the guidelines in Section 7, Integration, when assigning tasks to ensure that efforts are not duplicated.

- Prioritize and schedule data collection activities to optimize efficiency and to ensure that high-priority activities are conducted early in the process. A careful prioritization of these activities provides the opportunity to determine whether personnel resources and inspection time are sufficient to adequately evaluate the inspected topic.

In the **conduct phase**, inspectors:

- Use the detailed information under the Data Collection Activities subheading in each section as guidance for interviews, document reviews, and tours. Inspectors may choose to use the interview tools provided in each of the topic sections to assist in data collection.

- Review the Common Deficiencies/Potential Concerns subheading in each section after completing each data collection activity to determine whether any concerns are apparent at the facility. If so, inspectors should then determine whether subsequent activities should be re-prioritized.

- Review Section 8, Analyzing Data and Interpreting Results, after completing each data collection activity to determine whether additional data is needed to evaluate the program. If additional activities are needed, inspectors should then determine whether subsequent activities should be re-prioritized.

In the **closure phase**, inspectors:

- Refer to the DOE Order Summary Extracts and Summary Analysis Tables in Appendix A, Inspection Tool Kit (see Tool 3-3, Organization and Staffing DOE Order Summary Extracts, and Tool 3-4, Organization and Staffing Summary Analysis Table, respectively, in Appendix A) to assist in referencing and evaluating findings.

- Use the Analyzing Data and Interpreting Results subheading in each section to help analyze the collected data and identify the impacts of identified deficiencies. This will aid in determining the significance of findings, if any, and assist inspectors in writing the "analysis" section of the inspection report.

Integrated Safeguards and Security Management

The Department is committed to conducting work efficiently and securely. DOE Policy 470.1, *Integrated Safeguards and Security Management (ISSM) Policy*, is designed to formalize a framework that encompasses all levels of activities and documentation related to ISSM.

The guiding principles of ISSM are:

- Individual responsibility and participation
- Line management responsibility for safeguards and security
- Clear roles and responsibilities
- Competence commensurate with responsibilities
- Balanced priorities
- Identification of safeguards and security requirements
- Tailored protection strategies through feedback and continuous improvement.

The five core functions of ISSM are:

1. Define the scope of work.
2. Analyze the hazards.
3. Develop and implement hazard controls.
4. Perform work within controls.
5. Provide feedback and continuous improvement.

For the purposes of this Protection Program Management Inspectors Guide, ISSM is an inherent function of management.

Individual Responsibility and Participation. Each individual is directly responsible for following security requirements and contributing to secure missions and workplaces.

Line Management Responsibility for Safeguards and Security. Line management is directly responsible for the protection of DOE/National Nuclear Security Administration (NNSA) assets, and as such is required to analyze risk, develop controls, and verify the adequacy of these controls.

Clear Roles and Responsibilities. Clear roles and responsibilities are indispensable to effective authority and individual accountability.

Competence Commensurate with Responsibilities. Individuals must possess the experience, knowledge, skills, and abilities necessary to fulfill their responsibilities.

Balanced Priorities. Each element of the safeguards and security program relies to some degree on the other elements. Managers' allocations of resources should indicate a "total program" mindset that makes security a mission enabler, not a mission inhibitor.

Identification of Safeguards and Security Requirements. Safeguards and security requirements have been established that, if properly implemented, will provide appropriate assurance that DOE/NNSA assets, workers, and the public are protected.

Tailored Protection Strategies through Feedback and Continuous Improvement. Feedback information on measures and controls is gathered during inspections, surveys, and self-assessments. Opportunities for tailoring safeguards and security programs to the site mission are also identified.

It is important to note that the categories above are only used to organize information in a way that will help inspectors gather data about performance in a structured and consistent manner.

Section 2

PLANNING PROCESS

Contents

References

DOE Order 470.1, *Safeguards and Security Program*

DOE Order 470.2B, *Independent Oversight and Performance Assurance Program*

DOE Policy 470.1, Chg 1, *Integrated Safeguards and Security Management Policy*

DOE Order 413.3, *Program and Project Management for the Acquisition of Capital Assets*

DOE Manual 413.3-1, *Project Management for the Acquisition of Capital Assets*

DOE Guide 120.1-5, *Guidelines for Performance Measurement*

General Information

This chapter outlines the principles of planning and the major aspects of planning and project management that an inspector might encounter during an evaluation of the safeguards and security planning process.

The Role of Planning

Planning is the first step in the safeguards and security management process. It consists of identifying organizational goals and objectives and deciding how to attain them. Organization and staffing actions, budget activities, and program direction and control are all outcomes of successful execution of the program plan. Without plans, there is no basis for action and no basis for evaluating success. Planning not only provides the path for action, but also enables management to evaluate the probability of success. The evaluation of the planning process should objectively address the adequacy and completeness of the process and the quality of the plans first (compliance), and then the success of the implementation (performance) of those plans. In other words, it is not uncommon for inspection activities to find plans that meet DOE requirements, yet that management has neither followed nor implemented.

Types of Plans

Strategic Plans

DOE planning can be characterized as either strategic or operational. Strategic planning provides management's vision in the form of strategic goals and objectives that deal with the broad question of *what* the Department's programs or activities are striving toward. Strategic planning is normally accomplished at the Headquarters level with expert input from the field. These plans address the *where* aspect, namely, where we are now and where we are going, and usually contain the following elements in some form:

- Mission of the organization
- Analysis of the current situation
- Future objectives
- Potential problems in achieving future objectives
- Course of action to attain future objectives.

Operating Plans

Operating plans include both Headquarters and field-level action plans that address *how* to carry out the Department's programs. Operating plans are intended to provide the direction and resources necessary to accomplish strategic or organizational goals and objectives. Some operating plans are multi-year plans, characterized by long-, mid-, and short-range planning horizons. Long-range DOE program plans are typically an extrapolation of the present program mission. Mid-range plans within the DOE typically cover a three-to-five-year range, with some construction activities extending beyond the five-year point. Short-range plans normally span less than three years. An example of a short-range plan is the Annual Program Plan for the budget-execution year, which provides the direction for accomplishing the organizational mission with budget-year funds. Accordingly, the longer the range, the more general the direction and the more variable the final execution strategy. Inspectors should realize that plans can be scrapped quickly in response to changes in Departmental guidance and direction.

Regardless of how many separate safeguards and security plans are prepared or what each might be named, a good planning process will identify:

- Organizational goals and objectives
- The selected approach to achieving goals and objectives
- Specific tasks to be performed in order to achieve goals and objectives
- Prioritization and required time-phasing or linking of tasks

- Organization and person(s) responsible for each task
- Resources required to accomplish each task
- Internal milestones and/or specific products for each task
- A mechanism for adjusting the plan as necessary
- A mechanism for independent review of task accomplishment.

DOE Planning Requirements

Headquarters-Level Plans

Project planning requires a/an:

- Designated person in charge who is accountable (e.g., the project manager)
- Specifically defined responsibilities and authorities for the project
- Clear scope of work
- Schedule(s) with milestones
- Overall plan for performance
- Tracking system.

DOE Order 413.3, *Project Management for the Acquisition of Capital Assets*, requires projects with values over $5 million to implement a project management plan that includes a series of pre-programmed critical decisions (CDs). The CDs are:

- CD-0: Approve Mission Need
- CD-1: Approve Alternative Selection and Cost Range
- CD-2: Approve Performance Baseline
- CD-3: Approve Start of Construction
- CD-4: Approve Start of Operations or Project Closeout.

The authority for making these decisions is based on the magnitude of the project and project cost, and is listed in Figure 2-1.

Critical Decision Authority	Total Project Cost	
Secretarial Acquisition Executive	**> $400M or < $400M when designated by Secretarial Acquisition Executive**	
Under Secretary/NNSA Administrator (Acquisition Executive)	**< $400M**	**Acquisition Executive Delegation Allowed***
		To Program Secretarial Officers or Deputy Administrators/Associate Administrators for NNSA
Program Secretarial Officers or Deputy Administrators for NNSA	**< $100M**	To a Program Manager or field organization manager
	< $20M	To a direct reporting subordinate of the field organization manager

*Critical Decision-0 (CD-0), Approve Mission Need, may not be delegated below Program Secretarial Officer or NNSA Deputy Administrator level. The Under Secretary/Administrator NNSA and the Deputy Secretary must be formally notified of all CD-0, Approve Mission Need, and CD-4, Approve Start of Operations or Project Closeout, decisions for non-major systems projects $100M and over.

Figure 2-1. Critical Decision Authority (DOE Manual 413.3-1, Ch. 2.2.1)

Safeguards and security should be an integral part of project planning and execution. The integrated project team should include safeguards and security representation, and the safeguards and security requirements should be an integrated element of all projects. Life-cycle cost analysis and overall system engineering should identify the requirements and costs for safeguards and security during early project planning. Early integration is essential in identifying and integrating cost-effective solutions to security requirements. Safeguards and security should be considered and incorporated in all phases of a project. Examples include:

- Pre-conceptual planning, drafting a preliminary vulnerability assessment (VA), and initiating operational security considerations
- Conceptual design including a more detailed conceptual VA
- Safeguards and security standards and requirements incorporated into the design criteria, specifications, and drawings
- Construction and testing that addresses and confirms that safeguards and security design requirements are validated through documented VAs.

Plans and considerations related to safeguards and security should be included as part of the Project Execution Plan and might affect such other components of the Project Execution Plan as emergency preparedness planning, communications, and procurement planning. From an inspection perspective, when a major project is under development at an inspected site, inspectors should evaluate the degree of compliance with these requirements.

Field-Level Plans

While all organizations need integrated long-, mid-, and short-range planning, inspectors often do not find long- and mid-range planning documents pertaining specifically to safeguards and security at the field level. A lack of documented long- and mid-range plans does not automatically indicate that this type of planning is not occurring. In these cases, inspectors must examine the processes and such products as out-year budgets, minutes of planning committee meetings, and corrective action plans (CAPs), any of which might contain evidence of long-range safeguards and security planning.

The Site Safeguards and Security Plan (SSSP) is the primary planning document that establishes specific levels of protection and acceptable risk levels for the site's security interests. It summarizes the current level of protection, as indicated by VAs, system performance tests, surveys, and inspections. It also identifies upgrades that are needed to reduce risk levels and/or eliminate temporary compensatory measures or operate in a more cost-effective manner. Contractors are required to maintain thorough backup documentation to support the conclusions and upgrade decisions contained in the SSSP. This documentation could include:

- Complete VAs
- System performance test results and analyses
- Cost/benefit analyses
- Studies
- Survey and inspection results.

The results of self-assessments, operations office surveys, and SP-40 inspections are important inputs to the site's planning process. Sites must make decisions about how to best correct deficiencies identified during these activities. A documented process is a necessary input for a management control system intended to assign priorities to corrective actions based on the relative risks associated with the deficiencies and their estimated costs. In addition, cost-benefit analyses should be conducted whenever appropriate to evaluate the range of options that might exist for correcting a deficiency. Planning and budgeting documentation will normally

provide evidence that long-term, cost-effective corrective actions were considered and adopted when appropriate, instead of relying exclusively on personnel-intensive measures for permanent fixes.

Safeguards and Security Topic Plans/Procedures

Table 2-1 contains a partial list of plans and their relevant topic areas.

While most of these are short-term planning documents or procedures for day-to-day operations, some will also contain elements of long- and mid-term planning in their respective topic areas. The presence (or absence) and quality of documentation and content, as well as whether it has been kept up to date, are important indicators of the adequacy of a site's safeguards and security planning program.

Table 2-1. Required Safeguards and Security Plans

Computer Security - Automated Data Processing Security Plans - Computer Protection Plans	Physical Security Systems - Lock and Key Program - Testing, Maintenance, and Quality Assurance Plan
Emergency Management - Operational Emergency Plan - Operational Emergency Procedures	Protective Force - Post Orders - Response Plans - Training Plan
Information Security - Technical Surveillance Countermeasures (TSCM) Plan - TEMPEST Plan (Emissions Security)	Protection Program Management - Acceptance and Validation Testing Program - Performance Assurance Program Plan - Protection Against Radiological and Toxicological Sabotage - Safeguards and Security Training Program - Site Safeguards and Security Plan
Material Control and Accountability (MC&A) - Internal Review and Assessment Plan - MC&A Plan - Operations Office MC&A Requirements Document (draft order)	Protection Program Operations - Intra-site Movement of Special Nuclear Material
Operations Security (OPSEC) - OPSEC Program Plan	Surveys - Survey Program Procedures
Personnel Security - Human Reliability Program Implementation Plan	

Common Deficiencies/Potential Concerns

Headquarters Level

Insufficient Safeguards and Security Planning

When program offices fail to give proper emphasis to their safeguards and security issues in their planning, their program staff has little or no knowledge of safeguards and security issues and considers planning to be an overhead activity best dealt with by the security staff or almost anyone else. In one case, the responsible secretarial officer's staff was unaware that dedicated Headquarters safeguards and security activities existed. While this is an extreme case, the lack of full coordination between security and operations on Headquarters staffs is very common. As a result, there is often a lack of meaningful review of plans and projected expenditures in the safeguards and security area.

Lack of Formal Coordination Procedures

Some secretarial offices attempt to deal with safeguards and security matters in isolation from other programs having responsibilities at a given site. Some assume too much authority; others assume too little. Both situations negatively impact safeguards and security at the site. In one case, the program office discounted safeguards and security evaluations done by others and depended on their own investigations. Some such cases lead to needless expenses and efforts, while in other cases, important measures were not implemented. In the planning area, lack of coordinated effort results in fragmented planning and inadequate attention to safeguards and security issues in budget and program planning.

Operations/Site Office Level

Neglect of the Planning Process for Federal Oversight Functions

Planning to support oversight of the safeguards and security program is often neglected. It is less common for plans specifically called for in the orders to be neglected, although this happens as well. In one case, an office "could not find" its technical surveillance countermeasures (TSCM) plan and was updating a TEMPEST (i.e., an emissions security testing) plan that was several years out of date. In another case, there was a total lack of TEMPEST, TSCM, and other required plans. In numerous cases, structures that have been built near protected areas had serious impacts on tactical operations because their construction and placement were not coordinated with safeguards and security management at the Federal level. Even when plans are in place, they are often outdated in reference to specific requirements or in reference to protection interest changes that are created by programmatic changes.

There is sometimes no overall planning within the operations office to support safeguards and security programs. In one case, large expenditures were being approved for a managed site without any overall protection strategy definition or strategic goal for the protection posture. In many cases, the operations office has no written plan or procedure for managing risk and evaluating the priority for safeguards and security expenditures across its sites.

Ineffective Coordination at the Site Office Level

When site offices are unable to devote sufficient resources to safeguards and security, the deficiencies and potential concerns are much the same as for the operations office. When a dedicated staff is not available, safeguards and

security responsibilities are often assigned as an extra duty to site office personnel, who have little or no background in the area and who spend most of their time on their primary programmatic responsibilities. In one case, the area office individual who was assigned responsibility for safeguards and security matters had not read the SSSP, had no place to store classified documents, and made brief, irregular visits to the contractor's safeguards and security director to read anything he had not seen. In general, an area site office without the assigned safeguards and security expertise is likely to provide ineffective protection program planning for sites under its control.

Lack of Planning at Managed Sites

Managers at operations and site offices might tolerate planning failures at the sites they manage. They often believe that if the current system does not fail on surveys or inspections, there is no need to spend great effort in planning. As a result, resources are often diverted into other activities, leaving marginal and/or very expensive protective measures in place, rather than dedicating resources into the analysis and planning required to implement a more effective or cost-efficient protection measure. In many cases, there is a marked aversion to planning.

Lack of Expertise to Review Plans

Some operations and site offices lack the analytical expertise to provide meaningful review of safeguards and security plans and programs. In particular, Federal staff often lack the training needed to conduct the complex vulnerability analysis techniques underlying many SSSPs. In such cases, the contractor submitting the plan might be able to obtain DOE approval in spite of flawed procedures and systems. On the other hand, the contractor might be unable to convince DOE of the value in an innovative cost savings plan.

Lack of Accountability for Planning

Planning, as an inherent task in an organization's mission, applies to all organizational levels, including contractors. All too often, unskilled and untrained managers fail to assume accountability for tasks unless they are explicitly defined. In the absence of well-defined roles and accountabilities, such implicit tasks as planning might be performed by chance rather than by deliberate action. Compounding this problem, field management sometimes splits responsibility for specific safeguards and security systems. This further obscures security planning responsibilities and accountabilities. Computer security is a common example of split roles. Classified computer security responsibilities, including planning, rest with the safeguards and security element, while unclassified computer security responsibilities reside with an administrative organizational element. This split not only results in fragmented planning, but also erodes the effectiveness of management controls for the entire cyber security program.

In most field organizations, functions and responsibilities are usually assigned in an organizational functions manual or some other directive. However, performance plans for responsible management officials and planners might not contain performance criteria that would hold them accountable for their planning activities.

Contractor Facilities

Lack of Emphasis on Planning

Among the many documents the contractor is obligated to deliver, safeguards and security plans are often not considered to be a high priority. At some locations, the safeguards and security staff consists primarily of operationally oriented personnel who see little value in planning beyond specific "tactical plans." Such staff might be distant from the local budget process, and might have little voice in long-range planning for facility operation.

Lack of Planning and Analysis Expertise

Some contractor sites use operations personnel to perform safeguards and security analyses and prepare safeguards and security plans. Such people might not have sufficient knowledge of the requirements to perform an adequate analysis or to prepare a comprehensive plan, even though it is very appropriate that they be included in this planning. Outside contractors, often employed to provide the necessary expertise, can be effective, but can also lead to a different set of problems (e.g., poor interface with operational staff and ineffective transitions when contracts expire).

No Procedures for Updating Plans

Table 2-1 contains a partial list of required safeguards and security plans. DOE orders require that certain plans be reviewed and updated at specified intervals. Regardless of whether periodic reviews are required, if the site lacks a tracking system and documentation procedures, many plans will quickly become outdated. At one location, plans were found that predated orders as far back as two previous revisions, with no evidence of review or updating. In addition, safety and security plans are frequently interrelated; thus, a change in one plan often requires a change in other plans. Without good planning management, a clear understanding of the relationships among the various safeguards and security plans, and the use of a tracking system, plans could become outdated and overlooked until a crisis arises or an inspection is announced. Good self-inspection and survey programs should identify such problems.

No Procedures for Integrating Plans

Safeguards and security program effectiveness depends on integrating various protection systems. Some locations do not have adequate procedures, either written separately or as part of existing plans, to ensure that integrated planning takes place. For example, the physical protection of special nuclear material (SNM) and classified matter generally requires the integration of three protection systems: the material control and accountability (MC&A) system, physical security systems, and the protective force. A change in any of the three systems without compensatory changes in the other systems will likely create vulnerabilities in the overall integrated protection system. Thus, a change in procedures or the implementation of new capabilities in one system should prompt a review of the other systems, and a change, if necessary.

Failure to Integrate Resource Requirements

Some plans are written specifically to meet the requirements of DOE orders and directives. However, when this approach prevails in an organization, isolated planning takes place, and planners fail to integrate protection system elements with requirements for funding consideration and/or the budget submission. For example, the addition of more physical security system access control measures might not have considered the impact on the protective force posting, training, and contingency planning. Or, the contractor might also have learned that it does not pay to spend an inordinate amount of time projecting for adequate resources if the contractor has been advised in advance that there is simply no room in the budget to provide them.

Procedures Inconsistent with Plans

The lack of a systematic process to integrate planning often leads to inconsistencies among plans, orders, and procedures. In such cases, updating the plans could be adequate, but the procedures and instructions for their implementation might lag. Only a complete planning process will ensure that when changes are made to a plan, they are, in fact, implemented.

Planning Activities

Planning for an inspection of a site's safeguards and security planning program should focus on:

- Developing an understanding of the site and its mission
- Identifying (and reviewing as many as possible) relevant planning documents
- Conducting preliminary interviews with site representatives to gain a basic understanding of their planning process
- Identifying specific aspects of the program to focus on, such as, indicators of management effectiveness (case studies)
- Developing inspection-specific planning documentation, such as inspection plans, schedules, and data-gathering forms.

A good source for descriptive information on the site and its mission is the SSSP, which can be a source for such relevant planning documents as:

- A preliminary status assessment of the status of planning at the facility
- A preliminary list of key planning issues to include in the inspection
- A list of planning items that other topic teams will be covering (make arrangements to obtain any data needed from other topic teams)
- Any significant planning issues that are not being covered by another topic team for possible inclusion in the PPM planning subtopic
- A preliminary list of persons to be interviewed during data collection.

Further information for the planning process can be derived by:

- Determining through other document reviews and interviews with program office and site representatives whether other planning documents exist pertaining to safeguards and security at the site
- Requesting specific documents from the inspection chief and/or deputy inspection chief, or their designee(s)
- Reviewing program office and safeguards and security project planning documents for general familiarization
- Reviewing site-specific planning documents, such as the SSSP for general site information as well as upgrades identified during the SSSP process and the budgeting plans.

Guidance on preparing inspection plans and other supporting documents is contained in the Safeguards and Security Appraisal Process Guide. Several generic data collection tools are contained in this guide as well. They should be modified as necessary to meet inspection-specific needs.

The nature of the Planning Process subtopic limits data collection to the primary techniques of personal interview, document review, and the use of specific planning tools or techniques. Following a preliminary review of the documentation available and coordination with the other topic teams, the PPM team should develop a final set of issues to investigate during the inspection. From this set of issues, a data collection plan can then be developed and used to evaluate the overall status of PPM, including the planning subtopic. In final form, this collection plan will list documents to be formally evaluated, persons to be interviewed, and a minimum set of interview questions for each interview.

The data collection plan should correlate collected data with the issues being evaluated to ensure that only relevant data is collected and analyzed.

The case study approach is a good inspection technique for measuring management effectiveness in the planning or decision-making process. During inspection planning, issues are

identified to be pursued during the data collection process. By the end of the document review and/or preliminary interviews with the site representatives, the inspector should have identified those critical planning issues that seem weak. If there are no apparently weak systems or plans that need careful review, the inspector should look for one particularly noteworthy system and follow it through during data collection to scrutinize the process and determine exactly how management arrived at a particular decision or plan. An example might be a study of physical upgrades to determine how the operations office selected those particular upgrades and what cost analysis was completed to arrive at the resource plan.

Data Collection Activities

DOE Headquarters Guidance to the Field

A. Inspectors should interview key protection program personnel at the responsible Headquarters program and secretarial office level and review any formal Headquarters planning guidance that addresses protection strategies and requirements for the inspected site.

B. Inspectors should determine through interviews with field safeguards and security management personnel whether the guidance was received and in what form, whether it was understood, and how it was implemented.

C. Inspectors should compare the SSSP and its protection strategies, including the resource plan and/or budget submission, to Headquarters guidance for consistency.

SSSP Evaluation

D. The SSSP provides the planning basis for all other safeguards and security plans at an inspected facility that has Category I and II quantities of SNM. Inspectors should determine whether the inspected site has an SSSP and whether it is current. During this part of the inspection, it is essential that timely and effective coordination be conducted with the inspection team lead and SP-40 management. The physical security systems, protective force, and MC&A topic teams will all be evaluating various aspects of the details of the SSSP. The topic teams will emphasize the validity of the SSSP contents and how well the plan is being implemented. **The process used by the inspected facility to develop, review, and update the SSSP is a major PPM team interest item.**

E. Inspectors should conduct DOE Headquarters and site office interviews to identify pre-approval review procedures. Inspectors should review the SSSP thoroughly and coordinate with other topic teams to confirm that the security measures described therein are implemented. It is important to determine the last approval date, the process for producing the next SSSP, and the projected date for approval of a revised SSSP, and conduct interviews with those responsible for preparing, reviewing, and approving the SSSP.

Vulnerability Assessment Evaluation

F. Since VAs are to be the basis for site protection strategies, it is extremely important to ensure that they:

- Adequately address Department policy
- Accurately reflect the status of protective systems
- Are supported by performance tests or accurate data and/or expert opinion.

Inspectors should perform a careful and detailed review of the site's VA process, baseline assumptions, and the data used in the assessment. The Vulnerability Assessment Report (Tool 2-5) in Appendix A, the Inspection Tool Kit, treats this subject fully.

Topic Plan Evaluation

G. A strong indicator of the protection program planning status is the quality and comprehensiveness of required plans. These plans must be sufficient to assure that the facility protection system will not fail due to lack of planning. Inspectors should use the Plan Evaluation Worksheet in the Inspection Tool Kit (see Tool 2-3 in Appendix A) to help record the assessment of each plan reviewed. The planning elements contained in the worksheet should reflect the expected results from a valid planning process. Some of these elements will not apply in all plans. In these cases, inspectors should indicate "not applicable" (NA) under the section(s) heading and include any appropriate remarks in the reviewer comments column. Each of these elements refers to the plan being evaluated. For example, goals and objectives refer to whether the plan being evaluated states goals and objectives and, if so, where and how well. Similarly, the general approach refers to whether the general approach to achieving goals and objectives is included and is adequately addressed.

Emergency and Contingency Plan Evaluation

Because they do not affect daily operations, emergency and contingency plans are easily forgotten in the programmatic plan development process and the planning update cycle. These plans are extensions of the operational plans and are used to deal with unusual program occurrences or situations. Changes in the site or facility operational functions, including physical plant construction, directly affect emergency and contingency plans.

H. Inspectors should coordinate with other topic teams and ask them to compare the topic emergency and contingency plans to safeguards and security topic plans and the SSSP to determine whether the plans are current, consistent, and aimed at achieving a common protection strategy.

Procedures for Plan Development

A planning process without either formal or informal integration procedures (often called "change control" procedures) cannot ensure that all elements are considered in plan development. Such a process often results in fragmented and vague plans.

I. Inspectors should determine whether the PPM planning process includes procedures for obtaining technical input from appropriate topic experts at operations office and site organization levels, and whether management is actively involved in the plan review process.

Procedures for Controlling and Updating Plans

J. Through interviews and/or document reviews, identify the site's procedures for safeguards and security plan updates and how revisions are scheduled and documented. For example, there should be some means of recording when the plan was last reviewed and updated. Inspectors should review key safeguards and security plans to determine whether the plans contain sufficient methodologies and instructions to ensure adequate coordination and integration with other safeguards and security topic plans.

K. Inspectors should determine how plans and procedures are updated out of the normal cycle (e.g., the annual review) when abrupt programmatic or operational changes require immediate revisions.

Accountability for Planning

Control measures (e.g., award fee contracts) are available to management for holding contractors and individuals accountable for their assigned responsibilities.

L. Inspectors should determine whether management effectively uses the award fee and award fee plan either by interviewing appropriate line management and/or contract management or by reviewing the award fee plan. Planning requirements can be written into the award fee plan (with performance criteria) and periodically evaluated (usually every six months). Depending upon the weight given to the performance element, the amount of the award fee is either increased or decreased based on the level of performance.

M. Some of the best tools available to management for holding individuals accountable for planning are the individual performance plans, performance appraisals, compensation, and promotion systems. Inspectors should determine through interviews with line and safeguards and security management how they hold general management and staff accountable for their planning responsibilities, and whether they use these management tools.

N. When appropriate, inspectors should elect to review a sample of position descriptions of individuals who have responsibilities for planning functions to determine whether these responsibilities are adequately reflected at the individual level and whether personal accountability is documented.

Consistency Among Plans and Procedures

O. Inspectors should compare key safeguards and security plans with procedures actually practiced at the site or the facility. Inspectors should coordinate with other topic teams for assistance in this comparison, either through performance tests or interviews. For key plans that are not being covered by other topic teams, inspectors should interview appropriate management or staff and then compare the results to the key performance elements of the plan. Inspectors should look for consistency among the plans and the actual programmatic operations at the site. For example, inspectors should be sure that the SSSP accurately describes the functions actually being performed at the site and that the survey plan actually includes all facilities requiring surveys in the operations/area office's jurisdictional area.

Availability of Vulnerability Assessment Evidence Files

P. The risk acceptance in the SSSP must be based on carefully analyzed data in VAs that is validated through performance testing. These analyses and validations must be documented by the responsible organization.

Q. Inspectors should review the backup documentation and determine whether the VA documents and the validation results from the performance testing are on hand and whether these files are reviewed during the planning process and adequately support the final protection system design implemented at the site.

Observations by Other Topic Teams

During data collection, other topic teams might identify data points and concerns that are of interest to the PPM team during the planning process review. Findings and related indications developed by other topic teams are frequently excellent indicators of higher-level management problems in the planning process. Involve every topic team with evaluating the development and implementation of both centralized planning documents (e.g., SSSP) and planning documents associated with their topic areas (e.g., operations security [OPSEC] plan, MC&A plan). Expect that topic teams will inspect their topic area to determine the effectiveness of topic area plans. Draw heavily on the experience, expertise, and ongoing inspection activities of the other teams.

Section 3

ORGANIZATION AND STAFFING

Contents

References

DOE Policy 111.1, *Departmental Organization Management System*

DOE Order 360.1B, *Federal Employee Training*

DOE Manual 360.1B, *Federal Employee Training Manual*

DOE Order 320.1, *Acquiring and Positioning Human Resources*

DOE Order 470.1, *Safeguards and Security Program*

General Information

Organization

One function of safeguards and security management is to provide for the organization, staffing, training, and equipping of safeguards and security programs to assure full and efficient implementation of safeguards and security policy goals at all organizational levels. Organizational levels to be evaluated range from the Headquarters to the safeguards and security staffs of management and operations (M&O) and protective force contractors. Factors to be considered when inspecting this subtopic follow.

Level of Organization

The organizational level of the safeguards and security function affects its ability to perform effectively. A level that is too low means that the safeguards and security program might not be appropriately considered in allocating resources, and might lack the authority necessary to assure that safeguards and security functions are effectively implemented.

When evaluating this subtopic, it is important to assure that the operating base of strength for the safeguards and security function is the one that is evaluated. For example, an administrative vice president who has safeguards and security as one of many responsibilities is not the optimum base element for evaluation. Generally, the highest level full-time position represents control of the program (such as the director of safeguards and security or similar title) and the operating base of strength.

The appropriateness of the organizational level assigned to the safeguards and security function is determined by:

- Parallel interactions with site and field organizations
- Visibility of and priority afforded the site safeguards and security program
- Channels and authority for obtaining funding and personnel resources
- Access for safeguards and security to the site/operations office manager
- Formal and informal interaction with internal staff heads
- Authority to issue and implement safeguards and security policy
- Authority to develop and enforce safeguards and security program elements
- Formal and informal interaction with heads of operational elements
- Results of such interactions provide appropriate levels of security (this is the most important criterion).

Organizational Structure

The organizational structure is the means through which management can control, supervise, delegate, set responsibilities, and synchronize the work done by individuals, departments, and divisions. The structure also affects employee morale. For example, an organizational structure that allows workers to understand their jobs and reporting requirements, the functions and tasks for which they are accountable, and the parts they play in the global scene help to produce a successful safeguards and security program.

For inspection purposes, the following significant factors should be examined in relation to the specific site and organization being evaluated.

Integration of Safeguards and Security

DOE orders treat safeguards (e.g., MC&A) and security as separate topics, while recognizing that they are interrelated through ISSM policy and guidance. DOE orders do not direct the organizational level at which safeguards and security should be integrated. At some sites, the MC&A functions and other security functions are integrated at the level of the safeguards and security director. At such sites, the manager responsible for MC&A reports to the safeguards and security director, as do managers of other security functions. At other sites, the MC&A functions are placed under administrative organizations with audit and accounting responsibilities. Experience has shown that integration at the safeguards and security director level promotes effective communication and effective integration of nuclear MC&A functions with other security functions (most

importantly, physical security and protective force operations). If the nuclear MC&A functions and other security functions are not accountable to a manager who is actively involved in the total safeguards and security program, there will likely be communications failures or difficulty in effectively integrating the programs to protect all security interests.

These same considerations apply to other security functions for which line responsibility is sometimes assigned outside the security organization (e.g., computer security, security system hardware maintenance, badging, and visitor control). Current DOE trends toward flattening organizational structures might contribute to the dispersion of safeguards and security functions.

Management Principles

This overview of management principles highlights the types of attributes common to effective organizations and should aid the inspector in describing the degree to which the principles are present or absent.

Delegation of Authority. Managers delegate the authority to make decisions based on the decisions' potential impact, the responsibilities of the person who needs the authority delegated, and the frequency of the activity. Authority should be delegated in a manner that ensures that supervisors understand and are held accountable for the outcomes. Delegated authority should have a sufficient scope that permits an appropriate measure of control over subordinates. There must also be a distribution of authority, so that all decision-makers can discharge their duties promptly and with good judgment. Authority, responsibility, and accountability go together and should be clearly understood by every person in a supervisory capacity. Inspectors sometimes find programs where the owning manager does not have the authority to make the decisions necessary to be effective. For example, at one site, the owner of the survey program was not authorized to insist on effective corrective action plans from the contractor.

Span of Control. Span of control refers to the number of organizational and/or functional entities supervised or controlled by a single individual. Accordingly, the optimum span of control within a DOE organizational structure might vary according to institutional experience, the capability and personality of onsite managers, the existence or lack of indicators of organizational problems, and individual workload.

Too small a span of control might indicate excessive centralization, with its attendant inefficiencies and lack of response. Too great a span of control might indicate excessive decentralization, with the related problem of fragmented implementation of subprograms. The span of control should be evaluated for effectiveness with respect to an individual's responsibilities and how well it has supported the organizational mission.

Checks and Balances. The organizational structure should incorporate a system of checks and balances. Quality assurance, self-appraisal, and internal review groups are normally organizationally independent of the organizational elements they are expected to check; these independent functions typically report directly to a line manager. A well-defined line to top management is needed to assure that identified problem areas reach a level of authority and responsibility that can direct corrective action without conflict of interest.

Clearly Defined Duties. Each organizational element (or component) should have a clear statement of its mission and functions. An organization and functions manual or similar document should clearly define the tasks to be performed by each element and assure that no unintentional overlap or voids exist among elements. It is also essential to ensure that all required duties have been assigned and that accountability is established.

Subdivision of Supervisory Authority. The extent to which duties and functions are subdivided and the chain and delegation of

authority, responsibility, and accountability also must be clear. The same factors used to determine the basic organizational structure are applicable to evaluating subdivisions. The intermediate supervision required is determined by examining the number of workers involved, their degree of skill or professionalism, and the relative complexity of the functions to be performed. For example, at one site, the security manager responsible for the survey program had delegated the program to a subordinate just prior to the inspection. The person who was given responsibility for the survey program insisted that she was not the program manager; in fact, no one in the organization could identify the program manager.

Flexibility. Few organizational structures can be expected to prove satisfactory forever. Changes become necessary due to new or changed missions for the organization management, and/or organizational enhancements based on experience. For an inspection, the optimum organizational plan recognizes and anticipates the need for change and designs the organization accordingly. An adequate organizational structure can accommodate changes with minimum disruption of non-affected elements.

Levels of Management. An effective organizational structure provides a framework for coordinating and implementing the plans and policies developed by the top management of the organization being inspected. The main function of lower-level management and supervisors is to execute final decisions, develop the detailed plans and policies directed by top management, and implement the safeguards and security program accordingly. The organizational structure should support top management by addressing and solving evolving problems at the lowest level possible that controls the resources necessary to do so. For lower-level management, the structure should emphasize support for routine tasks.

Staffing/Budget Requirements. Any organizational structure produces a characteristic set of staffing and budget requirements. Budgetary limitations restricting the number of personnel or organizational levels might, in turn, affect how the organization is structured and its effectiveness.

Committee Organizations. Apart from the formal organizational structure, the committee organization, or working group, is frequently used within the DOE community. Working groups are not appropriate when used as a substitute for required organizational changes, or when they are used to carry out duties specifically assigned to personnel within the organization. An example of the latter would be a joint contractor-Federal committee with the authority to approve changes in security procedures instead of the responsible Federal manager. For example, in the past, two sites set up committees that were able to make final decisions that overruled the contractor and Federal site director's decisions.

The effectiveness of working groups can be evaluated by the results produced. In general, the advantages of a working group include:

- Concurrence can be promoted by including representatives of all affected organizational elements.
- Acceptance of the resulting decisions can be promoted by reducing the influence of personalities.

Typical disadvantages of working groups include:

- Results emerge relatively slowly.
- Products are usually compromised.
- Decision accountability can become diluted.

Communications

The structure and staffing of an organization have a direct impact on organizational communications. Effective management is dependent upon effective communications not only within the organization, but also among the organization and subordinate, superior, and lateral organizations. Timely, accurate, and clear

promulgation of management's policies, guidance, and decisions is essential. Equally important is the interaction among personnel and organizational components, and among the components of separate organizations. Some broad categories of communications are of value to consider during an inspection.

Vertical communication between higher and lower organizations and between internal organizational levels is required to clearly transmit oral and written direction and to provide a feedback and control system for the manager and other supervisors (see Section 6). Two-way vertical communication is essential for an organization to operate at peak efficiency.

Internal and external lateral communications are needed to coordinate projects and functions that affect more than one organizational component; effective communication might be important even if only one component is affected. Making and implementing policies require this type of coordination.

Formal and informal communications systems are found within all organizations. The formal system is designed by management and consists of elements such as the administrative procedures for providing program direction (see Section 5), paper flow, filing, delegation of authority, assignment of responsibility, and all related administrative/management policy and procedures. The informal communications system is normally based on personalities, working environment, voids or inefficiencies in the formal system, and associated factors. For example, one person having worked closely in a previous organization with a new supervisor might be more successful than others in having access to the new supervisor and thereby gaining acceptance of his or her opinions. If there are indications that a strong informal system is playing a significant role in the operation of the organization, it might indicate the formal system is inadequate or the informal system is working against the formal system. Either way, further evaluation is prudent. An organization that depends upon an informal communications system is likely to experience communication failures (e.g., failure to inform some groups of revisions to policies and procedures).

Staffing

The inspector's job is not to determine and validate specific staffing levels and individual performance; rather, the inspector should monitor staffing problems within the organization and determine what, if any, adverse impact might be affecting the facility's capability to achieve safeguards and security objectives.

Significant staffing factors to consider are discussed below.

Budget Limitations. Budget limitations may affect the staffing of an organization by restricting the level of qualifications that can be requested, the number of full-time equivalents authorized, limitations on new hires, or the overall personnel budget.

Impact of Organizational Structure. Staffing requirements, especially at the supervisory and managerial levels, are influenced directly by the organizational structure. The number and level of supervisory positions generally increase in fragmented organizations. The staffing at each site and for each organizational level should be evaluated against how successful and efficient it is in implementing an effective safeguards and security program.

Ratio of Supervisors to Supervised. While no prescribed rules exist for determining how many employees a supervisor can effectively supervise, as a general rule a first-level DOE supervisor should supervise a minimum of five employees, and a second-level supervisor should normally direct no less than three first-level supervisors.

Workload. Ideally, workload is the predominant factor for determining optimum staffing levels. However, many tasks are not easily quantified into work units that can be equated to requirements for a specific number of staff personnel. Also, workloads for safeguards and

security staff members typically have peaks and valleys and frequently are driven by unpredictable events. Accordingly, inspectors may be able to form an opinion on the workload assigned to a position or individual, but rarely are able to support the opinion with sufficient validated hard data to support a strong position that staffing is an issue because of excessive or moderate workload. Regardless, inspectors can readily identify when necessary program tasks are omitted or are not being accomplished adequately.

Position Description. Every government and contractor position should be supported by a written position description, ideally supported by a job-task analysis. Job-task analyses are typically performed to develop or validate a job description and to assist in position management. An unexplained discrepancy of any significance between the job description and the actual tasks being performed by the individual should be examined. Inspectors should look for evidence of a process that can design positions to combine logical and consistent duties and responsibilities into effective, efficient, and productive mission-oriented organizations.

Staff Qualifications and Training. A safeguards and security program is only as good as the capabilities of the personnel accountable for implementing the program. A formal training plan for Federal employees that identifies short- and long-term training requirements and individual skills development for the safeguards and security staff members is essential to assure that staffs are qualified. Ideally, such a plan addresses the entire spectrum of training, from on-the-job training to attendance at formal courses. Attendance at mandatory training and the attainment and maintenance of the required level of individual proficiency is typically documented. Without adequate plans and training records, the qualifications of the safeguards and security staff cannot be assured.

M&O contractor organizations are bound by various provisions of their contracts and by reference to DOE orders to provide qualified personnel in support of the contract. Although no general training requirements existed in the past for contractor organizations, a prudent contractor will support all personnel with a planned training program to maintain qualified personnel and demonstrate compliance with the contract and specific order provisions. An inspector should question the contractor and the operations office concerning the qualifications and training of the M&O contractor safeguards and security staff and the training points of contact required. If there are indications of a shortage of qualified personnel or a lack of adequate training, the condition should be evaluated.

Planning and Program Direction

Planning (see Section 2) and program direction (see Section 5) must be combined in a way that supports an effective safeguards and security program. To combine these functions effectively, a continuous management cycle of planning, organizing and staffing, directing, coordinating, and controlling is typically established. Planning is the starting point for most other management functions. It begins with an analysis of the organization's mission and functions.

Control Measures

Control systems are essential for establishing and maintaining an effective organizational structure that is properly staffed. The feedback element provides continuous information to the manager based upon surveys, inspections, self-evaluations/assessments, and reporting and critical issue tracking. Inspectors should determine whether such control feedback mechanisms have addressed the organization and staffing of the involved site/facilities.

Common Deficiencies/Potential Concerns

Excessive Use of Working Groups

Working groups can be effective and are frequently the optimum type of organization for implementing programs or solving problems. In some cases, they are prescribed by DOE orders. However, they are not appropriate as a substitute for a competently developed organizational structure.

Working groups are often formed simply to avoid, mitigate, or circumvent the influence of personalities, managers, or supervisors who should organizationally be assigned or participate in the task rather than the working group. Over-reliance on working groups can prolong an unpopular task or delay a difficult decision. Indications of such problems might be revealed by comparing the charter and bottom-line results of the working groups with the mission and functions of the staff sections within the organization. Often, working groups are tasked to perform functions routinely performed by staff elements. Interviews frequently provide the first indication of this problem by individuals expressing frustration about excessive, unwarranted, or ineffective time spent in working groups or coordinating with working groups.

Frequent Changes in the Organizational Structure

The frequency of organizational changes can be determined by interviews and document review. In addition to disrupting staff, inappropriate changes might indicate basic management problems. In every case, frequent organizational changes challenge the organization's communications effectiveness. Although some organizational changes are necessary, repeated changes not based on an identifiable need might indicate that management does not adequately consider basic organizational factors. Management might be simply lacking experience in developing functional organizational structures; they might be organizing around personalities, experimenting, or reacting to a high turnover in personnel or changing missions.

Lack of Documentation

Document review and interviews disclose the existence or nonexistence of backup material to support the need for organizational changes. Federal office organizational changes must be coordinated with the site's human resources group before announcement and implementation. The information and documentation required for this advance coordination is specified and should be available for review.

No similar requirement exists when the site M&O contractor develops or changes the security organization. However, site administrative procedures or the contract document generally requires, and good management practice dictates, documentation in the form of mission and functions statements, organization charts, justification for change, job descriptions, job-task analyses, and a formal approval process. In every case, frequent organizational changes challenge the organization's communications effectiveness.

Unclear Lines of Communication

The formal flow of information, responsibility, and authority should follow the organizational structure. Some poorly conceived organizations operate wholly on informal lines of communication that circumvent weaknesses inherent in the formal organization. This might indicate a major flaw in the organizational structure, or it may result from difficulties with personalities or human interactions. Regardless of the reason, in a properly organized and staffed program, formal lines of communication usually follow the organizational structure while informal lines of communication usually serve to expedite day-to-day consideration of issues prior to formal actions.

Lines of communication above the field elements must be in consonance with current Headquarters policy and guidance and should be clearly defined, understood, and followed so that management, policy, and budget matters flow smoothly.

Organizational Level Unsuitable for Ensuring Compliance

Inspectors might find that the person or organizational component responsible for policy and procedures is positioned too low in the organization to assure that deficiencies in compliance can be remedied. This condition is most likely present when the responsible component or person in the security organization has little control over the security activities of operations/production personnel. In such a case, operations/production managers may place low priority on complying with security policies and procedures.

This problem is more likely to become evident to other topic teams during the course of their data collection than to the PPM topic team. This potential situation should be identified and addressed during the planning meeting, and integration among all topic teams should be initiated. When this situation does appear, all involved topic teams should investigate it. (Overall organization and staffing should be examined by the PPM team; the effectiveness of managing the specific topic should be examined by the appropriate topic team.)

Responsibilities Not Assigned

Management might fail to fully document which organizations and persons are responsible and accountable for various safeguards and security program elements. This situation is found most often in organizations that have not followed a systematic procedure for assigning responsibility and accountability, or in organizations that have a history of deficient safeguards and security programs. Frequent organizational changes or shifts in responsibility can also result in documentation that is incomplete, inaccurate, nonexistent, or not effectively communicated throughout the organization. Although this problem might be discovered initially by another topic team, the root cause of the problem might well be an overall management problem. Such problems can best be addressed by the PPM topic team.

Planning Activities

During the planning meeting, inspectors identify the organizational elements involved, organizational structures of each involved Headquarters, lines of authority and responsibility from top to bottom, staffing levels, the cognizant secretarial officer (CSO), and other involved program offices for the inspected facility. The following documents from each of the organizational levels involved in the inspection should be reviewed:

- Site Safeguards and Security Plan
- Organizations and functions manual(s)
- Mission statement
- Organization and staffing studies and surveys
- Agreements and memoranda of understanding affecting organization and staffing
- Protection program budget and budget development guidance
- Organization and staffing-related policy and procedures
- Documents related to assignment of responsibility and accountability
- Safeguards and Security Information Management System (SSIMS) data related to previous findings and CAPs.

During this review, inspectors should identify the facilities and Headquarters elements deemed necessary to visit for data collection purposes. Interviews with points of contact and document review should provide the following information:

- Approved organization and associated staffing levels dedicated to safeguards and security at each organizational level
- Organizational elements and staff members contributing but not dedicated to safeguards and security
- Organizational alignments, responsibilities, and accountability from top to bottom, with emphasis on where the safeguards and security function is assigned
- Facility and organizational-level documentation, policy, and procedures that affect the safeguards and security organization and staff.

Inspectors should focus on determining the:

- Effectiveness of the organization
- Relationship among staffing levels and workload
- Qualifications and training of safeguards and security personnel.

Data Collection Activities

Staffing

A. The Inspection Tool Kit (see Tool 3-1, Organizational and Staffing General Data Collection Questions, and Tool 3-2, Organization and Staffing Specific Data Collection Questions, in Appendix A) provides a list of questions appropriate for initiating interviews, particularly at top-level management positions. These questions can also be helpful in more detailed interviews on specific topics. Inspectors should use the responses to help form an impression of the overall safeguards and security program and obtain leads for further investigation. Interviews should include, for example, the following questions:

- Has management established an effective and efficient organizational structure?
- Are staffing levels adequate to support the organizational structure and fulfill the functional requirements?
- Are personnel qualified and trained for their position?

Organizational Structure and Interfaces

Headquarters Elements

B. Inspectors should review the organization and the mission and functions statements of the applicable CSO, program office, and the Office of the Associate Deputy Secretary for Field Management to determine the safeguards and security responsibilities of each for the field element being inspected. Inspectors should maintain the primary objective of the review, which is to determine specifically how and by whom the safeguards and security function is executed at the Headquarters level.

Field Elements

C. Inspectors should review the operations office organizational charts and mission statements in detail, preferably with the assistance of a knowledgeable point of contact who can explain the duties and functions of each office. Inspectors should also identify the personnel/ offices with responsibility for each of the following functions: planning, budget development, MC&A, TSCM, OPSEC, surveys, personnel security, classified matter protection and control, computer security, protective force, self-assessments, and critical action tracking.

D. The following list identifies factors to focus on during the review; however, finding any of these factors is not necessarily a deficiency. Rather, the factors are general areas of interest where indicators of potential problems may be found. Inspectors should determine what additional information is needed to substantiate whether a problem exists (reference additional data collection activities as appropriate):

- Persons/offices having an unusually large number (more than five) of functions for which they are responsible, or a large number of organizational components reporting to them.

- Organization structures having an unusual number of layers with only a small number (less than three) of functions/office/personnel reporting to them.

- Offices/functions having security-related primary functions that are organizationally removed from the safeguards and security organization; for example, computer security groups that are in the information processing division; physical security hardware groups in plant maintenance; or badging in the administration division.

- The placement of an unusually large number of layers between the safeguards and security managers and the senior managers, or placement of the safeguards and security function in the organization such that it has little authority or interest to ensure that production/operations-related managers implement required safeguards and security functions.

- Organizational structures that appear to place the safeguards and security function at a level below that required for the safeguards and security manager to have the position, responsibility, and authority necessary to direct and implement the safeguards and security program.

- Functions and tasks required to be performed for which no organizational component is clearly accountable.

- Frequent changes in the organizational structure.

Communications

E. Inspectors should review the organizational structure of the Federal field element, the prime M&O contractor, and the protective force contractor (if different from the M&O contractor) in parallel to identify interfaces and the formal and informal lines of communication among the various organizations. The reviews should be structured to involve reviewing organizational charts and interviewing key safeguards and security managers. Inspectors may interview representatives of each organization present simultaneously or representatives of each organization in separate session, or a combination of both. (Simultaneous sessions are usually a better forum for gathering information quickly, whereas more candid responses might be elicited in separate sessions.) Inspectors should consider these elements and follow up on:

- Formal communications paths for safeguards and security direction to contractors that appear excessively convoluted; for example, operations office computer security group to the safeguards and security division to an administrative element to program office to program representative to contracting officer's technical representative (COTR) to contractor.

- Formal communications paths from the operations office to the contractor on safeguards and security matters that bypass the safeguards and security division (e.g., computer security to information security to COTR to contractor).

- Frequency of meetings between parallel offices at an equivalent level of responsibility (e.g., operations office safeguards and security director to contractor safeguards and security director, or operations office physical security branch chief to contractor physical security manager).

Responsibilities and Authorities

F. For selected functions/offices, inspectors should compare the mission and responsibilities against the authorities and resources. Such a comparison may be particularly important if there is a question about the span of control, or if there is some evidence of problems with accomplishing the assigned functions. The Inspection Tool Kit (see Tool 3-2, Organizational and Staffing Specific Data Collection Questions, in Appendix A) provides methods for conducting such reviews. Areas of concern may include:

- Too many functions reporting to the same manager
- Excessive levels of management
- An "isolated" office with safeguards and security responsibility
- Organizational level of the safeguards and security function.

Adequacy of Staffing

G. Detailed staffing surveys, position evaluations, and job-task analyses are the means by which adequate staffing levels are determined, and inspectors should obtain these documents for review. It is beyond the scope of the inspection to perform these specialized tasks; however, inspectors must be cognizant of staffing requirements by identifying potential shortages and overages of staff members. Except for guard posts, inspectors should understand that there are few formulas or criteria available to determine optimum staffing.

H. Inspectors should review the budget and related staffing-level documents to determine the actual and authorized full-time equivalent positions for the organization. Any significant differences between the full-time equivalents authorized and those actually performing the work might indicate a staffing problem. Inspectors should determine the impact of personnel shortages shown or claimed by the organization. A valid shortage of staff members will be accompanied by a quantifiable backlog of work that is easily identified and validated.

I. Personnel shortages, if they are perceived by management to exist, typically form one of the first topics that surface in interviews with managers and staff. Inspectors should identify inadequate staffing early; excess staffing will seldom be voluntarily identified and is not usual. (Caution: Inspectors must avoid being put in the position of validating specific numbers of shortages, which might then be used by management to justify staffing requests.) Inspectors must investigate apparent shortages that might simply result from an imbalance of personnel assignments. Most important, inspectors should also determine what impact the shortage of personnel has on the safeguards and security program. Indicators of staffing problems include:

- Unusually "steep" or "flat" organizational hierarchies
- Magnitude and effect of recent budget cuts
- Over-reliance on extensive (sub)contractor support
- Excessive paid and unpaid overtime
- Significant personnel turnover, possibly with an associated problem of recruiting qualified personnel
- Excessive detailing of personnel to accomplish routine tasks, to the detriment of their primary duties and responsibilities

- Frequent observation of inactivity in the workplace
- Habitual failure to complete the same work requirement
- Grossly outdated position descriptions
- Habitual use of safeguards and security personnel in nonessential and/or unrelated functions.

Other areas of potential concern include:

- Inadequate staff training
- Inappropriate use of working groups
- Frequent changes to the safeguards and security organization structure.

J. As a topic team, inspectors should identify data points and concerns that are of interest to PPM as the team reviews the organization and staffing. Findings and related indications developed by other topic teams are frequently excellent indicators of management problems caused by deficiencies in organization and staffing if the problems are a result of management inattention. Inspectors should not get involved with staffing concerns that management is aware of and can/could have resolved at the lowest level. However, inspectors should consider these indications by the PPM team for applicability to the evaluation of the organization and its staffing.

K. Inspectors should pay particular attention to staffing and personnel qualification issues identified by other topic teams as potential problems. If the problems are confined to one topic area, they might not be of concern to the PPM team. However, if there are staffing shortages or major training deficiencies in multiple topic areas, inspectors should scrutinize those elements and their impact on the safeguards and security function to determine whether they are indicators of PPM efficiency.

Other topic teams are frequently concerned about the location of their topic area within the overall safeguards and security organizational structure. If the PPM team discerns a potential problem with the organization for safeguards and security, other topic teams can assist in validating the problem by addressing the impact of the suspected organizational deficiencies. Other topic teams might also identify organizational problems that, when combined with related observations by the PPM and other teams, will reveal a concern about the organizational structure for further review.

Section 4

BUDGET PROCESS

Contents

References

DOE Order 413.1A, *Management Control Program*

DOE Order 130.1, *Budget Formulation*

DOE Manual 135.1-1, *Budget Execution Manual*

DOE Policy 111.1, *Departmental Organization Management System*

DOE Order 412.1A, *Work Authorization System*

DOE Policy 413.1, *Program and Project Management Policy for the Planning, Programming, Budgeting, and Acquisition of Capital Assets*

DOE Order 470.1, Chg 1, *Safeguards and Security Program*

General Information

Purpose

SP-40 does not review budget information to verify that funds are used appropriately or to duplicate the function of internal or external financial auditors. Rather, SP-40 reviews the budget subtopic to determine whether safeguards and security programs have the required level of resources to function effectively. This might involve determining whether budget issues (e.g., a delay in funding) are adversely impacting a planned upgrade.

This section provides an overview and explanation of the budget process as it pertains to PPM inspectors during preparation for and conduct of an inspection.

DOE Budget Formulation

The DOE chief financial officer (CFO) develops and implements appropriate policies and procedures to provide control and assistance for effective management of the Department's finances and related activities. The CFO:

- Assures the financial integrity, formulation, execution, and analysis of the Department's budget
- Develops and maintains an integrated Departmental accounting system with financial reporting and internal controls
- Plans and performs Department-wide reviews to determine compliance with the requirements of the Federal Managers' Financial Integrity Act and Departmental accounting and financial management policy
- Provides required reports that include a description and analysis of the status of financial management in the Department, annual financial statements, audit reports, and internal accounting and administrative control systems.

Of particular interest to the safeguards and security budget process is the formulation and execution of the Departmental budget. There are five distinct phases of the DOE budget process:

1. **Unified field budget call.** The CFO issues a call for field budget requests early in the second quarter of the fiscal year. These field budget requests address the current fiscal year plus two (e.g., the call issued in December 2005 addressed the fiscal year 2008 budget). These field budget requests are submitted to cognizant program offices and become a basis for the programmatic budget requests.

2. **Internal review budget.** The CFO issues an internal review budget call to program offices in the late-second or third quarter of the fiscal year. These budgets also primarily address the current fiscal year plus two; however, data for the current fiscal year and the previously submitted planning fiscal year are included. Each program prepares prioritized budget requests and is responsible for its presentation and defense within DOE. Based on these activities, the CFO prepares a Departmental budget for submission to the Office of Management and Budget (OMB).

3. **OMB budget.** DOE submits a budget to OMB in the fourth quarter. OMB examines the budget request, makes required changes, and passes it back to DOE for review and appeal, as appropriate. DOE then prepares the DOE portion of the President's budget for approval by OMB during the first or early-second quarter of the next fiscal year.

4. **Congressional budget process.** The President submits the budget, and DOE submits Congressional justification in early January. Congress conducts hearings and completes action on the President's budget resolution (nominally by April 15).

5. **Budget execution.** The funds represented by the planning fiscal year data in the President's budget are formally appropriated by Congress during the fourth quarter of the fiscal year to enable DOE to incur expenses against the funds beginning in October. If Congress does not complete the appropriation process for DOE by October, expenditures are usually authorized by one or more continuing resolutions that specify specific time limits and fund constraints.

As this discussion indicates, the data upon which budget execution is based is initially formulated about two and one half years before approval of the appropriation bill that authorizes fund expenditure. Funds are controlled at a macro level by appropriation. A number of Congressional appropriations provide resources to DOE. In no case can funds be moved from one appropriation to another without specific Congressional approval.

During budget formulation and execution, funds within these appropriations are accounted for through budget and reporting (B&R) codes. These codes contain information concerning the Headquarters office that controls the funds. Field and Headquarters expenditure of appropriated funds is authorized against these B&R codes. Fund expenditure for DOE elements is through the approved funding programs. Funds are made available to M&O contractors through work authorizations that specify funds to be expended, B&R codes to be charged, and a statement of work.

For other contractors, funds are usually made available through procurement requests. The contracting officer's representative submits the procurement request to the procurement officer specifying the contract, services to be performed, the estimated cost, and the available funds as designated by B&R code. Procurement determines whether funds are available, whether the services requested are appropriate under the specified contract, and whether all other considerations and constraints are properly addressed. Procurement then formally tasks the contractor to provide the service according to the specific contract involved. Small tasks may be individually contracted through a purchase order using essentially the same procedures. The key point for SP-40 inspectors is that neither DOE entities nor contractors are allowed to expend funds for work not authorized by the control and authorization instruments discussed here.

The DOE Headquarters manager of the funds within a B&R code may change the approved funding programs and, if more than one B&R code is controlled, may move funds from one B&R code to another if no funds are exchanged among different appropriations, appropriation subcategories, or, as discussed below, funding categories. Other controls may be put in place by Congress, OMB, DOE, or other agencies to further restrict flow of funds among projects. The specifics of these funding appropriations might vary on a case-by-case basis.

Funding Categories

Three major funding categories in the DOE budget system are of interest to the SP-40 inspection process: 1) operating expenses, 2) capital equipment, and 3) construction. In most cases, these funds are well defined and cannot be mixed. In a few cases, however, the DOE budget structure requires the use of operating expense funds for capital equipment and construction projects. Such projects include the Environmental Restoration Program, Strategic Petroleum Reserve, and Naval Petroleum Reserves. In general, operating expenses may be used for construction items with a projected useful life of less than two years. Items with a projected useful life of more than two years are funded under construction funds. If the cost of the project exceeds general plant projects (GPP) fund limits, Congressional approval of a budget line item is required.

GPP funds may be either construction or operating expenses funds, if the project cost is under the Congressional limitation for GPP. Field sites often use GPP to fund safeguards and security upgrades because many such items fit under the cost ceiling and GPP can be approved and completed much more quickly than larger construction projects. Note that if the useful life of the item is two years or more, construction funds must be used even though the relatively quick GPP process might be used. If the project cost exceeds the GPP limit, full budget approval for a construction line item is required. Note that line item approval might require several years, even if all levels of management and Congress support the project.

Operations Office Budget Formulation

The field budget process is the formal mechanism through which DOE Headquarters offices obtain uniform operations office input for the budget formulation process. The unified field budget call contains information concerning required submission formats as well as target budget levels and requirements for such special analysis and reporting as crosscut budgets. Field elements request proposed budgets from each facility and laboratory based on the instructions provided in the unified field budget call. Field elements then consolidate the budgets, prepare the required submissions, and forward them directly to appropriate Headquarters offices as directed by the unified field budget call. While the local structure to implement this process may vary, the elements of the process are specified in general terms by the unified field budget call.

Each field element is different with regard to size, programs administered, and number and type of contractors. Regardless of their differences, field elements generally share a common pattern for internal budget formulation. Program representatives within the field element coordinate the activities within their programmatic area, formulate program budgets, and defend these before one or more internal review groups. Safeguards and security budget elements are usually combined with other facility and administrative costs and are addressed at the same level as major programs. Methods for providing budget input depend on organizational placement of the safeguards and security director and the local budget formulation procedures.

The financial section of the operations office usually functions much like the DOE CFO on a local basis by providing budget planning target levels for each program; giving instructions regarding format and required special analyses and reports; and acting as coordinator for preparation of the operations office budget. The operations office manager makes final decisions regarding allocation of funds among competing programs.

Of specific interest to SP-40 inspectors is the method that various levels of field element management use to ensure that safeguards and security items are properly prioritized. Federal managers are responsible for funding and staffing to implement DOE protection programs as well as the other programs under their purview. There should be a documented process by which these responsibilities are given appropriate weight in the operations office budget process. In most cases, the safeguards and security budget will be prioritized within the program of an assistant manager or equivalent, and this program, in turn, will be prioritized within the overall operations office budget. Note that a decision to fund a line item is ultimately made and approved at DOE Headquarters, at the OMB, or even at the Congressional level. The field element only formulates a budget request. The continued involvement of the safeguards and security director or senior managers in achieving Headquarters support for critical projects can be of great importance, even though they have already completed the actions formally required of them by the budget process.

Area office involvement in the formulation of the safeguards and security budget is usually very limited. Ideally, the area office safeguards and security person, section, or branch acts as an advocate for safeguards and security funds as required by the area office and its contractors. At the very least, area office personnel should be aware of safeguards and security requirements within their area of responsibility, and should have developed and communicated a formal position on each to the area office manager, and the affected site(s).

Site Budget Formulation

Typically, research, development, special production, and testing sites are operated by M&O contractors. The contractors operate, maintain, and support DOE-owned and DOE-controlled facilities on a day-to-day management basis.

The roles of the various site contractors in the preparation of the budget are varied. In general, the M&O contractor prepares a budget request for the site and forwards that request to the appropriate field element, where it is consolidated with similar requests from other sites. The M&O contractor is not only responsible to the field element for required budget formulation procedures and submittals, but is also required to provide a great deal of input to Headquarters program offices and other concerned entities.

In most cases, the contractor responsible for operating a particular plant will be responsible for the budget, management, and, perhaps operation of the physical security systems placed within the facility, and for some other aspects of safeguards and security such as MC&A and control of classified matter. In most cases, the site protective force is also supplied by one or more contractors. The protective force may be under contract to the Federal field element directly, may be employees of the operating contractor, may be subcontractors to the operating contractor, or may work under still another arrangement. In any case, the largest portion of the safeguards and security-related expenditure of operating expenses funds at a site will probably be that devoted to providing protective force personnel. The significance of safeguards and security line items varies greatly from site to site, but most large line items throughout the DOE complex unique to safeguards and security have been completed, even though other programmatic line items might not have significant safeguards and security budget interests. For example, the budget for physical security systems in a new building would be included in the budget for the building, but would still involve safeguards and security interest and management.

Within a contractor's budget, the funds to provide safeguards and security services will in general fall within overhead, organizational burden, or distributed costs. In at least one case, the use of protective force personnel for such special projects as checking security credentials at the entrance to classified conferences has been charged to the program as a recharge. It has often been difficult for Federal oversight staff to determine how much money is being allocated or spent by the contractor in meeting safeguards and security requirements.

Budget Execution

A number of concepts should be well understood by an SP-40 inspector. First, two categories of fund obligation authority might be available to a project manager during an execution year: budget authority (BA) and budget outlay (BO). BA is authority provided by law (appropriation, for example) to enter into obligations that will result in immediate or future outlays involving Federal funds. BO is the amount of funds that may be transferred. The distinction is that the annual appropriation bill provides a certain amount of new money that may be used (BA). In addition to that money, additional money might be available from prior years and could be spent during the execution year. Therefore, the total funds available to a project manager is BO, which includes BA, but might be higher than BA.

As the execution year proceeds, funds will fall largely into three categories: 1) funds yet to be formally obligated (unobligated); 2) funds obligated to pay an expense for which no collection has yet been made (obligated, uncosted); and 3) funds already paid out (costed). The reason these categories are important in a safeguards and security context is somewhat complicated. When the budget is formulated, certain portions of project funds are allocated to safeguards and security. An example might be the inclusion of an alarm

system within a new building. If these funds were expected to be spent during the current fiscal year, they would be contained in the current fiscal year safeguards and security budget estimate, and the funds would be contained in the BA for the current fiscal year. Once BA for these funds is approved, they can be spent for any portion of the project, not just the alarm system. The likelihood of BA approval increases if the funds are carried over into the next fiscal year as additional BO. At this point, any documentation indicating that the funds are a "set-aside" dedicated for the alarm system has probably been lost. Many scenarios could evolve from this juncture, but all share the common thread of losing accountability of safeguards and security funds, with potentially significant impacts on achieving or not achieving an appropriate alarm system. Another byproduct is the potential for overstating the safeguards and security crosscut compared to actual expenditures.

Another possible scenario is that the alarm funds in question might remain unobligated at the end of the year. Most M&O contractors are allowed to retain a portion of their unobligated balance as "pre-financing," to allow continuous operation while new fiscal year funds are processed through the financial system. If the hypothetical unobligated alarm funds were assigned to this pre-financing fund, all project identification is lost and new funds would have to be identified to complete the alarm system, apparently increasing the program cost of the system.

Common Deficiencies/ Potential Concerns

Ineffective Safeguards and Security Participation in Budget Formulation

In the typical field element, the safeguards and security director responds to a very specific and restricted call from the financial section charged with preparing and coordinating the budget. In multi-program offices, many elements within the budget process may combine to make the budget allocation and the allocation of staff to the safeguards and security division seem unimportant. In most cases, safeguards and security is a cost-of-doing-business activity. Such activities are likely to be funded at a continuing level or with modest increases during times of plenty and to receive significant scrutiny when funds are being reduced. In many cases, this leads to a funding and staffing allocation defined by default over the past few years. For example, safeguards and security funding and staffing were increased a number of years ago in response to inspection or survey findings without detailed analysis of resource utilization. More recently, the safeguards and security director has often been faced with the need to fully justify his funding and staffing levels without having been involved in their defense or justification in the past. In such cases, the resources to perform required functions might not be forthcoming and the overall status of operations office program management might suffer from a lack of either specific expertise or sufficient numbers of personnel to manage all critical areas.

Failure to Monitor Safeguards and Security Budget Estimate

Most Federal field safeguards and security professionals lack both the financial information and the technical knowledge to effectively monitor funding details. They are usually comfortable with safeguards and security line items, since they are self-contained and well-defined. The costs and status of crosscut items that are imbedded in other line items or in allocated costs are much more difficult to isolate. In many cases, safeguards and security professionals fail to monitor such items. In some cases, the safeguards and security professionals might not review the safeguards and security crosscut for their areas of responsibility during budget formulation or budget execution. In such cases, there can be little assurance that safeguards and security funds are being expended for their intended use.

Inability to Monitor Unobligated and Uncosted Funds

As discussed previously, the status of unobligated and uncosted funds intended to fund safeguards and security expenses should be reviewed by safeguards and security managers. These funds are typically used to smooth the transition between fiscal years and between projects. They can, if properly monitored and managed, greatly assist in maintaining a consistent, cost-effective safeguards and security program. On the other hand, if not carefully managed, they can disappear into other projects, where they provide no benefit to the safeguards and security organizations that originally justified them.

Inability to Analyze Allocated Expenses

For those who monitor safeguards and security programs funded from allocated funds, the ability to determine how safeguards and security costs are allocated and how the identified resources are used are essential to good management. In most cases, the operations office safeguards and security director provides little direct funding of contractor safeguards and security activities. Therefore, information about allocated funding practices and policies is vital to understanding and influencing contractor actions. The directive from the CFO to the operations offices to implement an annual allocated cost budget review is an opportunity to obtain this information. In many cases, operations offices have no procedures for including safeguards and security expertise in this annual review.

Improper Use of Construction Funds

There have been instances of improper GPP usage to fund safeguards and security projects. As discussed above, GPP are construction projects of limited useful life and with a total cost below a congressionally mandated minimum. While operating expenses funds may be used to fund construction projects, GPP or others, with a useful life of less than two years, capital equipment and construction funds may never be used to fund operating expenses. In at least one case, a portion of a security force contract was funded under the guise of GPP using construction funds. This was done to meet a need that exceeded the operating expenses funds available. Severe legal sanctions are mandated for such actions, and discovery by SP-40 inspectors of any such subterfuge must be communicated immediately to SP-40 management.

Planning Activities

During the planning meeting, inspectors identify the safeguards and security budget structure for the field element and/or site to be inspected. This is accomplished by examining the DOE budget and the most recent field budget call. These will establish the appropriations, line items, and major DOE programs involved with site operation. These programmatic funds are the likely source of any funding through allocated costs. In addition, the current year and budget year safeguards and security crosscuts should be examined to develop a picture of total safeguards and security activity at the site. Inspection Took Kit, Tool 4-1, Budget Process Data Collection Questions, in Appendix A, should be initiated at this time.

Interaction with the staff responsible for monitoring the safeguards and security budget estimate will assist the inspection team in confirming that the data gathered from the budget documents is complete and correct. Other personnel should be knowledgeable concerning the status of various aspects of the safeguards and security program at the inspected site, although they are unlikely to know current fund expenditure status. The inspection team should attempt to identify any safeguards and security items or activities that the staff considers under-funded or that remain unfunded and have or could reasonably be expected to have a negative impact on security.

Team discussions with knowledgeable staff in Headquarters program offices with major safeguards and security funding requirements might be useful, depending on whether issues emerge from the discussions above. Close coordination with other topic teams, such as protective force, MC&A, and physical security systems, might result in improved planning and in identification of significant budget issues that might otherwise remain undetected. Similarly, budget issues identified by the PPM team should be fully discussed among the PPM team members and with other affected topic teams to determine the priority to be given to the issue in data collection and the primary responsibilities for data collection and interpretation.

Based on these initial activities, the team should identify key managers and staff at Headquarters and in the field from whom data should be gathered. Major points for discussion with each key staff member concerning his/her budget activities should be identified to ensure that data collection is efficient and complete and to minimize multiple interviews with individuals to obtain similar or related information. Requirements for interviews and data to support the budget process subtopic should be integrated into the PPM team interview and data requirements, as well as other affected topic teams.

During the planning process, inspectors should focus on determining:

- The budget appropriations providing significant safeguards and security funds
- Funding categories involved, e.g., operating expenses or construction
- Funding methods for key safeguards and security activities at the inspected site.

Data Collection Activities

Program Office Interviews

Following the planning activities, the inspection team should have a good general knowledge of safeguards and security funding at the inspected site.

A. Inspectors should interview Headquarters personnel in program offices to determine the degree of involvement and support that safeguards and security receives from the sources of funding.

Office of Safeguards and Security/NNSA Interviews

B. Inspectors should interview staff of the Office of Safeguards and Security or NNSA, as appropriate, to gather general information that might help identify areas that require further investigation. The Inspection Tool Kit, (see Tool 4-1 in Appendix A) has a list of suggested interview questions. Inspectors should conduct interviews with:

- The person responsible for monitoring the site's budget
- The designated point of contact for the site
- The Federal budget point of contact at the appropriate Headquarters element.

Safeguards and Security Managers and Staff

C. Inspectors should interview safeguards and security managers and their staffs at all field levels to determine their knowledge and involvement with the budget formulation and execution process. In most cases, inspectors

should interview the manager who first integrates safeguards and security into other activities to form an integrated budget. In field elements, the safeguards and security director reports to an assistant manager for facilities operation (or similar title) who integrates safeguards and security activities with other site support activities and then defends that unified budget during the budget formulation process. The Inspection Tool Kit (see Tool 4-1 in Appendix A) provides some sample questions.

Integration of Observations by Other Topic Teams

During data collection, other topic teams might identify data points and concerns that are of interest to the PPM team during their review of the budget process. Findings and related indications of inadequacies in the budget or budget process identified by other topic teams are frequently excellent indicators of higher-level management problems. A lack of adequate funding is frequently cited by facilities as the cause for not correcting known deficiencies. Such an alleged lack of funding results from a deficiency in the process for developing the budget, and therefore might be of major interest the PPM team. Or, the alleged problem could be the result of a local management decision on the allocation of available funds among competing safeguards and security functional areas. Consider these types of indications during evaluation of the budget process. Other topic teams must also provide information to the PPM team concerning the validity of claimed funding shortages and the associated impact.

This page intentionally left blank.

Section 5

PROGRAM DIRECTION

Contents

References

DOE Policy 111.1, *Departmental Organization Management System*

DOE Order 470.1, Chg 1, *Safeguards and Security Program*

General Information

The Program Direction subtopic addresses the effectiveness of management's guidance and control in assuring that all required, directed, and assumed objectives and goals are accomplished. Directors and managers at all levels can delegate authority (but not responsibility) to support program implementation. Management must have procedures in place to effectively direct organizational activities using DOE Headquarters and line management policy and procedures to assure efficient implementation of safeguards and security requirements.

This section provides an overview of the activities related to program direction that PPM inspectors could reasonably expect to find.

Line Management Responsibilities

Headquarters has primary responsibility for program and policy development, planning, guidance, and oversight. At the same time, the associate deputy director for field management has responsibility for: strategic planning for all field elements and management coordination and oversight of multi-program operations offices; policy development consistent with assigned functions; and follow-up on contractor employee complaints of reprisal.

Secretarial officers and program officers have primary responsibility to ensure that safeguards and security interests under their jurisdiction are protected in accordance with Departmental requirements. Secretarial officers are respon-

sible for safeguards and security program implementation and oversight by providing program and project direction consistent with safeguards and security directives and policy requirements. They are authorized a safeguards and security staff to accomplish this function.

Contractors provide the overall expertise and resources to effectively implement prescribed goals and objectives. They are the day-to-day operators of the facilities. There may be multiple contractors at sites that have more than one facility. Some facilities have one contractor to provide and manage the protective force, and another to operate the facility. The major effort surrounding protection program implementation occurs at this level.

Either the Federal security manager or the director of an area/site security office is responsible for the typical day-to-day activities to provide oversight of implementation, verification, and reporting of program activities and the management and direction of the onsite Federal staff.

Policy Development and Staff Technical Direction

The Office of Security Policy (SP-60) is the major developer of protection program direction. It develops Headquarters protection program policy, which is then promulgated via DOE orders and other administrative means to management for implementation. Headquarters-level program direction, resolution of security issues, and procedural coordination are the responsibility of SP-60.

Each site office typically has a staff element involved with the operation and implementation of the protection program at facilities within their area of responsibility. This staff element, along with its manager or director of safeguards and security, fulfills protection program responsibilities. Safeguards and security responsibilities assigned in DOE orders to site offices typically dictate a sizable staff element with heavy involvement in the safeguards and security program at this level. Involvement of the area office varies by the type of facility, organizational arrangements, and any local agreements. Again, inspectors must determine the extent and adequacy of this involvement.

The operating contractor's safeguards and security staff should be of a size and influence commensurate with the protection program requirements at that facility. At this level, the program requirements directed from higher echelons are made site-specific and defined in detail. The protective force contractor also responds to the directed program requirements. In both cases, this level of program direction is largely operational and more closely aligned with the detailed management of program implementation and operation, rather than program development and policy formulation.

Directives System

Effective program direction relies on some well-defined method to convey program directives in a timely fashion to everyone who must implement them. Below the formal level of Secretary of Energy notices, DOE notices, and DOE orders, site-specific directives vary widely. However, program direction issued from levels closer to the field can be more important to the offices and personnel who implement the site program. Inspectors must examine the Federal field element and site's directive systems and determine whether an effective system is in place for conveying safeguards and security program direction into site contracts. An effective system:

- Interfaces with and conforms to higher-level directives systems
- Has documentation supporting the system and defining procedures
- Disseminates information and makes it readily available to all who require it
- Includes appropriate coordination, review, and approval procedures

- Provides for handling, accountability, and security when applicable
- Establishes controls to ensure that changes are documented and disseminated in a timely manner
- Is simple and flexible
- Has a standardized and consistent format
- Includes quality control checks.

Common Deficiencies/ Potential Concerns

The potential concerns listed below are based on actual or related experience with organizations similar to those being inspected and similar inspection processes. Although program direction is separated below into three levels of interest (i.e., policy, direction, and implementation), the inspector should remain cognizant of the overlap among levels. Because the major interest is in the effectiveness of direction provided to the program, more potential concerns are listed at the policy level, where the program direction evolves, rather than at the implementation level. This inherent overlap in program direction should be considered during data gathering and analysis.

Policy-Level Concerns

Roles Not Clearly Defined

Specific issues might surface during data collection concerning the responsibilities of staff elements versus the management responsibilities of senior security managers. The issue might surface as a question about the correct level of decision-making capacity, or there might be confusion about where to go for direction, guidance, or decision on a particular type of action. At one site, responsibilities were so fragmented that no member of the security staff could identify the person who was responsible for the survey program. It must be clear who or what office approves deviations to DOE orders. When adequate direction is provided to the safeguards and security program, roles will be clearly defined.

Insufficient Direction from the CSO or Site Office

This problem might run a spectrum from lack of interest, to lack of adequate staff resources, to lack of safeguards and security knowledge and experience. Secretarial officers have primary responsibility to ensure that safeguards and security interests under their jurisdiction are protected in accordance with Departmental requirements. Site offices and program offices may place resources and emphasis on program-mission-oriented tasks in such a way that the support needed to adequately direct the protection program is not provided. Inspectors should look for a direct relationship between the oversight activities of the site office and the actions of the safeguards and security contractor.

Mismatch Between Policy Requirements and Resource Allocations

Historically, the promulgation of new policy, policy changes, and policy interpretations has not adequately considered the resources needed for implementation. As an example, the recent changes in the DBT resulting from the terrorist attacks on September 11, 2001, generated significant increases in both protective force and security systems costs without due consideration of the long-term impact of these changes. In some cases, policies have been developed and promulgated, but not fully implemented due to resource constraints (e.g., the Human Reliability Program [HRP]). Field elements usually have an opportunity to review and comment on new policies before implementation. It is incumbent on the site offices and field elements to determine whether new or revised policies can be implemented with the available resources. If not, it is their responsibility to request additional resources, request an exception, develop and implement an alternative approach, or request that the policy be revised. It is not sufficient for

site offices and field elements to simply ignore policies that they do not have resources to implement. The inspectors should review any mismatches among policy requirements and resources to determine whether the site offices and field elements are proactively resolving them. Program direction that cannot be implemented or that directs resource allocation to the detriment of the overall safeguards and security program is of little practical value.

SSSP Process Not Timely or Coordinated

Inspectors should evaluate the existence or nonexistence of an approved SSSP and the steps taken to achieve and comply with the SSSP process. This topic should be examined at all levels of line management and technical staff, since all levels might be contributing to any perceived problem with SSSP timeliness or coordination. In the absence of an approved SSSP, the inspector should determine what the facility uses as the basis for its safeguards and security program, as well as the root cause of the delinquent SSSP.

Inadequate Safeguards and Security Orders

DOE orders might lack specificity and contain inadequate information to help in directing, planning, organizing, and controlling safeguards and security activities. Such deficiencies in the orders and directives are evident at all levels, including orders issued by Headquarters and operations office supplements. During inspections, SP-40 focuses on the implementation of policy rather than the adequacy of DOE orders issued by Headquarters. However, SP-40 reviews the adequacy of policy during special studies and identifies policy issues when they arise during inspections.

As part of the review of the PPM program direction element, inspectors may review line management's efforts to interpret the general orders and implement the requirements at specific sites. Such line management efforts might include issuing supplemental orders or directives, requesting clarification from Headquarters, documenting site-specific approaches in SSSPs, issuing clarifications and implementing instructions to the affected facilities, and reviewing and approving site-specific plans and procedures. It is incumbent on the Federal oversight staff and contractors to ensure that they are in compliance by proactively seeking clarification of vague policy requirements.

Direction-Level Concerns

Poorly Defined Roles

Frequently, an agreement that specifically outlines protection program roles, responsibilities, and reporting relationships among the Federal field oversight office, the operating contractor, and the protective force contractor either is not completed or fails to adequately address safeguards and security. The contractual arrangement between the field oversight office and contractors prescribes major roles, responsibilities, and reporting relationships. Since the organizational and contract provisions vary among field elements, facilities, and contractors, a specific agreement or memorandum of agreement is necessary to avoid duplication and omissions, and ensure effective program performance. Without such an agreement, personnel responsible for safeguards and security functions might not understand their roles, or required functions might not be assigned.

Inadequate Plans and Procedures

At some sites, plans and procedures providing program direction for site- and situation-specific implementation of orders are outdated or nonexistent. The seriousness of this common problem is determined by the number and extent of outdated or nonexistent plans and procedures. Without adequate written direction, the protection program is likely to deteriorate. To be effective, the program direction provided at

all organizational levels in the form of plans and procedures must be timely, must clarify ambiguous issues, and must be documented. The lack of a formal, documented system for assuring the accuracy, clarity, and currency of program directives is often a root cause of inadequate plans and procedures. Favorable characteristics of a directives system are outlined under "Directives System," above.

Inappropriate Use of Informal Guidance

Informal direction provided as guidance or assistance to the field by higher-level technical staff is sometimes treated as a directive by the field element without adequate further analysis. Field sites undergo a large number of evaluations, staff visits, staff assistance visits, and informal indications of policy changes. In responding to the results of these activities, field organizations may accept and act on these results without further analysis, and in some cases, without appropriate review and approval. If program direction is provided through informal channels rather than the appropriate formal channels, personnel with line management responsibility, accountability, and detailed knowledge might be circumvented and the program direction implemented without adequate analysis or funding.

Inappropriately Distributed Safeguards and Security Directives

New orders, revised orders, directives, clarifications, or interpretations are typically developed by Headquarters and distributed to field elements or site offices for subsequent distribution to the facilities that must implement the requirements. However, in some cases, those directives/guidance are not distributed to the facilities. Facilities that are not aware of the requirements are likely to be out of compliance, or might be expending resources unnecessarily. More frequently, the directives/guidance are provided to some elements of an organization but are not distributed to all the affected elements, so that some portions of an organization are operating according to outdated or incomplete guidance.

Inadequate Direction for Security Functions Not Directly Related to Protection of Special Nuclear Material

Some security functions, such as TSCM, OPSEC, and unclassified computer security, are perceived as having lower priority than functions directly related to protection of SNM (e.g., protective force or MC&A). Accordingly, these "lower priority" functions receive a lower level of attention, and little or no direction is provided to the managers responsible for their implementation. As a result, those programs frequently are not implemented or are not fully functional.

Implementation-Level Concerns

Outdated Implementation Procedures

As discussed previously, when procedures are not updated in accordance with revised plans, the safeguards and security administrative system cannot keep pace with plan revisions, administrative changes, and operational changes. This concern specifically includes security police officer orders and procedures.

Inadequate Administrative Documentation

Administrative manuals and guides essential for efficient day-to-day operations and institutional memory may be nonexistent or outdated. This is a particular problem when frequent reorganization of security staffs results in outdated organization charts, organization and functions manuals, standard operating procedures, and other administrative direction guides and aids that personnel need for day-to-day work. Inadequate documentation might indicate poor management direction due to frequent and non-decisive reorganizations.

Other common causes of inadequate documentation are a lack of staff personnel resources or expertise and faulty assignment of priorities. The greater the staff turbulence, the greater the absolute need for adequate administrative program documentation.

Excessive Reliance on Deviations

Inspected elements might concentrate on gaining deviations to DOE orders rather than on how to comply with the direction. Sometimes, when a site cannot meet requirements, it attempts to use the deviation process to lower the requirement. In some cases, the deviations may be "in process" for an extended period of time, while the facility operates as if it has already been approved. During preparation for SP-40 or operations office reviews, facilities often conduct their own compliance inspections and often "solve" the identified noncompliance issues by requesting deviations. This is sometimes erroneously considered an acceptable method of passing an SP-40 inspection.

Planning Activities

During the planning meeting, inspectors identify how organizational elements provide program direction to the safeguards and security program. They also determine the involved site offices and other program offices for the inspected facility. The following documents from each of the organizational levels involved in the inspection should be reviewed:

- Site Safeguards and Security Plan
- Administrative procedures
- Facility/office guidelines and procedures
- Supplements or other elaboration of Departmental policy
- Organization diagrams
- Organization and functions manual(s)
- Mission statement
- Any agreements and memoranda of agreement affecting program direction
- Protection program budget and budget development guidance
- Organization- and staffing-related policy and procedures
- List of approved and pending deviations
- Documents related to assignment of responsibility and accountability.

During the document review, inspectors should identify the facilities and Headquarters elements deemed necessary to visit for data collection purposes and any unique points of contact required to characterize the program direction environment. Interviews with points of contact should provide the following information:

- Types of documents used to provide program direction in functional areas other than safeguards and security
- The documented safeguards and security-related program direction
- Procedures used for obtaining exceptions
- Approved exceptions to requirements and associated compliance schedule agreements
- Status of SSSP and related planning documents
- Organizational alignments, responsibilities, and accountability from top to bottom, with emphasis on where the safeguards and security function is assigned.

Data Collection Activities

Management Interviews

A. The Inspection Tool Kit (see Tool 5-1, Program Direction General Data Collection Questions, and Tool 5-2, Program Direction Specific Data Collection Questions, in Appendix A) provides suggested general questions for initiating program direction related interviews, particularly at the top management positions. Responses to these general questions help the inspector form an impression of the overall safeguards and security program and obtain leads for further investigation, in addition to providing information concerning the narrow topic of program direction. The interviews should attempt to answer basic questions:

- Is the program implemented in accordance with DOE policy and direction?
- Is there evidence of active program direction by each level of the organization?
- Is the program direction documented accurately and to a degree that it provides long-term direction to the protection program?
- Does program administration support program direction?

Case Studies

B. Inspectors should use a recently issued DOE order or notice and trace the Federal site office's activities that led to implementation by the contractor. Policy documents may be used for examples if they contain specific requirements that must be met by line management. Inspectors should determine what actions the site office took upon receipt of the order and specifically what direction was provided to the field for policy implementation.

C. Inspectors should determine the extent and effectiveness of interaction between the site safeguards and security staff and contractor to determine whether the relationship is one of cooperation, particularly in policy development, and whether the roles and responsibilities are clearly delineated and understood by both parties.

Document Review: Field Element

D. Inspectors should review documentation that prescribes the administrative system for the receipt, control, and distribution of directive materials. Inspectors should determine whether the administrative processes and document review responsibilities are clearly defined, formally documented, communicated, and understood. An efficient document review system allows for timely changes; it does not obstruct changes and cause a significant lag in documenting locally developed policy and procedures. Inspectors should also determine how the field element process worked using the orders or notices selected for review as examples.

E. Inspectors should review any agreements, memoranda of agreement, or similar documents that outline protection program roles, responsibilities, and reporting relationships between the operations office, the operating contractor, and the protective force contractor. In the absence of such agreements, inspectors should determine whether there are frequent internal disputes or confusion between contractors on which one is responsible for tasks that are in a fringe area of the contracts. Protective force performance testing is an example. Are the performance tests required by the orders and local directives to be run by the protective force contractor or the M&O safeguards and security staff? If run by the M&O staff, inspectors should examine the delineation of the coordination required with the

protective force contractors, and their level of participation. Also, inspectors should determine who is responsible for writing the performance test plan, and which safety officer is responsible for approving the plan.

F. Inspectors should review procedures for identifying the need for a deviation (i.e., variance, waiver, exception), and the process followed to request the deviation once identified and determine whether the deviation process is being used appropriately. Inspectors should examine the timeliness of approved deviations by comparing the date of the originating office's request for deviation to the date approved. Different deviations and the time required for approval at the various echelons of the organization should be examined to determine any pattern of slow response to requests. Inspectors should determine whether any of the deviations have been "in process" for an excessive period of time and, if so, the reason for the delay and any impact on the protection program.

Document Review: Site Contractor

G. Inspectors should review the administrative procedures and related documentation used to translate program direction of any form into the lowest level of documentation required for full implementation. Specifically, inspectors should examine the actions taken at this level for full implementation of the DOE orders or notices selected for this review. Inspectors should pay particular attention to the coordination effort with the operations and other non-safeguards and security elements, as well as the approval level required by the administrative procedures for various types of actions.

H. Inspectors should review documentation that prescribes the administrative system for the receipt, control, and distribution of directive materials and determine whether the processes and responsibilities are clearly defined, formally documented, communicated, understood, and adhered to. Inspectors should determine whether the system will support timely changes rather than obstructing change and causing a significant lag in documenting locally developed policy and procedure changes.

I. Inspectors should determine the level of interaction among the M&O contractor safeguards and security staff, the protective force, and the operations office safeguards and security element. For relationships to be productive, clearly delineated roles and responsibilities must be understood by all parties. If there is a productive relationship, the operations office and site contractor will perceive similar quality in their interactions.

J. Inspectors should determine whether there are any ongoing actions related to the SSSP, and the impact the potential changes would have on implementation of the plan. Inspectors should verify that adequate direction exists for producing or changing the SSSP and review the development and approval history of the SSSP process, with emphasis on timeliness. Inspectors should also expand the investigation of any event that may have contributed to a delay or non-provision of significant direction for the safeguards and security program. Because SSSP actions are usually accomplished at this level, inspectors should determine the adequacy of the direction and guidance provided to the SSSP process by interviewing the personnel who do the work.

Observations by Other Topic Teams

During data collection, other topic teams may identify data points and concerns that are of interest to the PPM team. Findings and related indications developed by other topic teams are frequently excellent indicators of higher-level management problems. For example, one performance indicator tied to award fees might

be the timely submission of CAPs for self-assessment and survey program findings. One program with this type of performance award fee changed the nomenclature of discovered problems by calling them "observations" instead of findings and thus avoided the requirement to create CAPs. Since this action eliminated "findings," there were never any delinquent CAPs. Therefore this section of the contract award fee was always perfect by default. These indications should be considered by the PPM team for applicability to the evaluation of program direction.

This page intentionally left blank.

Section 6

CONTROL SYSTEMS

Contents

References

DOE Order 470.1, Chg 1, *Safeguards and Security Program*

DOE Order 471.2A, *Information Security Program*

DOE Order 470.2B, *Independent Oversight and Performance Assurance Program*

DOE *Self-Assessment Kit*

General Information

A subsystem of safeguards and security management provides control systems for

safeguards and security activities through surveys, inspections, self-evaluations/ assessments, reporting, and corrective action. For inspection purposes, control systems are the organizational and procedural measures implemented by Departmental and contractor management to evaluate and enhance a protection program in accordance with DOE Headquarters and line management policies and procedures. Safeguards and security management includes those personnel and offices at all DOE/NNSA and contractor levels of organization that are assigned responsibilities for managing and implementing the protection program.

Self-Assessment Planning

Inspectors should first determine whether an approved self-assessment program is in place at each safeguards and security organizational level and whether management has published self-assessment guidance. Inspectors should review the guidance and/or plan to determine whether it contains adequate instructions and procedures for assessing all aspects of the protection program. Inspectors should then coordinate with other topic teams that normally assess implementation of a self-assessment program in their respective areas for both Federal oversight staff and contractors.

Self-Assessments

A self-assessment program is a management control system with major objectives to establish accountability and excellence at the grassroots level, thereby involving people who are the most familiar with the processes being assessed and their management. Self-assessment is a continual line management activity that acquires, assimilates, documents, and reports through all levels of an organization on the effectiveness, adequacy, efficiency, and economy of its activities. Inspected facilities are expected to implement a self-assessment program that provides coverage for all elements of the protection program. Additionally, some of the elements of the safeguards and security program (e.g., classified matter protection and control and MC&A) are expected to have program-specific self-assessments. The effectiveness of the program at all levels is of significant importance to the PPM topic team.

Internal Oversight

Managers may establish their own internal self-directed control measures based on the size, complexity, and mission of the organization. These measures span a spectrum from the assignment of ad hoc, informal, and part-time responsibilities to the establishment of an office with full-time staffing and a prescribed mission of quality control, organizational development, total quality management, internal review, or other related functions. Included in this category of oversight are the normal reporting systems inherent in line management operations. The PPM topic team should become aware of these measures and determine their effectiveness as control systems.

Survey Program

The survey program is a major topical area for SP-40 inspections; the PPM topic team evaluates the detailed implementation of the program and how effectively line managers use the information developed by this control system.

DOE Order 470.1 prescribes requirements for the conduct of surveys. This program is a primary control system by which DOE/NNSA line management approves facilities for the handling and storage of safeguards and security interests on site, and actively monitors the continuing status of safeguards and security. Survey reports are distributed to all organizations with a registered activity at the surveyed facility and to applicable Headquarters elements.

Performance Assurance Program

Facilities with the requirement to protect Category I and/or Category II quantities that roll up to the Category I-level of SNM and Top Secret matter are required to implement a program that assures the performance of critical safeguards and security systems. These safeguards and security systems are essential components (e.g., equipment, hardware, administrative procedures, protective forces, personnel) that are used to protect these materials. The performance assurance program evaluates the operability and effectiveness of these systems. Unsatisfactory results must be addressed in site CAPs.

Performance assurance program tests help ensure that the information used in VAs is accurate and reliable. The results of these tests determine the effectiveness of the essential safeguards and security elements identified within the physical security systems, protective force, and MC&A programs. It is most important for these programs to determine whether a performance assurance program exists and whether the site has developed a critical protection element (CPE) list. Finally, the PPM team is very interested in the ability of the tests run under a performance assurance program to measure the effectiveness of the protection element. The PPM team should be providing the other topical teams with both the information regarding the elements that should be candidate CPEs and the specific type of performance that is needed in order to validate VA data inputs.

Award Fee Determination Plan

The purpose of a contract award fee is to motivate the contractor to achieve optimum performance by providing the opportunity to earn an increased fee. Award fees to contractors are determined by various site-specific and comprehensive evaluations of contractor performance. As part of the contract, a performance evaluation plan is developed to specify performance objectives, assign weights to objectives, specify the organizational responsibilities for evaluating performance, and specify the evaluation procedures to be followed.

Feedback developed as part of the award fee procedure might serve as a supplementary management tool for determining the progress of programs and identifying problem areas. The PPM topic team should determine whether management is making appropriate use of this information.

Corrective Action Plan Program

Subsystems and processes used by management to develop and track corrective action on identified issues are as important as the control systems used to initially identify issues. It is essential to have an effective system for developing and tracking critical issues until they are resolved. The corrective action process includes an analysis of the root cause of identified deficiencies, the development of actions to address the deficiency, the assignment of responsibility for completion of corrective action, and a trend analysis of results. This tracking system normally records the status of actions, provides for periodic updating, and follows procedures designed to assure that recorded results are reviewed and acted upon by a level of management that has the resources and authority to correct the issue.

Locally Developed Control Systems

Various reporting and information systems might have a secondary use as a control system. Such systems can provide significant additional information to management with only a minimum expenditure of additional effort. Types of activities and reports that could contribute to an effective control system include management walk-downs, budget program reviews, reports of security infractions, personnel status reports, the SSSP development process, and personal observations.

Common Deficiencies/Potential Concerns

Vague or Ineffective Self-Assessment Plans

Some program offices and most field elements develop self-assessment programs. Often, procedures or plans to implement the program are incomplete, with only vague descriptions of the tasks and functional elements to be assessed. Procedures and performance-oriented criteria are frequently absent. In addition, requirements for CAPs, trend analyses, identification of root causes for findings, and tracking are either vague or not included. From time to time, programs will attempt to circumvent CAP development and other requirements by labeling findings as "observations," "concerns," or some term other than "finding." Often, corrective action is still taken, but it is spurious, undocumented, and without appropriate causal analysis or tracking. These deficiencies are also common to contractor organizations.

Inadequate Corrective Action Plans

Organizations frequently fail to effectively accomplish one or more of the following actions: 1) prioritize deficiencies so that resources can be used to correct the most serious ones first; 2) establish a corrective action schedule with milestones so that progress can be monitored and schedule slippage identified early; 3) assign responsibility for completion to specific organizations and individuals; 4) continually update the plan as known deficiencies are corrected and new ones are identified; 5) ensure that adequate resources are applied to correcting deficiencies; and 6) conduct root cause analysis or trending for identified deficiencies. Frequently, managers devote their resources to correcting the most recently identified deficiency instead of the most serious ones.

Inadequate Self-Assessments

Self-assessments can be an important element of safeguards and security programs, but they are not always fully and effectively implemented. As a result, self-assessments may not be thorough. Also, because revising the organizational structure or staffing levels is sensitive for managers, supervisors, and personnel, self-assessments rarely recommend eliminating jobs or combining functions in the interest of efficiency. Inspectors should not limit themselves to a review of only self-assessments as they examine the control systems. Sites often develop additional feedback/control systems to address the adequacy of organization and staffing, provide feedback to the manager, and mitigate deficiencies in the self-assessment program. For example, in addition to the self-assessment program, one site had mandatory "management walk-downs" during which mid- and senior-level managers were given specific topics to evaluate depending on what the area senior site managers felt needed emphasis. At another site, a quality control branch was tasked with providing assessments of specific processes and programs based on locally developed metrics.

Ineffectively Implemented Self-Assessment and Survey Programs

Self-assessment and survey programs within the Department vary substantially. The following problems in the implementation of self-assessments have been observed:

- The assessments and surveys vary significantly in depth of coverage; many do not include adequate performance testing. This is often because insufficient resources have been made available to successfully implement these programs.

- Personnel performing the self-assessment or survey generally focus on their specific area of responsibility without considering the impact of closely related functions.

- Self-assessment and survey reports do not support the conclusions reached.

- CAPs generated as a result of a self-assessment or survey fail to identify applicable causal factors and/or fail to include actions that will address the identified deficiency.

- Deficiencies found during self-assessments and surveys are not always characterized as findings and therefore no corrective action takes place.

- Results of previous inspections, surveys, or assessments are not used when conducting self-assessments and surveys to ensure that similar deficiencies do not exist.

- Personnel assigned responsibility to conduct self-assessments and surveys do not have the background or expertise to effectively evaluate program status.

Ineffective Survey Programs

The purpose of the survey program is to grant facility approval before permitting safeguards and security interests on the premises and to determine the status of facilities with safeguards and security interests. The survey program develops information that may be used for other purposes as well, and also provides an interface between the surveying office and surveyed sites. In many cases, this is the only onsite interface. The survey program should be examined by management to ensure that program capabilities are used to the best advantage.

Management may have delegated responsibility for the survey program to a level where the prescribed program may be effectively run, but the results do not reach the level of supervision or management necessary to make optimum use of the information available through the survey program. Survey programs often become routine within an organization and require revitalization. A system for informing top managers of survey results from which they can extract performance and management indicators is needed if the survey program goals are to be met. Additionally, all levels of line management above the survey team organization may use the survey team's capabilities and results to enhance management. Efficient managers do not develop control systems that duplicate the capability of the survey program.

Unsupportive Award Fee Processes

A primary means for adding emphasis to a program and to ensure a high state of security awareness and performance by contractors is to motivate the contractor through the award fee process. There is no prescribed formula for granting award fees; however, the process may shortchange or even omit safeguards and security. Without such emphasis, the safeguards and security program suffers when priority is placed on operational and other administrative programs that typically have more visibility to management. An award fee allocated to safeguards and security is an extremely effective control measure, and the information gathered for the award fee process may be used for other elements of management.

When granted, award fees should be clearly correlated with specific indicators of good contractor performance. Significant disparity between award fees and performance indicates a need for further investigation to determine the cause for the disparity.

Reactive Organizational Oversight

In the absence of internal control programs, line managers are forced to constantly react to external findings and associated impacts on how safeguards and security resources are used. A program will not be effective unless line organizations take a proactive approach by critically examining their effectiveness; identifying strengths and weaknesses; determining root causes for weaknesses; and designing, implementing, and evaluating the

effectiveness of programs. All such actions are designed to correct weaknesses while maximizing strengths and have the objective of achieving change through informed management. Adequate control subsystems are required to keep management informed.

Planning Activities

During planning, inspectors identify the control systems used at all echelons of management. The program office(s) and secretarial officers primarily involved with the inspected facility or office should be identified. This information will help establish priorities and task assignments to team members.

Data Collection Activities

Oversight Records

A. Inspectors should review the following documents from each involved organizational level:

- SSSPs
- Organization and functions manual(s)
- Mission statement
- Procedures for CAPs
- Self-assessment program plan and procedures
- Survey program procedures
- Performance assurance program plans
- Award fee determination plan.

B. During this review, inspectors should identify which facilities and Headquarters elements to visit for data collection. Inspectors should obtain the following information and identify points of contact to interview during the onsite phase of the inspection:

- Formal control systems that are in effect at each level of management
- Informal control systems that are not necessarily institutionalized but are relied upon as a control measure
- Internal self-directed oversight and control measures.

C. Inspectors should review the SP-40 files containing inspection or assessment reports conducted during the past three years that affect the operations of the inspected facility. Inspectors should identify reports, such as from the General Accounting Office and the DOE Office of the Inspector General and review as appropriate.

D. From the review of these reports, inspectors should identify the findings/issues that should have been addressed and resolved by one or more levels of management. At each appropriate level of line management, inspectors should check management's actions to assure that all issues were entered into a tracking system, tracked to resolution, and appropriately documented if not resolved. By examining the distribution of these types of reports, inspectors can determine whether they are reviewed by site personnel who are responsible and accountable for solving issues identified in the external reports. Inspectors should also determine what offices reviewed the SP-40 reports and specifically what office(s) acted upon the identified issues. Inspectors should check for a CAP tracking system; if there is none, then determine why and investigate further as a potential finding.

Corrective Action Plans

Good management practice and DOE directives mandate a system by which findings/major issues are corrected and tracked to resolution.

E. Inspectors should review system effectiveness by following an issue from identification to resolution by selecting findings from previous SP-40 surveys and self-assessment reports. By tracking these findings in the system, inspectors can determine whether: 1) identified corrective actions are supported by causal analysis; 2) corrective actions address the identified deficiency; 3) milestones for completion appear to be appropriate; 4) someone was assigned responsibility for implementation of the corrective action; 5) the corrective actions are entered into a tracking system that allows for monitoring status; and 6) the corrective actions are tracked until validation of completion.

F. There is no prescribed system and no direction that an issue-tracking system must be automated. However, an effective manager will take advantage of automation and at a minimum include the elements outlined above. Inspectors should also review the interface between the system being reviewed and the SSIMS. Inspectors can expect to find compatibility among the systems, matching information on tracking data, and maximum integration and use of the SSIMS capability. If the essential features of a critical issue tracking system are not present, or if there are significant omissions or inaccuracies, inspectors should also investigate the topic in greater detail as a potential finding.

Self-Assessment Program

G. Inspectors should evaluate the overall self-assessment program to determine how results of the program are being used to enhance the safeguards and security program. Inspectors should recognize that self-assessment programs might not be dedicated to safeguards and security functions and that integration of safeguards and security with other functional area self-assessment programs is normal and expected.

The self-assessment function is sometimes integrated with other quality management programs. Inspectors should identify the offices and staff with responsibility for the function, and gain an understanding of the program at each level being inspected. Inspectors should also determine the effectiveness of the program by conducting interviews and examining the reports produced by the self-assessment system. These reports to safeguards and security management may be used as a control system to measure the effectiveness of the self-assessment program.

A formal part of the self-assessment program is the tracking and reporting system to ensure that corrective actions are addressed in a timely manner and to provide line managers with current, accurate, and consistent information. Inspectors should include a description of the tracking system in the program implementation plan.

Survey Program

H. The survey program is a prime source of information available to managers. Inspectors should determine whether the survey program is comprehensive, whether it includes assurance of compliance and performance testing, and whether the information developed by the survey program is used effectively by managers. By reviewing the survey program policy and procedures, inspectors can determine the size of the program, the flow of survey results, and the completeness and distribution of reports. Inspectors should expect to find reports approved and monitored at a level that assures management attention to the overall program, as well as to the details of the report.

I. Inspectors should interview survey personnel to determine whether they have been adequately trained or possess the necessary knowledge to perform surveys. By interviewing line managers, inspectors can determine whether management collects and uses the information and knowledge they have accumulated as a result of their repeated onsite presence and inspections of facilities.

Internal Oversight

J. Inspectors can determine by interview and document review whether other internal control measures (in addition to self-assessments, which are discussed in activity "C," above) have been established by management at each organizational level and determine the interfaces among these elements. Inspectors should also check for the training, qualifications, and experience of personnel assigned the task of contributing to internal oversight of the safeguards and security program. Inspectors may obtain this information through interviews and a review of the results, rather than by examining personnel records.

K. Inspectors should check for duplication of effort and for appropriate interfaces between internal and external control and feedback systems. For example, if the self-assessment and survey programs are capable of providing the manager with the required information, other internal oversight measures might not be necessary. The most effective manager will make maximum use of the information provided by mandatory programs and meet any unfulfilled local requirements by supplementing the mandatory programs with internal assignments. As with other control systems, tracking and reporting systems must ensure that corrective actions are addressed in a timely manner and provide managers with current, accurate, and consistent feedback information.

Award Fee Determination Plan

L. Inspectors can determine whether a cost-plus award fee contract exists for the M&O contractor and the protective force contractor. Inspectors should also determine contractor progress toward achievement of the objectives. Inspectors should examine the award fee determination plan(s) for safeguards and security objectives, performance indicators, and measurement methodology, and focus on these facets of the plan and its implementation:

- Does the allocation of objectives and award fee percentages appear sound and reflect adequate support for the safeguards and security program?
- Is the evaluation of contract performance (used to determine the aware fee) consistent with the results of other evaluations, inspections, or performance indicators?
- Is the information that is used to determine the objectives and measure contractor progress also used by the manager as control system feedback?

Locally Developed Control Systems

M. Through interviews and review of the subsystems already examined, inspectors should check to see whether there are other subsystems that provide information on a regular basis that could be used in the control system. Inspectors should also determine whether the manager has consolidated the information from all sources to achieve a complete understanding of the status of safeguards and security.

Impact of Deficient Corrective Action Process

N. If the essential features of a corrective action process are not present, or if there are significant omissions or inaccuracies, the inspection team should address the topic in greater detail to determine the impact on the security program. Potential impacts are:

- Deficiencies identified but not corrected
- Management not aware of status of individual findings
- Magnitude of deficiencies unknown
- Trend analysis not conducted
- Root cause analysis not conducted.

Potential root causes are:

- Inadequate management emphasis and direction
- Poor program design
- Poor program implementation
- Lack of program documentation
- Inadequate staffing and/or training.

Award Fee Percentage

O. There is no minimum standard or "correct" percentage of an award fee that should be allocated to safeguards and security. SP-40 field experience suggests that between 1 to 10 percent of an award fee for M&O contractors is generally allocated to safeguards and security. If the safeguards and security award fee appears to be inadequate, inspectors should question the management personnel (including security, contracts, and the DOE/NNSA manager) to determine the rationale for the allocation. Because of the subjectivity of the decision, inspectors should also determine whether safeguards and security was adequately represented during the allocation process to assure that the control system is effective for safeguards and security. Inspectors should consider these frequently cited factors in determining the allocation percentage:

- History of safeguards and security performance by contractor
- Need for emphasis on safeguards and security as determined by the operations/site office
- Adequacy of other control measures to assure performance
- Safeguards and security budget compared to total budget.

Observations by Other Topic Teams

During data collection, other topic teams might identify data points and concerns that are of interest to the PPM team. Findings and related indications developed by other topic teams are frequently excellent indicators of higher-level management problems. These indications should be considered by the PPM team for applicability because SP-40 experience indicates that the integration of other topic team observations is especially applicable to the control systems subtopic.

Other topic teams are an essential and excellent source of information for determining the root cause for the lack of an effective corrective action process. Other SP-40 topic teams checking to determine the status of findings and corrective actions in their topic areas also can provide valuable data. This information, along with that already gathered by the PPM topic team, will normally be sufficient to determine a root cause for the problem and to identify the impact of a deficient corrective action process.

For example, the root cause of major deficiencies identified by the other topic teams is frequently a failure of some element of the control system. Either the control systems in effect at the site failed to detect the deficiencies or the corrective action system failed to identify the problem to management at the level necessary to ensure correction. Conversely, when the PPM team evaluates the observations by other topic teams for impact on PPM, it might find that adequate control systems are in place, but that other factors (e.g., non-availability of resources, human error, management's judgment) might have been the cause of the problem.

When problems indicating a potential control system deficiency are discovered by another topic team, it is essential that the PPM team coordinate with the other teams to obtain their observations on the effectiveness of the management control systems. If the control systems at the PPM level are the problem, they will typically be evident in more than one topic.

This page intentionally left blank.

Section 7

INTEGRATION

Contents

Integration

Integration is the coordination and interface among inspection team members to achieve a more accurate, effective, and organized inspection effort. Integration is possibly the most important and productive inspection activity. This is particularly true for the PPM topic. Thorough integration creates a synergism and enhances the quality and validity of the SP-40 inspection report. This combines with other unique attributes to strengthen the overall SP-40 capacity to provide significant, value-added contributions to the safeguards and security community, as well as to DOE as a whole.

To take into account the interdependency of elements of the overall protection program, the integration process among topic teams must continue throughout all SP-40 inspection phases to ensure that all pertinent inspection data has been shared. This integration is simply an exchange of information by different topic teams and an accompanying discussion of how information developed by one topic team influences the analysis of the performance observed in another topic area.

From the topic team point of view, there are three major objectives of integration. The first objective is to allow topic teams to align their efforts so that their activities complement rather than detract from one another. Whereas other topic teams typically review management of the topic area, PPM examines management's performance in integrating and directing all subsystems into an effective and viable protection program. This parallel inspection of closely related areas by two teams must be coordinated to preclude duplicate data-gathering efforts and data not being gathered because one team assumed the other was collecting that information. Early and continuing integration helps ensure that the activities of all topic teams are unified and contribute to the overall goal.

A second objective of integration is to allow topic teams to benefit from the knowledge, experience, and efforts of other topic teams. For example, the personnel security team might conclude that the inspected personnel section does not have enough resources to get the job done. By inspecting the safeguards and security budget and organization and staffing subtopics for the operations office,

the PPM topic team might be aware of such issues as management's longstanding, but unsuccessful, request for additional resources for the personnel security function. It might therefore be productive for the personnel security team to shift emphasis to other areas within the topic because PPM data collection would include this aspect of the situation. Because of this integration between teams, the root cause of a personnel security problem partially shifts to a PPM topic issue.

The third objective of integration is to prevent topic teams from interfering with each other. This is of particular importance to the PPM team. Integration among topic teams can preclude this problem by having one or two topic teams visit a particular location and collect the data for several teams. All topic teams should be aware of what other topic teams are doing, where they are doing it, and how it will affect their own activities.

Integration with Other Topic Teams

The very nature of the PPM topic mandates total integration with *all* topic teams. PPM includes the higher-level management aspects of each topic area. It drives the overall security program and is accountable for everything the program does or fails to do. For these reasons, PPM cannot be inspected in isolation.

Planning Phase

Throughout the planning meeting, the PPM team must integrate its planned activities with other topic teams. Document reviews and interviews conducted as part of the inspection planning process might suggest specific lines of inquiry for both PPM and the other project teams. As an example, a preliminary review of the VA data might result in questions regarding the effectiveness of specific protective force functions. The PPM team should provide the data to the protective force team and request special attention to this function during the inspection. Similarly, a review of recent Headquarters guidance documents, coupled with interviews with Headquarters personnel, might raise questions regarding the level of implementation. These questions should be relayed to the appropriate teams for further investigation.

Conduct Phase

Throughout the conduct phase of the inspection, the PPM team should discuss findings and issues during the daily inspection management update meetings. PPM should be listening for issues and findings from the other topic teams that might indicate PPM-related problems. As an example, if the protective force reports a potentially excessive amount of scheduled overtime being worked by the security police officers, this might indicate a failure to obtain a sufficient budget for program operations. Discussions should facilitate the topic team interface effort by assuring that all PPM-related issues are appropriately identified.

Closure Phase

It is imperative that issues involving several topic teams be resolved, that impacts be clearly understood, and that a preliminary decision be made as to how and by whom the issue will be reported. This PPM topic interface must be timely and effective. The report writing and rating determination for PPM is based on data collected by the PPM team as well as selected validated facets of other topics having an impact on the PPM area. Thorough coordination among teams should assure that all observations the team desires to report are recorded, and that unintentional duplicative reporting does not occur.

Integration of PPM Subtopic Areas

The PPM subtopics are closely related and practically inseparable. Each subsystem of the management program is important to all others. Thus, data collected for one subtopic typically will include data applicable to one or more other subtopics, and data sharing will be more effective between certain subtopics. For example:

- The **planning** process is closely tied to program direction, control, budget, and organization and staffing. In fact, planning is the basis for action in each of the other areas. For example, the budget process must support the results of the planning effort, and planning is directly affected by the budget.

- The quality of **organization and staffing** can affect all other elements of PPM. Without an effective organizational structure and adequate staffing, the effectiveness of the other protection program topics might be diminished.

- The results of the **budget process** determine the ultimate resource allocation for the protection program. Ineffective management involvement in the budget process (e.g., PPM weaknesses in formulation and execution) might seriously degrade the effectiveness of planning, direction, and control actions.

- PPM control systems are a major factor in determining whether the system of promulgating **program direction** is effective, or whether the direction is in fact inadequate or incorrect.

- Adequate **control systems** provide management with sufficient and correct information for decision-making. Planning, organization and staffing, and budgeting processes are all dependent upon feedback about the current operating environment and the status of actions required to change the work environment. Program direction provided to the line and staff is directly related to feedback developed through control systems.

Planning Process

Normally, inspection teams in other topic areas evaluate plans and procedures pertaining to their topics as part of their data-gathering efforts. The PPM team should coordinate the evaluation of topic-specific plans and procedures with the other teams to ensure that a sufficient number of plans are examined. Specific planning findings from the topic teams should be aggregated on a programmatic level if they are to be reported as PPM planning findings.

Organization and Staffing

The organization and staffing PPM subtopic affects each topic team because management determines the organizational structure and the allocation of personnel resources to functions within the organization. How well the mission for each topic area is performed might be directly or indirectly related to management actions concerning organization and staffing of the function. Issues that frequently require coordination often involve lines of authority and responsibility for a function as determined and implemented by management. The results of data collection for other PPM subtopics will contribute significantly to the data collection requirements of the organization and staffing subtopic.

Budget Process

The PPM team should coordinate with all other topic teams, providing them with data on significant budgetary issues and soliciting budgetary indicators that they might have observed in their respective topic areas. Two hypothetical examples of such information exchange follow.

Hypothetical Example #1:

In inspecting the protective force topic at Site X, a major issue surfaced involving the provision of temporary security inspectors to replace those who were out on strike during the timeframe XXX - YYY. There was much criticism of the qualifications and training of the replacements, the procedures used to obtain them, and the effect of these shortcomings on the eventual contract settlement. During the investigation, the protective force team attempted to discover the source of funds used to pay the temporary replacements. No one in the security branch seemed to know. All they knew was that,

"Finance took care of it." Preliminary coordination with the PPM budget inspector revealed no obvious cost element. Subsequent investigation revealed that construction funds were used as a GPP item "with anticipated lifetime of less than two years," which eliminated many of the normal construction fund controls. While this had no impact on the protective force topic, it did reveal a management problem.

Hypothetical Example #2:

In inspecting physical security systems at Site Y, inspectors found that an updated alarm system installation was underway. While the old system had demonstrated weaknesses, management had formally accepted the increased risk in the interim through the SSSP. In the SSSP, the alarm system was projected to be complete by the end of the current fiscal year. Discussion with the PPM topic team revealed that no funds for alarm system procurement and installation had been programmed for the current year or for the next two years. Instead, the current activity had been funded with an uncosted balance from the previous fiscal year and those funds were now expended. It therefore became clear that the alarm system installation would not occur on time, the risk accepted by management would continue longer than anticipated, and management at some level was not supporting commitments made in the SSSP. Thus, a much more intense examination of compensatory measures was required and a potential management issue was identified.

Program Direction

The PPM team should be made aware if inadequate direction is being provided to topic areas so as to identify any trends toward a systemic issue concerning program direction. Conversely, other teams should be made aware of PPM issues that affect their areas of interest. All topic teams are affected by the system used for providing program direction. The PPM team should solicit an opinion from each team on how well the system is working in its topic area.

Control Systems

Inspection teams for each inspection topic area must determine and evaluate the control system(s) in effect for their topic. If any topic team finds that its control systems are inadequate to the overall evaluation of control systems, topic teams should examine their topic control systems at the input level while the PPM topic team should check on how the information is used thereafter.

By communicating topic team observations among topic teams and the PPM team, a pattern of deficiencies might be identified in more than one topic area, and thus be indicative of a systemic control system problem at the PPM topic level. Coordination among topic teams prevents soliciting the same information from the same management person(s) by multiple teams, and supports efforts to determine the impact of deficiencies across control systems.

Section 8

ANALYZING DATA AND INTERPRETING RESULTS

Contents

Introduction

This section provides guidelines to help inspectors analyze data and interpret the results of data collection activities. The guidelines include information on the analysis process, including factors to consider while conducting an analysis. Information is also included on the significance of potential deficiencies, as well as suggestions for additional activities that may be appropriate if deficiencies are identified in a particular area. After completing each activity, inspectors can refer to this section for assistance in analyzing data and interpreting results to determine whether additional information is necessary for accurately evaluating PPM.

When analyzing the data collected on a particular aspect of management, it is important to consider both the individual facets of the management program and the program as a whole. In other words, failure of a single facet of a management program does not necessarily mean that management failed. One must analyze issues in terms of the entire management environment. Throughout the analysis process, PPM focuses on the highest levels of management accountability reasonable for each issue. For example, the Department issued a policy to reduce the amount of overtime security police worked each month since 9/11. At location "A," the metric they used to measure protective forces management effectiveness was the reduction of *unscheduled overtime* over the previous year. Under this metric, protective forces management appeared successful because it had in fact reduced the amount of unscheduled overtime. However, closer examination revealed that protective forces still worked the same amount of overtime hours but now the *unscheduled* overtime was artificially reduced by adjusting the *normal* scheduled shift from an 8-hour day to a 10-hour day. Thus, *normal* shifts automatically included two hours of overtime.

Analysis of Results

The analysis process involves the critical consideration by topic team members of all inspection results, including the results in other topic areas. Analyses will lead to logical, supportable conclusions regarding how well the protection program is managed and therefore meets the required standards and satisfies the intent of DOE policy. A workable approach is to first analyze each PPM subtopic individually and then integrate the results to determine: 1) the

effects of subtopics on each other; and 2) the overall status of the topic. Following the analyses of PPM topic indicators, results from other inspection topics can be used, much as the performance test might be used, to further illuminate the current status of PPM.

Objective, validated data should be the backbone of analysis. Though the PPM topic does not lend itself to the same types of quantified analysis as other subtopics, most subtopics at least offer the opportunity for go/no-go types of observations that address minimum requirements even if such characterizations do not describe the quality of efforts. For example, objective analysis within a survey program can indicate whether or not a team leader has been appointed, a schedule written, all areas surveyed, and whether the survey was predominantly document reviews or performance based. If a number of these elements are missing (no-go), the analysis will have a more objective basis prior to descriptions of the qualitative nature of the program. Conversely, inspectors must avoid the pitfall of defaulting to all issues as *ultimately management failures* simply because management is always accountable. Inspectors should consider the lowest organizational level capable or responsible for addressing an issue when assigning findings to specific subtopics. If an issue is too broad or requires resources and authority outside the scope of subtopic element managers, this might be greater evidence that it is a PPM-level issue.

If there are no deficiencies, the analysis can proceed from compliance to performance and make inferences as to whether or not PPM elements provide plausible assurance that security requirements have been met. If there are negative findings, weaknesses, deficiencies, or standards that are not fully met, analyses must consider the importance and impact of those conditions. In particular, deficiencies identified in other topic areas must be analyzed to determine whether they are caused by topic-related factors or are indicators of a broader PPM concern. Deficiencies must be analyzed both individually and in concert with other deficiencies, and balanced against any strengths and mitigating factors to determine their overall impact on safeguards and security management's ability to meet the required standards. Factors that should be considered during analyses include:

- Whether the deficiency is isolated or systemic
- Whether management personnel knew of the deficiency, and what action was taken
- The importance or significance of the issue affected by the deficiency
- Mitigating factors, such as the effectiveness of other management actions that could compensate for the deficiency
- The deficiency's actual or potential effect on mission performance or accomplishment
- The magnitude and significance of the actual or potential vulnerability of DOE security interests resulting from the deficiency.

All analyses must result in a conclusion concerning the degree to which PPM meets required standards and provides an acceptable level of safeguards and security.

Relative Importance of PPM Subtopics

Because of the extensive and close interrelationship of the five PPM subtopics, they are not rated as stand-alone elements. Identification of the subtopics assists in the definition and understanding of PPM, aids in structuring data gathering, and helps strengthen the analysis process. There is no single subtopic of greater importance than another. Neither is it accurate to declare each subtopic as representing 20 percent of the overall score and then attempting to rate accordingly. As with topic areas, a determination of the relative weight of an issue within a subtopic area can only be made on a case-by-case basis. However, inspection

experience has demonstrated that a problem might exist within a single PPM subtopic area that is of such magnitude that it impacts either directly or indirectly on other aspects of the management program and, accordingly, has an adverse impact on the overall rating for PPM. In addition, the overall performance of the safeguards and security system, as measured by the evaluation of other topics, must be considered in assigning a PPM rating. The conclusions reached through the analyses of PPM subtopic inspections result in the assignment of a single rating for the subtopic. The topic team is responsible for recommending the PPM rating to the inspection team chief. However, ratings are not determined until vetted through the quality review board process.

Observations leading to **ratings assigned to other topics** and their subtopic areas should be considered during deliberations on assigning a rating to the PPM topic. The relationship of all topic areas to PPM is so close that all ratings must be considered as part of the final PPM rating. The effect of other topic ratings on the PPM topic rating can be determined only on a case-by-case basis after the issues are well defined and their relative importance to the protection program have been evaluated. The following questions should be considered concerning the ratings and issues of other topic areas:

- Has a pattern of similar findings in multiple topic areas shown an overall management shortfall in the protection program?

- To what extent did the PPM issue contained in or underlying the finding contribute to the topic rating? In other words, would a less than satisfactory rating for the PPM topic constitute double jeopardy?

- Does the root cause of the topic issue impact the PPM topic directly, indirectly, or not at all?

- Even when there are no management-related findings in other topic areas, is the cumulative effect of ratings and issues in the other topic areas of a magnitude to significantly impact the PPM area?

- Would timely management actions have precluded the deficiency?

- Do analyses of ratings and issues of the other topics reveal a systemic PPM problem?

Interpreting Results

Planning Process

The most significant challenge in evaluating protection program planning is the analysis of collected data to determine the impact and root causes. The close interrelationships among the PPM subtopics and, in fact, the high degree of interdependence among PPM and the other topic areas complicate the analysis of the impact of a specific shortcoming in protection program planning. There is usually no easy answer to such questions as: "If our planning is so bad, why do we get satisfactory ratings in all the other topics?" or "If our planning is so good, how can we fail in _____?"

Planning cannot be considered in isolation among the various skills and disciplines that make up PPM. Good plans are ineffective if poorly implemented or if there is minimal monitoring of progress and/or reaction by management to a lack of progress. Some managers might be able to make their programs work without formal plans by making ad hoc, seat-of-the-pants decisions as issues arise. A severe test of the system, such as an SP-40 inspection or an actual adversary attack, might be the first indicator of the weakness inherent in such a system. Also, a system might be effective in meeting threats and performing its assigned tasks while being very inefficient, especially in the area of program cost effectiveness.

An adequate planning process must provide assurance that the facility protection system will not fail due to the lack of adequate planning. Key indicators of a good planning process are:

- Site management is involved in the site/facility planning process.
- Safeguards and security managers support planning as a key element of the program.
- Planning procedures, responsibilities, and authorities are documented.
- Guidance on planning techniques and plan content is readily available.
- Plans are current and reviewed on a regular basis.
- Plans are fully coordinated with all affected parties.
- A process for revising plans is clearly identified.
- Responsibilities, authorities, and milestones for the planning process are documented and understood by key personnel.
- A mechanism for periodic, independent review of plans is established.
- A competent planning staff exists.
- The planning process includes measures to assure effective implementation of plans and changes thereto.

The evaluator(s) of protection program planning must take a number of factors into account and determine whether the overall planning environment exists to assure an adequate planning base, both now and in the future. A negative evaluation will not, in itself, indicate a management failure, but will indicate overall PPM planning effectiveness, which must be factored into the overall PPM picture by the topic team. Answering the following questions[1] will help determine whether the PPM planning process is adequate:

- Did the responsible secretarial office provide programmatic guidance and information to the operations office to assist in developing the SSSP? Is this guidance further refined if necessary and provided to the responsible planning organizational levels?
- Is the SSSP approved and current? Does it contain all of the required components?
- Is the SSSP supported by accurate, current, and validated VA analysis?
- Do the VA evidence files provide adequate support for the assumptions and decisions made in the analysis?
- Are Headquarters, field element, and site PPM key personnel aware of safeguards and security planning requirements and actively involved in the safeguards and security planning process?

Organization and Staffing

Suitable organization and staffing is a fundamental requirement for a viable protection program. Results of the data collection should be interpreted in relation to the immediate- and long-term positive and negative effects of the organization and staffing that exist at the time of the inspection. Although the current status of the protection program as determined by other topic teams might be a consideration, the overall effectiveness of the subtopic should normally be based on the data gathered specifically for this subtopic.

Organizations are formed to accomplish goals and objectives. Inspectors are cautioned to recognize that many different organizational

[1] These questions are intended to complement, not replace, any standards and criteria issued through official DOE channels.

structures can accomplish the same task. *The primary consideration is whether the current organization can meet its goals and objectives efficiently.* Deficiencies identified in the organization and staffing subtopic are usually identified by another topic team as well. The PPM topic team might contribute significantly to identifying a root cause for organization and staffing issues observed by other topic teams.

In general, if the answers to the following questions are all affirmative, the facility's organization and staffing are probably sufficient to meet its goals:

- Has management established an effective and efficient organizational structure?
- Are staffing levels adequate to support the organizational structure and fulfill the functional requirements?
- Are personnel qualified and trained for their positions?

Budget Process

The failure of a manager to successfully address budget concerns might not result in immediate programmatic failure. However, failure to adequately plan for and monitor use of resources might be an underlying cause of other safeguards and security programmatic difficulties, or might reduce the effectiveness of the program in the future. Budget matters might also explain apparent deficiencies in the PPM elements of the planning process or program control systems. No assessment of the status of PPM can be complete without consideration of the degree of budget and cost control exercised by the various levels of management. In general, if the answers to the following questions are all affirmative, then safeguards and security budget activities are probably sufficient to support an adequate program:

- Do the Federal oversight element and contractor budget processes include mechanisms to properly identify and prioritize safeguards and security items relative to other activities reflected in the budget?
- Does the Federal oversight element safeguards and security director (or equivalent safeguards and security management level) participate in the operations office budget formulation process?
- Does the contractor safeguards and security director (or equivalent safeguards and security management level) and staff participate in the site budget formulation process?
- Do the appropriate field element staff responsible for safeguards and security activities demonstrate that they are knowledgeable of and participate, at least indirectly, in the operations office budget formulation process?
- Do the appropriate field element safeguards and security staff demonstrate that they are knowledgeable of contractor safeguards and security budget formulation processes?
- Do the appropriate field element personnel (not necessarily safeguards and security) actively support safeguards and security items during the Headquarters budget formulation and approval process?
- Do the appropriate field element safeguards and security staff demonstrate that they are knowledgeable of the safeguards and security budget estimate items under their purview?
- Do contractor safeguards and security staff demonstrate that they are knowledgeable of the safeguards and security budget estimate items under their purview?

- Do the appropriate field element safeguards and security staff understand, in general terms, the various appropriations, funding categories, and budget execution concepts?

- Do the appropriate field element safeguards and security staff monitor progress of fund expenditure for safeguards and security activities, including the status of allocated costs, obligations, costed items, etc?

- Do the contractor safeguards and security staff monitor the progress of fund expenditures for safeguards and security activities, including the status of allocated costs, obligations, costed items, etc?

- Do the appropriate field element staffs participate in or closely monitor the annual allocated cost budget review?

The significance of each of these issues will depend on the situation. Inspectors should remember that, in most cases, the budget directly associated with safeguards and security is a relatively minor portion of the operations office or contractor budget. For this reason, personnel in the mainstream budget formulation process are not accustomed to working with safeguards and security staff. In addition, safeguards and security professionals, especially Federal staff, are largely conditioned by past experience to believe that the budget formulation and execution process is complicated and irrelevant to their main function. These cultural factors will tend to limit the activity of the safeguards and security staff in the budget process. A very solid safeguards and security program will have some personnel who understand, to some degree, both the budget and safeguards and security worlds. If such staff members exist and are involved in the overall program management process, adverse budget-related issues will normally be minimal except for availability of adequate funds. The safeguards and security director should have general knowledge of the program budget status and a good understanding of how he/she can best support his/her priorities in the local budget formulation and execution process. Field element safeguards and security staff should be knowledgeable of the budget and expenditure status of safeguards and security activities within their purview.

Program Direction

Adequate program direction is essential to a viable protection program. Inadequate program direction can significantly degrade the overall ability of the protection program to consistently achieve its goals and objectives. Program direction data collected during the inspection should be interpreted in relation to the immediate and long-term effects of the program direction that exist at the time of the inspection. Programs operating largely on impromptu and verbal direction typically fail to efficiently implement a lasting, effective protection program. Even if no immediate effects of questionable direction are apparent, the longer-term impact should be examined. For these reasons, a major factor in interpreting results of the data collection is the existence, accuracy, and usefulness of the program direction provided in DOE orders, memoranda of understanding, memoranda of agreement, plans, policies, procedures, standard operating procedures, and special police officer instructions.

The bottom line is whether program direction is communicated effectively from the DOE Headquarters level to the special police officer at the security post level. If the answers to the following questions are all affirmative, the inspector might generally consider program direction to be adequate:

- Is the program implemented in accordance with DOE policy and direction?

- Is there evidence of active program direction by each level of the organization?

- Is the program direction documented accurately and to a degree that provides long-term direction to the protection program?

Control Systems

Effective control systems at all levels of management are a fundamental requirement for managing a protection program. Although each level has requirements for different kinds of data and information as feedback, each also has common requirements. Generally, greater detail is required lower in the hierarchy, while top-level management is normally interested primarily in major issues, specific data, and standardized reports. A failure in establishing and implementing adequate control systems could result in management making decisions based on insufficient or inaccurate information. Effective control systems provide each manager sufficient information to determine the status of the organization.

The bottom line for the inspector is to determine whether the control systems in place provide the necessary feedback to the manager on the status of the protection program elements. If the answers to the following questions are all affirmative, the inspector should generally consider the control systems to be adequate:

- Are surveys, inspections, self-assessments, and other internal control systems in place to determine the effectiveness of the safeguards and security program on a recurring basis?

- Is there an effective system for identifying, tracking, and bringing to timely closure deficiencies noted in surveys, inspections, self-assessments, and self-directed control systems?

- Are control system reports provided to the appropriate organizational level to ensure proper management attention?

Including Results from Other Topics

When including results and findings from other topics, the discussion of each should be presented under one of the PPM subtopics. For example, failure of the survey program to detect long-standing deficiencies in protective force and physical security systems should be appropriately addressed under organization and staffing, control, or direction depending on the root cause. Other issues should be placed under appropriate subtopics in PPM according to a best analysis of the root cause of the condition within the management system. Such issues should be fully integrated into the analysis of the status of each subtopic, leading to an overall topic rating.

This page intentionally left blank.

Appendix A

INSPECTION TOOL KIT

Contents

The following tools and forms are designed to help inspectors request site protection program management documentation as a "data call," systematically plan and schedule topic activities, and record and evaluate the effectiveness of individual elements of protection program management. These tools and forms can be used

at the inspector's discretion and should be tailored for each inspection. The tools and forms are arranged to support an inspector through all phases of the inspection process and may require revision in response to new or modified U.S. Department of Energy (DOE) direction.

In evaluating each element and assigning ratings, it is important to consider all compensatory systems and mitigating factors. Professional judgment must be used to arrive at the overall ratings.

PROTECTION PROGRAM MANAGEMENT PERFORMANCE MEASURES

PROTECTION PROGRAM MANAGEMENT PERFORMANCE MEASURES

PLANNING

Determine whether the set of site vulnerability assessments (VAs) and resulting security plans accurately represent the total site operating environment by asking:

- Does the set of site VAs represent the total site operating environment?
- Do VAs portray a threat appropriate for site operations?
- Are there assumptions made that unreasonably limit adversary actions or capabilities?
- Do the adversary strategies and tactics evaluated reflect the best choices for the adversaries under the prevailing assumptions?
- Do strategies and tactics reflect those actually trained for and used by the site?
- Is the methodology used to evaluate protection effectiveness adequate to evaluate adversary and site actions and responses?
- What methodologies are used for site VAs?
- Are these methodologies adequate to evaluate the site's vulnerabilities in light of the operational environment?
- Is DOE standard modeling data being used, such as the standard DOE Probability of Hit (PH) and Probability of Kill (PK) file for Joint Tactical Simulation/Joint Conflict and Tactical Simulation (JTS/JCATS) tactical models?
- How are unique site and adversary weapons characterized in simulations?
- How is other unique site and adversary equipment (e.g., vehicles) characterized in the modeling?
- How are adversary delays determined?
- How are adversary task requirements determined?
- Do the sites and conditions under which performance tests are conducted match those depicted in computer simulations closely enough to allow comparison? If so, how well do they compare?
- How many workstations were allocated to adversaries and to the site protective force during Joint Tactical Simulation (JTS) simulations? Did this have any effect on the outcome of particular scenarios?
- Have the results of the VAs been portrayed correctly in the Site Safeguards and Security Plan (SSSP)?

- Does the description of site operations include all current activities?
- Does the description of site protection measures accurately reflect those implemented?
- Does the process for preparing an SSSP provide for reasonable input from all concerned parties?
- Is the approval current?
- What is the status of identified upgrades?

RESOURCES

Determine whether National Nuclear Security Administration (NNSA) has allocated the resources necessary to effectively perform the mission of the site and sufficient levels of staff are trained and qualified for the duties they are assigned by asking:

- Are DOE safeguards and security (S&S) managers involved in the S&S budget formulation process?
- What are the assumptions and guidance under which the budget was formulated?
- Are these assumptions and this guidance consistent with commitments made in the SSSP and in corrective action plans (CAPs)?
- How is direct labor charged to an S&S account? Is there a charge code?
- Is the charge code related to a work breakdown structure or similar work planning and tracking system?
- How are the work breakdown system (or equivalent) elements related to the S&S budget and reporting codes?
- Is there a current year spending plan? How well are expenditures to date matching that plan?
- What is the overall indirect burden on S&S funds?
- What are its major components?
- How does it compare to the indirect burden on other project funds?
- Is there an area where lack of funding might create a protection issue?
- What means are used by Federal S&S managers to track S&S achievements versus expenditures?
- Have responsibilities been explicitly assigned to individuals?
- Has there been an analysis, either formal or informal, of the job skills needed to fulfill each assigned responsibility?

- Do these assignments of responsibility frequently change?
- Is there a mechanism to track individual qualifications versus currently assigned responsibilities?
- Is there evidence that management is ensuring that individuals gain and maintain the job skills needed to fulfill assigned responsibilities?
- Are sufficient training funds available?
- Are there one or more areas in which additional training emphasis is needed?
- If all Federal staff are not fully competent to discharge their assigned duties, what is the primary cause for this?

CONTROLS

Determine whether an effective process is in place for incorporating new directives into the site contract and whether an effective mechanism is in the contract to reward or penalize contractor performance by asking:

- What is the process for incorporating new directives into the site contract?
- How are new directives incorporated into daily implementation for site-related DOE organizations?
- Has the incorporation of any DOE directive been unduly delayed?
- Are all deviations correctly characterized as variances, waivers, and/or exceptions?
- Have any increased risks associated with deviations or delay in incorporating directives into contracts or into routine DOE operations been correctly analyzed and stated in decision packages?
- Have any other topic teams identified a weakness that was caused by a delay in implementing directives or inappropriate approval of deviations?
- Are there formal, scheduled meetings at several management levels?
- Are mechanisms established to provide S&S technical direction to the contractor?
- Are there memoranda or other evidence that local Federal managers provide effective direction to the contractor?
- Do interviews establish that there is free communication among corresponding levels of Federal and contractor management?
- Are there examples of cases where complex issues of local implementation have been successfully resolved between Federal and contractor management?
- What mechanisms exist in site contracts?

- How much money is involved—both total and as a percentage of payments—in a billing period?
- What is the process for using the mechanism?
- Has it been used?
- Was the desired result achieved?

FEEDBACK

Determine whether effective management processes are in place that enable the Federal staff to accurately examine and document the contractor's S&S performance and require corrective actions that preclude recurrence of identified weaknesses.

Determine whether effective management processes are in place that enable the contractor staff to accurately self-examine and document the S&S program performance and produce corrective actions that preclude recurrence of identified weaknesses by asking:

- Do formal survey procedures exist?
- Are they followed?
- Is there evidence that sufficient expertise is included on survey teams to provide a valid review?
- Is sufficient time allowed to support a valid review?
- Have surveys been conducted on time?
- Are reports published on time?
- Are reports sufficiently detailed to support the ratings given?
- Are findings made when weaknesses are identified?
- What other methods of identifying weaknesses or opportunities for improvements are used?
- Are findings promptly entered into Safeguards and Security Information Management System (SSIMS)?
- Do formal self-assessment procedures exist?
- Are they followed?
- Is there evidence that sufficient expertise is included on self-assessment teams to provide a valid review?
- Is sufficient time allowed to support a valid review?

- Have self-assessments been conducted on time?
- Are reports published on time?
- Are reports sufficiently detailed to support the ratings given?
- Are findings made when weaknesses are identified?
- What other methods of identifying weaknesses or opportunities for improvements are used?
- Are findings and other items of note entered into a tracking system?
- Are CAPs prepared for all findings?
- Are CAPs prepared for other observations made during a review?
- Are CAPs supported by effective analysis?
- Do CAPs contain all necessary information elements?
- Is effective root cause analysis and cost-benefit analysis conducted?
- Is effective risk assessment performed?
- Are corrective actions completed on schedule?
- Are corrective actions completed in a timeframe commensurate with the impact of the protection weakness?
- Is there a procedure for tracking and trending findings?

ISSM

Determine whether formal mechanisms are in place to ensure implementation of integrated safeguards and security management (ISSM) guiding principles and whether the program produces a fully integrated management approach to the S&S program by asking:

- What formal mechanisms are in place to ensure implementation of ISSM guiding principles?
- What informal mechanisms are used to implement ISSM guiding principles?
- Should any informal mechanisms be formalized?
- What formal mechanisms are in place to ensure that the five core functions of ISSM will be evident in each site project?
- Are there informal mechanisms used to implement core functions?

- Should any informal mechanisms implementing core functions be formalized?
- Are there formal mechanisms to identify requirements for S&S knowledge and skill requirements for S&S staff and for others with key ISSM roles?
- Does a failure to implement ISSM guiding principles or integrate ISSM core functions into site operations appear to be a contributing or root cause for protection deficiencies?
- Do position descriptions describe S&S requirements, including key ISSM roles?
- Do performance evaluations indicate that S&S performance is regarded as a significant portion of job performance for those with key ISSM roles and for other staff?
- Do S&S staff and others with key ISSM roles have the necessary skills and knowledge to effectively perform their duties?
- Do interviews reveal a sense of responsibility for S&S program effectiveness on the part of those with explicit ISSM responsibilities as well as those with more general responsibility for ISSM?
- Are key ISSM positions formally identified?
- Have personnel filling ISSM positions been formally assigned to them?
- Do those personnel have sufficient authority to discharge their ISSM responsibilities?
- Are the ISSM responsibilities of other line managers and security managers sufficiently clear, in procedures and in practice, to support the ISSM objective?
- Do recent non-security-specific project procedures indicate that ISSM is being practiced?
- Do recent actions to support operational missions indicate that ISSM is being practiced?
- Were security managers and line managers cognizant of any risk acceptance decisions that may have led to weaknesses noted during the inspection?
- Have responsible managers balanced security risks and operational requirements?

PROTECTION PROGRAM MANAGEMENT
DETAILED INSPECTION PLAN

PROTECTION PROGRAM MANAGEMENT SAMPLE DETAILED INSPECTION PLAN

The performance measures feed directly into this document by being distilled into the activities that reflect compliance and performance in each topic area at the levels required by DOE to provide adequate safeguards and security. The subtopic objectives are posed in the form of a question. The impact of not achieving these objectives is described in the statement below. On a site-by-site basis, lines of inquiry are developed for the performance measures and the data collection is tailored to address them. Remarks are used as necessary.

PERFORMANCE MEASURE	CRITICAL CRITERIA/LINES OF INQUIRY	DATA COLLECTION ACTIVITIES	REMARKS
PLANNING: 1. Are all plans current, do they accurately reflect DOE requirements, and are they approved by the appropriate authority? 2. Are vulnerability assessments (VAs) used to support the SSSP, deviation requests, and projected changes in facility mission and accurately characterize the site and the effectiveness of safeguards and security systems? 3. Does the site conduct and document planning activities used to implement changes in safeguards and security organization, procedures, training, and equipment? **IMPACT:** Planning is a critical element of the safeguards and security program because it is the basis for the budget, organization, training, staffing, procedures, doctrine, and equipment. Validity and confidence are directly attributable to the accuracy of the characterization of the protection system, and its physical attributes, and protective force capabilities to detect an intrusion, transmit the alarm, and respond effectively.			
Management: Personal competence and training are maintained by management making adequate resources available to perform all security program functions.	Are resources (staffing and budget) planned to adequately support the structure; do they demonstrate timely completion of functional requirements?	1. Review corrective action plans (CAPs) to determine the time required to address identified program weaknesses. 2. Conduct interviews and review records to determine the extent of any overdue plan revisions and VA activities impacting program implementation. 3. Review records to determine the number and type of additional duties.	pre-planning pre-planning and onsite pre-planning

PERFORMANCE MEASURE	CRITICAL CRITERIA/LINES OF INQUIRY	DATA COLLECTION ACTIVITIES	REMARKS
		4. Interview managers to identify budgetary impacts on program implementation. Also determine the relationship between projected work and the amount of scheduled/unscheduled (paid and unpaid) overtime granted during the past year. 5. Obtain information to determine how work is scheduled to insure all necessary activities are accomplished. 6. Review records to determine the number of personnel assigned against the number authorized.	onsite pre-planning
Management: Personal competence and training are maintained by management making adequate resources available to perform all security program functions.	1. Is the basis used by the Safeguards and Security Director (SSD) sufficient to assert that individuals performing security functions are technically competent? 2. Has the level of turnover of security specialists impacted the program? 3. Is there a structured program (on-the-job training [OJT] program, desk-side procedures, mentoring, etc.) for preparing new personnel for duties as a security specialist?	1. Interview the SSD or person responsible for the training of the security professionals to determine whether the program has been formalized, if it is based on a needs and job-task analysis, and whether lesson plans have been developed to support locally developed training. 2. Interview personnel security program managers or professionals (both continuing and new hires) to determine their satisfaction with the training program. 3. Review position descriptions to verify that responsibilities are actually reflected at the individual's level. 4. Interview personnel/review records to determine both the turnover in personnel security professionals and what program is in place for new hires.	onsite onsite pre-planning onsite

PERFORMANCE MEASURE	CRITICAL CRITERIA/LINES OF INQUIRY	DATA COLLECTION ACTIVITIES	REMARKS
Management: Program direction, plans, and records are supported by security program representatives' involvement in the development of plans to analyze and mitigate the risk represented by insiders, and/or to determine the level of assumed risk. Management ensures that security plans, policies, and priorities are adjusted to meet changing threat situations.	1. Are security concerns adequately addressed in the site operational and security planning processes? 2. Does security professionals' participation in threat analysis studies, management-level meetings, and budget allocation deliberations lead to security program issues being identified, analyzed, and addressed? 3. Are security program plans and procedures sufficient (i.e., accurate and comprehensive) to support the successful implementation of all elements of the security program?	1. Interview managers and security professionals to determine the extent to which security professionals participate in planning meetings, budget discussions, and management-level decisions. 2. Review the SSSP and other security and operational planning documents to determine the manner in which security concerns are addressed. 3. Review site policies to determine whether security program officials are in a position to ensure compliance. 4. Interview personnel/review records to determine whether any program weaknesses are due to a lack of authority over operational elements to implement requirements (including CAPs). 5. Review site security program procedures to determine whether they are accurate and comprehensive. 6. Interview managers to determine what incentives are used to encourage good performance.	onsite pre-planning pre-planning onsite pre-planning onsite
Management: Feedback and improvement is supported by effective self-assessment and corrective action programs.	1. Has the self-assessment program identified significant program weaknesses that, when addressed, would materially enhance program implementation? 2. Does the corrective action process include all the required elements (i.e., analyze root cause and prioritize actions, establish corrective action schedule that will allow monitoring	1. Review past self-assessments to determine whether they reflect thorough coverage of the security program and are conducted on a regular basis. 2. Review records to determine who conducts the self-assessments and their qualifications. 3. Review records to determine whether concerns identified during self-assessments are entered into a	pre-planning pre-planning pre-planning

PERFORMANCE MEASURE	CRITICAL CRITERIA/LINES OF INQUIRY	DATA COLLECTION ACTIVITIES	REMARKS
	progress, assign responsibility for each action to a specific individual, continually update the plan, and ensure adequate resources are applied) to ensure that identified weaknesses are addressed in the most effective and efficient manner?	central tracking system. 4. Review procedures to determine whether the corrective action process contains all the required elements. 5. Review records to determine whether some form of independent verification of closure of findings is in place.	 pre-planning pre-planning

PROTECTION PROGRAM MANAGEMENT
INSPECTION PROCESS MATRIX

PROTECTION PROGRAM MANAGEMENT INSPECTION PROCESS MATRIX

STEPS	COMPLETION DATE	ACTION OFFICER(S)/REMARKS
PRE-PLANNING		
Develop an overview of past security program issues and concerns by reviewing past inspection results and discussing them with team members.		Team Leader. ***Throughout pre-planning, the team leader will consult with other team members to identify and analyze past and current site-specific or complex-wide security program issues.***
Review site protection strategy, VAs/SSSP, security plan, Classified Material Protection and Control (CMPC) team data or cyber security team data to develop a list of potential adversary targets/facilities and personnel positions critical to the protection of special nuclear material (SNM), and review classified and sensitive unclassified information on which to base data collection activities/sampling. Examples: -Facilities processing, handling, and storing SNM -Facilities/vaults that require enrollment in a human reliability program (HRP)		Team Leader
Contact Deputy Inspection Chief and obtain the name of the operations office and contractor security program points of contact.		Team Leader
After the completion of the above: -Confirm topic and subtopic objectives and scope. -Assign personnel/resources to support data collection activities. -Develop expectations regarding the completion of data collection tasks.		Team Leader
Refine topic objectives and scope, and tailor the document request list.		Team Leader

STEPS	COMPLETION DATE	ACTION OFFICER(S)/REMARKS
Develop the security input for the inspection plan (topic focus [topic elements and/or issues that will have the most bearing on determining the effectiveness of the topic], performance testing, management interviews, potential issues, and data collection assignments).		Team Leader
Develop topic team schedule. (The schedule is a general forecast of activities and not a precise description of each day's activities.)		Team Leader
Contact field points of contact; provide (via email) topic objectives, data collection activities/schedule, and the document request list, which identifies items that need to be sent to Germantown in advance of onsite activities and those items that are needed at the site.		Team Leader
Meet with Headquarters topic points of contact to gather information and to discuss data collection activities.		Team Leader
Draft topic annex/subtopic report submission (intro, background, and conduct), save to computer disk, and provide to document control center for transmission to site.		Team Leader or Principal Writer
Identify items to be sent from the site to the document control center.		Team Leader
Prepare a list of additional documentation needed from the site for use before or during the planning meeting and provide to Deputy Inspection Chief; email the request to points of contact.		Team Leader
Receive and review requested documentation in preparation of the planning meeting.		Team Leader
Verify initial schedule with team and points of contact.		Team Leader

STEPS	COMPLETION DATE	ACTION OFFICER(S)/REMARKS
CONDUCT ONSITE PLANNING AND INITIAL DATA COLLECTION (FOUR DAYS)		
Assemble at badge office, **Monday**		Team
Attend site security and safety training, **Monday**		Team
Attend In-Briefing, **Monday**		Team
Meet field points of contact, confirm/refine schedule, **Monday**		Team
Assemble at work space to conduct topic team meeting to discuss matters as appropriate before the initiation of planning/data collection activities, **Monday**		Team
Sign copies of the computer security plan, and post the plan, **Monday**		Team
Verify receipt of all requested documents and provide to Administrative Support Manager, **Tuesday or Wednesday**		Team Leader
Collect data, **Tuesday-Thursday** -Interview security program officials and specialists. -Complete reviews and record results on file review form. Validate data (as team will be split, each team member will validate data as it is collected and then summarized with attending field points of contact when a data collection activity is completed).		Team Team
Must keep Team Leader informed of location and phone number (may be done via administrative support personnel).		Team
Daily, prepare data collection forms (personal preference: either complete before the daily team meeting, after the meeting, but not later than the initiation of the next day's data collection activities). Data collected on the forms should represent a roll-up and **not a verbatim transcription** of an individual's notes. In this way, the analysis process will be initiated and it should ease preparation of		Team

STEPS	COMPLETION DATE	ACTION OFFICER(S)/REMARKS
Issue Forms (when required) and the inspection report. Distribute to Deputy Inspection Chief and Administrative Coordinator.		 Team Leader
When required, prepare Issue Forms. Review Issue Forms and provide to inspection management. Resolve site comments.		Team Member Team Leader Team Leader and Member
Topic team discusses results of data collection, leading to drafting of evening bullets, and confirms/revises schedule (should occur briefly before the daily meeting, over the phone if necessary). *The topic team leader is responsible for deciding when an issue will be raised during the evening meeting and may want to delay discussion of that issue during the evening meeting until team consensus can be achieved. *Issues that could impact the topic rating should normally be discussed in the evening meeting only after: -Topic team has reached agreement on the importance of the issue -Integration with other topic teams has been completed -Inspection team management has been informed off-line (no surprises). ***Assign a team member the responsibility to capture on an Issue Form any issues that could***		Team Leader

STEPS	COMPLETION DATE	ACTION OFFICER(S)/REMARKS
impact the rating. (Initially this will assist internal topic and inspection team discussions of the issue, and may lead to formulation of an issue paper for site response.)		
Attend daily team meeting. Team Leader may coordinate the absent team members.		Team
Finalize evening bullets and provide to Deputy Inspection Chief during the evening meeting.		Team Leader
Conduct end-of-the-day security checks.		Team
Throughout this phase of the inspection the team works to: - Identify the key results to date. - Determine the facts that support the key results, and capture these facts on an Issue Form for rating impacting issues *(initially this will assist internal topic and inspection team discussions of the issue, and may lead to formulation of an issue paper for site response).* - Revise data collection plan and adjust resources to collect this data. - Revise topic annex/sub-topic report submissions/bulleted outlines (intro, background, and conduct, and results if possible).		Team
Meet with field points of contact to provide summary of initial results, and to schedule future data collection activities for HRP, safeguards and security awareness, and unclassified foreign visits and assignments (FV&A), **Thursday**		Team
Identify and destroy unwanted papers; return pagers, keys, and dosimeters to administrative support personnel, **Thursday**		Team

STEPS	COMPLETION DATE	ACTION OFFICER(S)/REMARKS
POST-PLANNING ACTIVITIES		
Conduct Headquarters interviews (Principal Security Officers, NNSA, etc.).		Team Leader
Review additional documentation.		Team Leader and Team
Collect and validate data.		Team Leader
Analyze data collection results to date.		Team
Refine inspection focus and topic assignments.		Team Leader
Coordinate inspection activities with field points of contact.		Team
When required, prepare data collection forms, and distribute to Deputy Inspection Chief and Administrative Coordinator.		Team Leader
When required, prepare Issue Forms, review Issue Forms, and provide to Deputy Inspection Chief; resolve site comments on Issue Forms.		Team Leader
DATA COLLECTION, DRAFT REPORT, AND APPENDIX PREPARATION (TWO WEEKS)		
New team members report to badge office, attend training, and sign computer security plans, **Monday afternoon**		Team Member (s)
Conduct topic team meeting on first day of data collection to confirm/refine schedule, **Monday afternoon**		Team Leader
Collect data, Tuesday through Thursday - Follow up on any issues related to the security program. Validate data (as team will be split, each team member will validate data as it is collected and then summarized with the attending field points of contact when a data collection activity is completed). *The topic team leader is responsible for deciding when an		Team Team

STEPS	COMPLETION DATE	ACTION OFFICER(S)/REMARKS
issue will be raised during the evening meeting and may want to delay discussion of that issue during the evening meeting until team consensus can be achieved. *Issues that could impact the topic rating should normally be discussed in the evening meeting only after: - Topic team has reached agreement on the importance of the issue - Integration with other topic teams has been completed - Inspection team management has been informed off-line (no surprises). ***Assign a team member to prepare an Issue Form as soon as such an issue has been identified.***		Team Leader
Must keep Team Leader informed of location and phone number (do not rely on administrative support personnel).		Team
Daily, prepare data collection forms (personal preference: complete either before the daily team meeting or after the meeting, but not later than the initiation of the next day's data collection activities).		Team Team Leader
When required, prepare Issue Forms. Review Issue Forms and provide to inspection management. Resolve site comments.		Team Member Team Leader Team Leader and Member
Attend daily team meeting (as before, team members may be absent with approval).		Team
Finalize evening bullets.		Team Leader
Conduct end-of-the-day security checks.		Team

STEPS	COMPLETION DATE	ACTION OFFICER(S)/REMARKS
Principal writer continues work on the draft appendix by completing work on security program sub-section, **Wednesday**		Principal Writer
Subtopic inspectors turn in all data collection forms and/or draft sub-sections of the appendix to the principal writer by **Friday close of business**		Team
When required, conduct discussion with team members on **Friday afternoon** to prepare the Inspection Chief focus briefing, to include: - Finalize the key points (conclusions) to be made in the inspection report - List the facts that support each key point - Do not over-emphasize lesser strengths or weaknesses that might obscure the presentation of the key points - Findings - Policy issues - Proposed rating		Team
When required, present Inspection Chief focus briefing, **Saturday**		Team Leader
Finalize draft topic appendix, **Saturday**		Principal Writer
Conduct reviews of the draft appendix for content and readability; provide comments to principal writer, **Saturday and Monday morning**		Team
Conduct technical edit of draft appendix; provide input to principal writer**, Monday afternoon**		Team
Turn in draft inspection report to the Quality Review Board (QRB), **Monday or Tuesday morning**		Team Leader
Provide list of acronyms, interviews, and references to Administrative Support Manager, **Tuesday**		Team

STEPS	COMPLETION DATE	ACTION OFFICER(S)/REMARKS
Address QRB/site comments (inform Quality Review Board of actions) **Tuesday or Wednesday**		Team Leader
Meet with site personnel to discuss the disposition of comments on the draft inspection report appendix, **Tuesday or Wednesday**		Team
Prepare briefing bullets and notes, **Tuesday**		Team
Participate in roundtable, **Wednesday or Thursday**		Team
Identify documents for return to Germantown; return room keys, dosimeters, and pagers; destroy unwanted documents; return supplies; return site documents, **Wednesday and Thursday**		Team Leader
Conduct topic team lessons-learned meeting, **Thursday**		Team Leader
FINAL REPORT PREPARATION AND POST-INSPECTION ACTIVITIES		
Review 10-day site comments and incorporate as appropriate.		Team Leader
Review and respond to initial and final corrective actions and provide to Deputy Inspection Chief.		Team Leader
Revise Topic Inspection Process Matrix and distribute.		Team Leader

This page intentionally left blank.

DOCUMENT REQUEST LIST

DOCUMENT REQUEST LIST
PROTECTION PROGRAM MANAGEMENT TOPIC TEAM

XXXXX Inspection 200X

The following information is requested to support the protection program management topic (planning, organizations and staffing, budget process, program direction, and control systems) team.

The preferred method of transmission of any unclassified items is an attached file to an email message to the identified SP-40 point of contact. The alternative method of transmission is in hardcopy sent to DOE Headquarters – Germantown Building (Attention SP-40 point of contact). Any classified information must be sent to SP-40 according to DOE directives for mailing classified information.

Questions should be addressed to (SP-40 point of contact at (301) 903-XXXX).

1. **The following documents and/or information is requested to be sent to SP-41 by XXXX XX, 200X** (*one month prior to the planning week)*:

   a. ASSESS model files supporting each SSSP, including all associated module input and output files (1.44 MB diskette or compact disc). These files should be accompanied by a short list or explanation relating ASSESS files to facilities and SSSP scenarios.

   b. Most recently approved SSSP and the most current draft of each SSSP (if revisions are underway).

GENERAL INFORMATION

2. **Access to the following documents and/or information will be required during the onsite phase as indicated.**

Program Management: The exact titles and terminology of documents may differ.

Resource Allocation

1. Work breakdown structure(s) or similar documentation with correlation to safeguards and security budget and reporting codes.

2. Safeguards and security-related work authorization documents for the current fiscal year.

3. Site and Site Office safeguards and security budgets for the current fiscal year, previous budget submission, and any guidance received pertaining to the upcoming budget submission (only S&S data is needed).

4. Documentation of current status and projections of safeguards and security expenditures for the current and next fiscal years.

5. A summary description of the use of any safeguards and security supplementals for the current and last year.

6. A description of current and projected line items that include safeguards and security significant items and a summary of the status of each.

7. A description of current and projected non-line-item projects (General Plant Projects [GPP], etc.) that include safeguards and security significant items and a summary of the status of each.

Planning – Vulnerability Assessments

1. Most recent vulnerability reports for each target location (including mature drafts, if applicable).

2. Data from protective force performance testing that supports the most recent vulnerability analysis or protective force performance assumptions made in vulnerability assessments, particularly any performance tests included in the calculation of the probability of neutralization.

3. Other data from vulnerability analysis and modeling that support the current determination of site status.

Planning – Site Safeguards and Security Plans

1. NNSA site 10-Year Plan.

2. Site or Site Office safeguards and security strategic or mid-term plans reflecting SSSP commitments and/or those showing coordination with the 10-Year Plan.

3. List of critical systems and elements for safeguards and security.

4. Performance Assurance (PA) Test Plan for critical systems and elements.

Line Management Oversight

1. Documents describing the Site Office survey program.

2. Documents describing the Site S&S self-assessment programs.

3. Site and Site Office procedures for addressing inspection, survey, and self-assessment issues, findings, concerns, observations, and/or other action items related to the mitigation of identified weaknesses in the safeguards and security program.

4. Corrective action plans (CAPs) for all inspection, survey, and self-assessment issues, findings, concerns, and/or observations for the past three years and any current fiscal year CAPS that are available.

5. Records (including SSIMS) that reflect DOE and contractor verification, validation, and closure of issues, findings, concerns, and/or observations for the above CAPs.

TOOLS RELATED TO SECTION 2, PLANNING PROCESS

Tool 2-1

PLANNING WORKSHEET
FOR
PROTECTION PROGRAM MANAGEMENT

Facility/Site: _____

Subtopic: _____ Issue: _____

LINE OF INQUIRY	DOCUMENTS TO BE EVALUATED	INTERVIEWS TO CONDUCT	INTERVIEW QUESTIONS

Tool 2-2

PROGRAM PLANS AND PROCEDURES CHECKLIST
FOR
PROTECTION PROGRAM MANAGEMENT

Facility/Site: _____ Date of Evaluation _____

TOPIC AREA	PLAN	PLAN EXISTS?	PLAN ADEQUATE?	REVIEWER COMMENTS
Protection Program Management	Site Safeguards and Security Plan	☐ Yes ☐ No	☐ Yes ☐ No	
	Training Approval Program	☐ Yes ☐ No	☐ Yes ☐ No	
	Performance Assurance Program	☐ Yes ☐ No	☐ Yes ☐ No	
Protection Program Operations	Intra-site Movement of SNM	☐ Yes ☐ No	☐ Yes ☐ No	
Material Control and Accountability (MC&A)	MC&A Plan	☐ Yes ☐ No	☐ Yes ☐ No	

TOPIC AREA	PLAN	PLAN EXISTS?	PLAN ADEQUATE?	REVIEWER COMMENTS
	Self-Assessment Plans	☐ Yes ☐ No	☐ Yes ☐ No	
Protective Force (Pro-Force)	Tactical Response Plans	☐ Yes ☐ No	☐ Yes ☐ No	
	Post Orders	☐ Yes ☐ No	☐ Yes ☐ No	
	Annual Training Plan	☐ Yes ☐ No	☐ Yes ☐ No	
Physical Security Systems	Corrective Maintenance Schedule	☐ Yes ☐ No	☐ Yes ☐ No	
	Performance Assurance Program Plan	☐ Yes ☐ No	☐ Yes ☐ No	
Personnel Security	HRP Implementation Plan	☐ Yes ☐ No	☐ Yes ☐ No	

TOPIC AREA	PLAN	PLAN EXISTS?	PLAN ADEQUATE?	REVIEWER COMMENTS
	FV&A Generic and Specific Plans	☐ Yes ☐ No	☐ Yes ☐ No	
S&S	Emergency (Security Condition) Plans	☐ Yes ☐ No	☐ Yes ☐ No	
Emergency Management (EM)	Emergency Plan Implementing Procedures	☐ Yes ☐ No	☐ Yes ☐ No	
Information Security	Technical Security Countermeasures Plan	☐ Yes ☐ No	☐ Yes ☐ No	
	TEMPEST Plan	☐ Yes ☐ No	☐ Yes ☐ No	
Computer Security	Master ADP Security Plans	☐ Yes ☐ No	☐ Yes ☐ No	
	Individual Personal Computer Security Plans	☐ Yes ☐ No	☐ Yes ☐ No	

TOPIC AREA	PLAN	PLAN EXISTS?	PLAN ADEQUATE?	REVIEWER COMMENTS
Survey Program	Survey Program Procedures	☐ Yes ☐ No	☐ Yes ☐ No	
Operations Security (OPSEC)	OPSEC Program Plan	☐ Yes ☐ No	☐ Yes ☐ No	
Corrective Action Plan (CAP)	Corrective Action or Issue Management Plans	☐ Yes ☐ No	☐ Yes ☐ No	

Tool 2-3

PLAN EVALUATION WORKSHEET FOR PROTECTION PROGRAM MANAGEMENT

Plan: _____ Date of Evaluation: _____

Date of Plan: _____ Last Reviewed: _____ Evaluation Team: _____

EVALUATION ELEMENT	SECTION(S)	PAGES(S)	DEPTH OF COVERAGE	REVIEWER COMMENTS
Goals and Objectives			☐ Sufficient ☐ Insufficient	
General Approach			☐ Sufficient ☐ Insufficient	
Task Definition			☐ Sufficient ☐ Insufficient	
Priority of Tasks			☐ Sufficient ☐ Insufficient	
Task Linkages			☐ Sufficient ☐ Insufficient	
Identification of Resources			☐ Sufficient ☐ Insufficient	

EVALUATION ELEMENT	SECTION(S)	PAGES(S)	DEPTH OF COVERAGE	REVIEWER COMMENTS
Functions, Responsibilities, and Authorities			☐ Sufficient ☐ Insufficient	
Milestones and/or Products Defined			☐ Sufficient ☐ Insufficient	
Plan Modification Methodology			☐ Sufficient ☐ Insufficient	
Independent Review Mechanism			☐ Sufficient ☐ Insufficient	
Integration throughout S&S Program			☐ Sufficient ☐ Insufficient	
			☐ Sufficient ☐ Insufficient	
			☐ Sufficient ☐ Insufficient	
			☐ Sufficient ☐ Insufficient	

Tool 2-4

SAFEGUARDS AND SECURITY PLAN
DETAILED REVIEW

	SSSP DATA COLLECTION QUESTIONS	YES	NO
1.	**Has the SSSP been recently approved by the Operations/Site Office?**		
	If not, when was the last time it was approved?		
	What are the reasons for not having an approved SSSP?		
2.	**Is there formal evidence of an annual review?**		
	If so, how is this documented?		
3.	**Does the SSSP identify all Category I/II facilities at the site?**		
4.	**Does the SSSP discuss the potential for roll-up to Category I/II quantities from facilities located outside a Protected Area?**		
5.	**Does the SSSP identify any non-SNM critical facilities?**		
	Bio-research laboratories?		
	Critical computer facilities?		
	Large-dose radiation facilities?		
	Facilities critical to weapons production/stewardship?		
	Other? (List)		
6.	**Does the SSSP accurately describe the site's mission as well as the mission of listed facilities?**		
	If not, explain:		
7.	**Does the SSSP accurately describe and reflect the status of the Site's S&S program?**		

	SSSP DATA COLLECTION QUESTIONS	YES	NO
	If not, explain:		
8.	**Does the SSSP include a list of deviations from DOE requirements?**		
	Has the list been updated to match current requirements?		
	Have appropriate VAs been conducted to support the deviation request?		
	Comment:		
	Are there any deviations from requirements that should have been the subject of a deviation request, but weren't?		
	If so, explain:		
9.	**Are there any "non-standard" assumptions?**		
	If so, list them and the rationale the site used to justify them and whether the justification is adequate.		
10.	**Does the SSSP describe the current level of system effectiveness (risk) for each key facility and target?**		
	If no, explain:		

SSSP DATA COLLECTION QUESTIONS		YES	NO
11.	**Does the SSSP describe the change in system effectiveness (risk) resulting from proposed upgrades?**		
	Comment:		
12.	**Does the SSSP list alternatives considered and justification for recommended upgrades?**		
	Comment:		
13.	**Does the SSSP provide a schedule/plan for accomplishing the recommended upgrades?**		
14.	**Describe the process used to develop and approve the SSSP.**		

Tool 2-5

VULNERABILITY ASSESSMENT REPORT
DETAILED REVIEW

Facility:_____

VULNERABILITY ASSESSMENT QUESTIONS		YES	NO
1.	**Are VAs based on the current Design Basis Threat (DBT) statement?**		
	• If not, why?		
2.	**Adversary Acts:**		
	• Theft of SNM?		
	• Radiological sabotage?		
	• Critical mission curtailment?		
	• Weapons of Mass Destruction (WMD)?		
	• Other:		
3.	**Do VAs address the following aspects of the DBT:**		
	• Terrorists acting alone?		
	• Terrorists colluding with a passive insider?		
	• Terrorists colluding with an active insider?		
	• Terrorists colluding with a violent insider?		
	• Criminals acting alone?		
	• Criminals colluding with a passive insider?		
	• Criminals colluding with an active insider?		
	• Criminals colluding with a violent insider?		
	Explain any outsider threats that were not analyzed:		
	• Active non-violent insiders?		
	• Active violent insiders?		

	VULNERABILITY ASSESSMENT QUESTIONS	YES	NO
	Explain any insider threats that were not analyzed:		
4.	**How does the site define "insiders"?**		
5.	**Does the site have a Human Reliability Program (HRP)?**		
6.	**To whom does it apply?**		
	• Those with routine unescorted access to the Material Access Area?		
	• Those with "hands on" access to SNM?		
	• Those with routine unescorted access to the Protected Area?		
	• Armed Protective Force members?		
	• Central Alarm System/Secondary Alarm System operators?		
	• Critical protective force support personnel, e.g., armorers, technicians?		
7.	**Are there individuals with routine access to the Protected Area who are not enrolled in the HRP?**		
8.	**Are there individuals with routine access to the Material Access Area who are not enrolled in the HRP?**		
9.	**Does the site use HRP to mitigate violent or active insiders?**		
	• If yes, do they mitigate before they analyze?		
10.	**Does the site use the full spectrum of the Adversary Capability List?**		
	• If no, provide rationale.		
11.	**Did the site consider/analyze the following types of scenarios?**		
	• Overt attack?		
	• Airborne insertions?		
	• Airborne extractions?		
	• Trojan horse strategies?		
	• Emergency vehicle access?		
	Comment:		

	VULNERABILITY ASSESSMENT QUESTIONS	YES	NO
12.	**Did the insider/outsider collusion analysis include the following types of scenarios?**		
	• Insider actively circumventing or disabling protective system elements?		
	• Insider using violence?		
	• Insider removing material from authorized location?		
	Comment:		
13.	**Did insider scenarios consider the following strategies?**		
	• Piggybacking on waste shipments?		
	• Falsifying shipping records?		
	• Building evacuations?		
	• Emergency crash-out?		
	• Piggybacking on non-radiological shipments/transfers?		
	Comment:		
14.	**Does the site move Category I or II quantities of SNM between facilities?**		
15.	**Did the site analyze transportation-related scenarios?**		
16.	**What methodology was used for the VAs?**		
	• ASSESS/ATLAS?		
	• VISA?		
	• Other computerized method?		
	• Other qualitative/expert opinion?		

Tool 2-6

ASSESS/ATLAS
FACILITY CHARACTERIZATION FILES
DETAILED REVIEW

1. Select a sample of facility files to review.

2. Review either each protection element in the model or a representative sample of protection elements, focusing on those that are on the "worst case" pathways, but also looking at protection elements that are not on the "worst case" path to determine why they were not selected.

3. Complete the following table for each element reviewed.

ASSESS/ATLAS FACILITY CHARACTERIZATION FILES
DETAILED REVIEW

Facility:_____ File Name:_____ Last Update: _____

FACILITY CHARACTERIZATION	
Element Type:	
Element Name:	
Location:	
Concerns:	*Describe Concern*
• Dimensions	
• Characteristics	
• Passage	
- Vehicles	
- Personnel	
- Materials	
• Safeguards	
- Access Control	
Evidence Files	File/Document Name: Date: Location: Comment:
- Contraband Detection	
Evidence Files	File/Document Name: Date: Location: Comment:
- SNM Detection	
Evidence Files	File/Document Name: Date: Location: Comment:
- Material Transfers	
Evidence Files	File/Document Name: Date: Location: Comment:

FACILITY CHARACTERIZATION	
- Intrusion Detection	
Evidence Files	File/Document Name: Date: Location: Comment:
- Access Delay	
Evidence Files	File/Document Name: Date: Location: Comment:
- Security Inspectors	
Evidence Files	File/Document Name: Date: Location: Comment:
General Comments	

Tool 2-7

ASSESS/ATLAS OUTSIDER ANALYSIS
DETAILED REVIEW

FACILITY:	**FILE NAME:**
RFT:	**ADVERSARY:**
STATE:	**STRATEGY:**
Describe the Critical Path *(highlight Critical Decision Path)*	Describe the tactic used to defeat element
•	
•	
•	
•	
•	
•	
•	
•	
•	
•	
Describe any direct settings/overrides?	Comment:
•	
Evidence Files	File/Document Name: Date: Location: Comment:
•	
•	
•	
•	
Evidence Files	File/Document Name: Date: Location: Comment:
Comment/Concern:	

Tool 2-8

ASSESS/ATLAS INSIDER FILE
DETAILED REVIEW

FACILITY:	FILE NAME:	YES	NO
Review Personnel List			
	Does it accurately portray the types/classes of personnel with access to the facility?		
	If no, describe categories that are missing:		
	•		
	•		
	•		
Review Access & Authority Table			
	Does it accurately portray the situation at the facility?		
	If no, describe apparent discrepancies:		
	•		
	•		
Review Key List			
	Does it accurately portray the situation at the facility?		
	If no, describe apparent discrepancies:		
	•		
	•		
Review the Adversary Strategies			
	Are there any Personnel Types whose strategies appear questionable?		
For each questionable Personnel Type, complete the actions below:			
Describe the Critical Path	Describe the tactic used to defeat element. Is the tactic justified? (YES/NO)		
•			
•			
•			
•			
•			
•			
•			
•			
•			
•			
Describe any direct settings/overrides?	Comment:		
•			

FACILITY:	**FILE NAME:**	**YES**	**NO**
Evidence Files	File/Document Name: Date: Location: Comment:		
•			
•			
•			
•			
Evidence Files	File/Document Name: Date: Location: Comment:		
Comment/Concern:			

Tool 2-9

JTS/JCATS NEUTRALIZATION ANALYSIS

1. Review any background data on the process used to develop and conduct scenarios.

2. Review the process used to calculate Probability of Neutralization.

3. Review replays of a sample of the scenario runs conducted by the facility; ensure that at least one of every type of scenario is reviewed.

4. For each replay reviewed, complete the following form.

FACILITY:		**FILE NAME:**	
NUMBER OF ADVERSARIES:		**NUMBER OF PROTECTIVE FORCE:**	
NUMBER OF ADVERSARY TERMINALS:		**NUMBER OF PRO-FORCE TERMINALS:**	
DESCRIBE ADVERSARY STRATEGY:			
DESCRIBE EXPECTED PRO-FORCE RESPONSE:			
QUESTIONS		**YES**	**NO**
1.	Were there any special modifications to account for model limitations?		
	Describe:		
2.	Does the Pro-Force weapons load reflect actual conditions?		
	If not, explain:		
3.	Does the Pro-Force deployment reflect actual conditions?		
	If not, explain:		
4.	Is the Adversary weapons load consistent with the approved Adversary Capabilities List (ACL)?		
	If not, explain:		
5.	Does the amount and type of ammunition assigned to each unit seem reasonable?		
	If not, explain:		
6.	Were Pro-Force tactics consistent with training?		
	If not, explain:		
7.	Did the Pro-Force respond in a coordinated fashion to the attack?		
	If not, explain:		
8.	Did the Adversary make good use of force multipliers?		
	If not, explain:		
9.	Was the Adversary attack well planned and coordinated?		
	If not, explain:		
10.	Was the Adversary appropriately aggressive?		
	If not, explain:		

FACILITY:	**FILE NAME:**	
NUMBER OF ADVERSARIES:	**NUMBER OF PROTECTIVE FORCE:**	
NUMBER OF ADVERSARY TERMINALS:	**NUMBER OF PRO-FORCE TERMINALS:**	
DESCRIBE ADVERSARY STRATEGY:		
DESCRIBE EXPECTED PRO-FORCE RESPONSE:		
General Comments/Observations:		

Tool 2-10

TABLETOP/QUALITATIVE EVALUATIONS

1. Review any documentation that describes the process.

2. Review any evidence files related to the evaluation.

FACILITY:	**STATE:**	**DATES OF EVALUATION:**	
ADVERSARY OBJECTIVE:			
TYPE OF ADVERSARY:	**NUMBER OF ADVERSARIES:**	**NUMBER OF PRO-FORCE:**	**PRO-FORCE RESPONSE STRATEGY:**

	QUESTIONS	**YES**	**NO**
1.	Describe the criteria used to identify scenarios:		
2.	Do the scenarios appear realistic and challenging to the facility?		
	If not, explain:		
3.	Are scenario assumptions well documented?		
	File/Document Name: Date: Location: Comment:		
4.	Was there representation from all stakeholders on the evaluation team?		
	If not, explain:		
5.	Are facility characteristics consistent with reality?		
	If not, explain:		
6.	Does the Pro-Force deployment reflect actual conditions?		
	If not, explain:		
7.	Is the Adversary weapons load consistent with the approved ACL?		
	If not, explain:		
8.	Does the amount and type of ammunition assigned to each unit seem reasonable?		
	If not, explain:		
9.	Were Pro-Force tactics consistent with training?		
	If not, explain:		
10.	Did the Pro-Force respond in a coordinated fashion to the attack?		
	If not, explain:		
11.	Was the facility response consistent with policy and training?		
	If not, explain:		
12.	Did the Adversary make good use of force multipliers?		
	If not, explain:		
13.	Was the Adversary attack well planned and coordinated?		
	If not, explain:		

FACILITY:	**STATE:**	**DATES OF EVALUATION:**	
ADVERSARY OBJECTIVE:			
TYPE OF ADVERSARY:	**NUMBER OF ADVERSARIES:**	**NUMBER OF PRO-FORCE:**	**PRO-FORCE RESPONSE STRATEGY:**

	QUESTIONS	**YES**	**NO**
14.	Was the Adversary appropriately aggressive?		
	If not, explain:		

General Comments/Observations:

Tool 2-11

VULNERABILITY ASSESSMENT
SUMMARY ANALYSIS TABLE

	N/A*	A	M	I	REMARKS
THREAT ANALYSIS					
Outsider					
- Number of Adversaries					
- Equipment/Weapons					
- Goals/Objectives					
- Assumptions					
Insider					
- Non-violent					
- Violent					
- Assumptions					
FACILITY CHARACTERIZATION					
Protected Area					
- Access Controls					
- Intrusion Detection					
- Delay					
- Pro-Force Deployment					
Target Building					
- Access Controls					
- Intrusion Detection					
- Delay					
- Pro-Force Deployment					

* N/A = Not Applicable A = Adequate M = Marginal I= Inadequate

	N/A*	A	M	I	REMARKS
Target					
- Access Controls					
- Intrusion Detection					
- Delay					
- Pro-Force Deployment					
Evidence Files/Support Documentation					
- Currency					
- Relevance					
- Accessibility					
PATH/STRATEGY ANALYSIS					
Outsider					
- Response Force Time Support					
- Strategies					
- Non-viable Pathways					
- User-defined Settings					
Outsider/Insider Collusion					
- Assumptions					
- Strategies					

	N/A*	A	M	I	REMARKS
Non-violent Insider					
- Personnel Characterization					
- Assumptions					
- Strategies					
- Capabilities					
- User-defined Settings					
Violent Insider					
- Personnel Characterization					
- Assumptions					
- Strategies					
- Capabilities					
- User-defined Settings					
NEUTRALIZATION ANALYSIS					
Process					
- Use of "standardized" databases					
- Method for dealing with undefined weapons characteristics					
- Modeling center setup					
- Method for determining probability of neutralization (Pn)					
Adversary Tactics					
- Compatibility w/ASSESS/ATLAS scenarios					
- Level of creativity					
- Use of resources					

	N/A*	A	M	I	REMARKS
Protective Force Tactics					
- Compatibility w/existing tactical response plans					
- Use of resources					
- Compatibility w/normal operations and training					
CALCULATION OF SYSTEM EFFECTIVENESS VALUES					
- Use of standard methodology					
- Justification for variance					
TABLETOP/QUALITATIVE ASSESSMENTS					
Process					
- Methodology for scenario development					
- Composition of Evaluation Team					
- Compatibility with DBT					
- Compatibility with Pro-Force capabilities/training/ deployment					
- Conduct of evaluation					

CONCLUSION: Are Vulnerability Assessments adequate? _____ YES
_____ MARGINAL
_____ NO

* N/A = Not Applicable A = Adequate M = Marginal I= Inadequate

This page intentionally left blank.

TOOLS RELATED TO SECTION 3, ORGANIZATION AND STAFFING

Tool 3-1

ORGANIZATION AND STAFFING
GENERAL DATA COLLECTION QUESTIONS

Person Interviewed: _____ Interviewer:_____

Organization: _____ Date: _____

GENERAL QUESTIONS	NOTES
• Describe your responsibilities for the protection program.	
• Who do you interact with on a daily (weekly, monthly) basis?	
• Do you interact primarily with the Site Office or a Program Office?	

GENERAL QUESTIONS	NOTES
• Are you satisfied with the way the program is running?	
• What have you tried to change, but been unable to accomplish?	
• What is your opinion on the support provided to you by the existing S&S organizational structure?	

GENERAL QUESTIONS	NOTES
• Is your S&S organization and staff adequate to support you in managing the protection program?	

Tool 3-2

ORGANIZATION AND STAFFING
SPECIFIC DATA COLLECTION QUESTIONS

Person Interviewed: _____ Interviewer:_____

Organization: _____ Date: _____

SPECIFIC QUESTIONS (*With Indicators of Performance*)	**NOTES**
• Has management established an effective and efficient organizational structure? - *Authority, responsibility, and duties clearly defined and assigned?* - *Span-of-control, parallelism, delegation of authority, and flexibility considered?* - *Satisfied with organizational structure?* - *Satisfied with organizational level of the safeguards and security function?*	
• Has management established an effective and efficient organizational structure? - *Frequent changes to the structure?* – *Frequent changes to the structure?* - *Undue reliance on the use of informal lines of communication?* - *Excessive use of working groups?* - *Lines of communication, accountability, and authority clear?*	

SPECIFIC QUESTIONS (*With Indicators of Performance*)	**NOTES**
- *Personnel familiar with assigned responsibilities, authority, and accountability?*	
• Has management established an effective and efficient organizational structure? - *Documented and promulgated?* - *Organizational levels appropriate?* - *Lack of visibility or support?* - *Organization review process in place* - *Significant differences in workload?* - *Persons with safeguards and security responsibilities is an "isolated" office?*	
• Are staffing levels adequate to support the structure and fulfill functional requirements? - *Excessive use of paid and uncompensated overtime?* - *Budget or personnel restrictions?* - *Contractor/(sub) or consultant support?* - *Permanent replacement for support positions?*	
• Are staffing levels adequate to support the structure and fulfill functional requirements? - *Excessive use of working groups?* - *Actual duties and job description same?*	

SPECIFIC QUESTIONS (*With Indicators of Performance*)	**NOTES**
- *Job descriptions reviewed and current?* - *Supervisor to supervised ratio reasonable?*	
• Are staffing levels adequate to support the structure and fulfill functional requirements? - *Vacant positions over extended periods?* - *Frequently missed internal and external suspense dates?* - *Contractor/subcontractor staff support necessary? Used effectively?* - *Significant backlogs of work attributed to a shortage of personnel?*	
• Are personnel qualified and trained for their position? - *Is recruiting a problem?* - *Contractor provides trained personnel in accordance with the contract and order provisions?*	

SPECIFIC QUESTIONS (*With Indicators of Performance*)	**NOTES**
• Are personnel qualified and trained for their position? - *Training records maintained and current?* - *Current formal training plan in place?* - *Plan includes short- and long-term training requirements?*	
• Are personnel qualified and trained for their position? - *Mandatory training requirements fulfilled?* - *All required certification completed?* - *National Training Center (NTC) courses and assistance utilized?* - *Contractor personnel adequately trained?*	

Tool 3-3

ORGANIZATION AND STAFFING
DOE SUMMARY EXTRACTS

REFERENCE	SUMMARY EXTRACT
ORGANIZATIONAL STRUCTURE	
Office of Personnel Management (OPM) Standard TS-107	Federal managers have the responsibility to organize work to accomplish the agency's mission in the most efficient and economical manner. The policy of the Federal Government is to assign work in a way that will make optimum use of available resources.
OPM Guide HRCD-5	Managers are responsible for designing organizations and structuring positions and functions in a manner that optimizes efficiency, economy, productivity, and organizational effectiveness.
DOE Order 470.1, 5.a.(1).(a).1	(Secretarial Officers) Ensure adequate protection is afforded safeguards and security interests.
DOE Order 470.1, 5.a.(1)	(Secretarial Officers) Provide program and project direction consistent with the Safeguards and Security directives and policy requirements.
DOE Order 471.2A, Attachment 1,5.a	Maintain a clear chain of responsibility for information security within each organization.
PERSONNEL STAFFING	
OPM Guide HRCD-5	Work leaders lead three or more employees.
OPM Guide HRCD-5	Team leaders identify, distribute, and balance workload and tasks among employees in accordance with established work flow, skill level, and/or occupational specialization; making adjustments to accomplish the workload in accordance with established priorities to ensure timely accomplishment of assigned team tasks; and ensuring that each employee has an integral role in developing the final team product.
OPM Standard TS-107	A position description is a statement of major duties, responsibilities, and supervisory relationships of a given position. The description of each position must be kept up-to-date and include information about the job that is significant to its classification.
DOE Order 470.1, 5.a.(5)	(Secretarial Officers) Ensure that safeguards and security budget proposals are adequate, and that resources are provided to implement them.
DOE Order 470.1, 5.j	Heads of field elements shall ensure that all operations under their jurisdiction are implemented consistent with acceptable safeguards and security practices and in accordance with Safeguards and Security directives.

REFERENCE	SUMMARY EXTRACT
PERSONNEL QUALIFICATIONS AND TRAINING	
DOE Order 360.1B, 5.k.(3)	(Managers, Supervisors, and Employees) Ensure timely request, approval authorization, and notification of training.
DOE Order 470.1, 5.b.(1).(h).8	(Office of Security) Ensure development, conduct, and management of an effective Safeguards and Security Training Program.
DOE Order 470.1, Chapter II, 3.g	Training shall be provided to individuals to qualify or improve their qualifications to perform assigned safeguards and/or security tasks or responsibilities.
OPM Guide HRCD-5	Leaders are responsible to instruct employees in specific tasks and job techniques and make available written instructions, reference materials, and supplies, and to provide on-the-job training to new employees in accordance with established procedures and practices.
DOE Order 360.1B, 5.(k).(5)	(Managers, Supervisors, and Employees) Review and maintain the accuracy of training records, and document performance requirements and competencies related to training.
DOE Order 470.1, Chapter II, 3.l	The National Training Center, DOE Elements, and covered contractors shall implement a standardized training records management system.
DOE Order 473.2, 4.b	Protective forces must be provided training, equipment, and resources to ensure effective performance of assigned functions and tasks under both normal and emergency conditions.

Tool 3-4

ORGANIZATION AND STAFFING
SUMMARY ANALYSIS TABLE

ORGANIZATIONAL LEVEL	N/A*	A	M	I	REMARKS
ADEQUACY OF ORGANIZATIONAL STRUCTURE					
Operations Office					
Operations Office S&S Staff					
Site Office S&S Staff					
Management and Operations (M&O) Contractor					
M&O Contractor S&S Staff					
Pro-Force Management					
ADEQUACY OF STAFFING LEVEL					
Operations Office S&S Staff					
Site Office S&S Staff					
M&O Contractor S&S Staff					
Pro-Force Management					
ADEQUACY OF STAFF QUALIFICATION AND TRAINING					
Operations Office S&S Staff					
Site Office S&S Staff					
M&O Contractor S&S Staff					
Pro-Force Management					
CONCLUSION: Is organization and staffing adequate?					_____ YES _____ MARGINAL _____ NO

* N/A = Not Applicable A = Adequate M = Marginal I= Inadequate

TOOLS RELATED TO SECTION 4, BUDGET PROCESS

Tool 4-1

BUDGET PROCESS
DATA COLLECTION QUESTIONS

Person Interviewed: _____ Interviewer:_____

Organization: _____ Date: _____

SPECIFIC QUESTIONS	NOTES
What are the assumptions and guidance under which the budget was formulated?	
Are these assumptions and this guidance consistent with commitments made in the SSSP and in corrective action plans?	
Do you believe that the S&S program is adequately funded?	

SPECIFIC QUESTIONS	NOTES
What is your role in supporting or approving funding for S&S activities?	
How do you determine that S&S resource requests reflect actual requirements?	
How do you prioritize S&S budget requests relative to other expense elements within your budget?	

SPECIFIC QUESTIONS	NOTES
How do you determine that actual S&S expenditures follow budgeted expenditure levels and are spent on the appropriate S&S projects?	
How would you provide resources to correct a serious weakness discovered during this inspection?	
What are your major S&S expense items?	

SPECIFIC QUESTIONS	NOTES
What is the current funding status of each?	
What reasons might be given to an inspector if the review of the budget identified S&S projects that never seem to make it to the "funded" stage or if funded projects fail to get completed in a reasonable period of time?	

SPECIFIC QUESTIONS	NOTES
Will there be uncosted obligations or unobligated funds for any S&S line item at the end of the fiscal year?	
Will there be uncosted obligations or unobligated funds for any programs funding significant S&S activities at the end of the fiscal year? Will you have any influence over the allocation of those funds during the next fiscal year?	

Tool 4-2

BUDGET PROCESS
BUDGET STRUCTURE WORKSHEET

Appropriation _____ Subdivision _____

Fund Category: _____ Site/Facility _____

ACTIVITY DESCRIPTION	**EXPENSE TYPE** (Operating, Construction, GPP, etc.)	**HEADQUARTERS PROGRAM OFFICE**	**BEGINNING FISCAL YEAR** (use * for continuing project)	**COMPLETION FISCAL YEAR** (leave blank for continuing project)	**TOTAL COST** (leave blank for continuing project)	**CURRENT FISCAL YEAR BUDGET**

Tool 4-3

BUDGET PROCESS
SUMMARY ANALYSIS TABLE

	N/A*	A	M	I	REMARKS
BUDGET PREPARATION					
VAs are used to support protection system changes					
Level of site personnel involvement					
Level of field element involvement					
BUDGET EXECUTION					
Site Level Expenditure Monitoring					
Field Element Expenditure Monitoring					
CONCLUSION: Is budgeting adequate?					_____ YES _____ MARGINAL _____ NO

* N/A = Not Applicable A = Adequate M = Marginal I= Inadequate

This page intentionally left blank.

TOOLS RELATED TO SECTION 5, PROGRAM DIRECTION

Tool 5-1

PROGRAM DIRECTION
GENERAL DATA COLLECTION QUESTIONS

Person Interviewed: _____ Interviewer:_____

Organization: _____ Date: _____

GENERAL QUESTIONS	NOTES
• Is the program direction provided to you from higher levels of the organization adequate for your needs?	
• Do you receive informal program direction from higher levels that you feel obligated to comply with?	
• What program direction related initiatives have you attempted to change but been unable to accomplish?	

GENERAL QUESTIONS	NOTES
• What do you consider your greatest challenge in fulfilling your responsibility for providing direction to the S&S program?	
• Are requirements and guidance received, translated into site-specific guidance, and transmitted in a consistent and timely fashion?	

Tool 5-2

PROGRAM DIRECTION
SPECIFIC DATA COLLECTION QUESTIONS

Person Interviewed: _____ Interviewer:_____

Organization: _____ Date: _____

SPECIFIC QUESTIONS *(Performance Criteria)*	**NOTES**
• Has management effectively established program direction? - *Documented and current?* - *Coordinated by and promulgated from appropriate offices?* - *Contradictory direction?* - *Direction received and understood by subordinates?* - *DOE requirements accurately translated?*	
• SSSPs and other plans approved? - *Affected Security Officers aware of status and content?* - *Documents serve their intended purposes?*	
• Deviations to policy properly processed for approval? - *Timely identification of need for a deviation?* - *Approved by correct office?* - *Documented in SSSP?* - *Equivalent measures have been implemented?*	

SPECIFIC QUESTIONS *(Performance Criteria)*	**NOTES**
• Is there adequate delegation of authority? – *Subordinates contribute?* – *Policy stalled at top?* – *Delegation documented?* – *Evidence of participatory management?*	
• Does program administration support program direction? – *Change procedure timely and efficient?* – *Documents current?* – *Evidence of goals, objectives, and schedules?* – *Control of direction materials effective and documented?*	

Tool 5-3

PROGRAM DIRECTION
DOE SUMMARY EXTRACTS

REFERENCE	SUMMARY EXTRACT
HEADS OF HEADQUARTERS ELEMENTS	
DOE Order 470.1, 5.a.(1).(a).1	(Secretarial Officers) Ensure adequate protection is afforded safeguards and security interests.
DOE Order 470.1, 5.a.(1)	(Secretarial Officers) Provide program and project direction consistent with Safeguards and Security directives and policy requirements.
DOE Order 470.1, 5.a.(9)	(Secretarial Officers) Approve Site Safeguards and Security Plans and annual revisions thereto.
DOE Order 470.1, 5.a.(6)	(Secretarial Officers) Participate in the development and review of policy and standards for safeguards and security interests.
OFFICE OF SECURITY POLICY	
DOE Order 470.1, 5.b.(a)	Establish S&S policies, requirements, standards, and guidance for DOE operations, including DBT, for use in designing and implementing DOE protection programs.
DOE Order 470.1, 5.b.(c)	Approve all SSSPs and participate in validation and verification reviews at field sites.
HEADS OF FIELD ELEMENTS	
DOE Order 470.1, j	Heads of field elements shall ensure that all operations under their jurisdiction are implemented consistent with acceptable safeguards and security practices and in accordance with Safeguards and Security directives.
ALTERNATIVE MEANS AND DEVIATIONS	
DOE Order 470.1, 4.f.(1).(a)	Variances shall be approved by the head of a field element. The Office of Security and appropriate program officers shall be notified.
DOE Order 470.1, 4.f.(2).(c)	A waiver shall not exceed two years. Extensions may be requested using the same process.
DOE Order 470.1, 4.f.(3).(c)	Exceptions shall not exceed three years. Extensions may be requested using the same process.

Tool 5-4

PROGRAM DIRECTION
SUMMARY ANALYSIS TABLE

ORGANIZATIONAL LEVEL	N/A*	A	M	I	REMARKS
PROGRAM POLICY EMPHASIS					
DOE Office of Security Policy					
Security Officers					
Staff					
PROGRAM DIRECTION EMPHASIS					
Operations Office					
Operations Office Safeguards and Security Director (SSD)					
Site Office					
Site SSD Staff					
PROGRAM IMPLEMENTATION EMPHASIS					
Operating Contractor					
Operating Contractor SSD					
Pro-Force Contractor					
Pro-Force Contractor Staff					
CONCLUSION: Is program direction adequate?					_____ YES _____ MARGINAL _____ NO

***** N/A = Not Applicable A = Adequate I = Inadequate M = Marginal

TOOLS RELATED TO SECTION 6, CONTROL SYSTEMS

Tool 6-1

CONTROL SYSTEMS
GENERAL DATA COLLECTION QUESTIONS

Person Interviewed: _____ Interviewer:_____

Organization: _____ Date: _____

GENERAL QUESTIONS	NOTES
• Please describe your responsibilities for the protection program.	
• Are you satisfied with the way the program is running?	
• Who do you interact with on a daily (weekly, monthly) basis?	
• Do you deal mainly with the Headquarters program office or a local staff member?	
• Is there a cost plus award fee contract in place that includes or should include S&S performance objectives?	
• What is your opinion on the management oversight and feedback support provided you by the existing system of control measures? Is it effective?	
• What would you like to see changed?	
• Are your present control systems and associated staff and facilities adequate to assist you in managing the protection program?	
• What have you tried to change but been unable to accomplish?	

Tool 6-2

CONTROL SYSTEMS
SPECIFIC DATA COLLECTION QUESTIONS

Person Interviewed: _____ Interviewer:_____

Organization: _____ Date: _____

SPECIFIC QUESTIONS *(Performance Criteria)*	**NOTES**
• Are survey, inspection, and self-assessment programs in place to determine the effectiveness of the S&S program on a recurring basis? – *Documented and promulgated?* – *Responsibility and accountability clear?* – *Personnel understand responsibilities?* – *Programs comply with DOE orders?* – *Provide adequate feedback?* – *Organization and staffing adequate?*	
• Is the interface between the control systems at the Headquarters, Operations Office, and contractor levels adequate? – *Redundant systems within the organizational levels?* – *Higher level developed information available to lower levels?* – *Headquarters direction adequate to develop integrated systems?*	

SPECIFIC QUESTIONS *(Performance Criteria)*	**NOTES**
• Are there internal (self-directed) control systems in place that supplement the mandatory control system programs? – *Determine if any exist* – *Are they productive and efficient?* – *Are there redundant reporting systems?* – *Is there an unfulfilled need for a self-directed control system(s)?*	
• Is there an effective system for identifying, tracking, and bringing to timely closure deficiencies noted in surveys, inspections, self-assessments, and self-directed control systems? – *Is there a tracking system?* – *Properly implemented and effective?* – *Provides timely and useful information?* – *System properly documented?* – *Contains all necessary information?* – *Accountability is assigned?* – *Integrated to prevent redundant reporting?*	
• Are reports developed by the control systems provided to the appropriate organizational level to ensure proper management attention? – *Positive identification of S&S issues?* – *Thorough internal distribution of reports?* – *Priorities assigned by system?*	

SPECIFIC QUESTIONS *(Performance Criteria)*	**NOTES**
– *Format clear, concise, and effective?* – *Reports distributed to permit use in correcting common problems?* – *Reports reviewed by top management when appropriate?*	

Tool 6-3

CONTROL SYSTEMS
DOE SUMMARY EXTRACTS

REFERENCE	SUMMARY EXTRACT
DOE Order 470.1, Chapter III,3.a; Chapter IX,1; and Chapter X, 3.a	Performance assurance programs shall provide for operability and effectiveness tests of systems and/or components of systems. The adequacy of safeguards and security measures shall be validated through various means, such as surveys conducted by the DOE Surveying Office. Self-assessment programs shall be conducted and documented for all approved facilities.
DOE Order 470.2B, 5.(a).(5)	(Office of Independent Oversight) Directs, manages, and conducts the safeguards and security; cyber security; emergency management; and environment, safety, and health independent oversight programs.
DOE Order 470.2B, 5.(a).(2) & (3)	(Office of Independent Oversight) Advises appropriate site and Headquarters managers promptly (within 24 hours) of major vulnerabilities or imminent danger identified during appraisal activities at evaluated sites. Briefs senior DOE officials, including the NNSA Administrator, Under Secretary, cognizant secretarial officers (CSOs), the Office of Security, DOE policy organizations, and the managers of DOE sites on the results of appraisal activities.
DOE Order 470.2B, Attachment 2, 5	The contractor shall prepare, implement, and track to completion approved corrective action plans that address findings identified during the appraisals on the effectiveness of safeguards and security, cyber security, emergency management, and environment, safety and health programs.
DOE Order 470.1, Chapter X,3.c	Findings resulting from self-assessments shall be processed as follows: reviewed during the surveys by the Surveying Office; addressed by facility/organization management through a documented corrective action plan; and reviewed and the status of findings tracked until closed.
DOE Order 470.1, Chapter III, 4.a.(3)	Addressing unsatisfactory results of performance assurance activities, how they are to be captured in the site corrective action program, and how corrections will be implemented.

REFERENCE	SUMMARY EXTRACT
DOE Order 470.1, Chapter IX, 10.a & b	A. When a survey contains findings, the surveyed organization shall submit a response identifying corrective actions(s) for each finding to the Responsible Office and Surveying Office no later than 30 working days after formal receipt of findings. The corrective action(s) should be based on documented root cause analysis, risk assessment, and cost-benefit analysis. B. When a survey indicates a composite rating of satisfactory but contains findings requiring corrective action, the Lead Responsible Office shall enter the findings and status of corrective actions in the Safeguards and Security Information Management System and quarterly provide electronic status notification to the Office of Security, the appropriate Secretarial Officers, and the Surveying Office (if appropriate).
DOE Order 470.1, Chapter IX,7.c	Within 60 working days after final closeout of the survey, the Surveying Office shall distribute the final survey report to all Departmental Elements with a registered activity and to all appropriate Headquarters Elements.
DOE Order 470.1, Chapter IX, 10.f	A finding associated with a significant vulnerability shall not be closed until associated corrective action has been completed and the Office of Security and Security Officers are notified.
DOE Order 470.1, Chapter III, 1	A safeguards and security self-assessment program shall be implemented to ensure internal monitoring of compliance and performance with safeguards and security requirements.
DOE Order 471.2A, Attachment 1,5.g	Ensure (contractor) management is involved in and supports all aspects of information security. This involvement and support shall be demonstrated by regular visits to and inspections of information security operations to ensure that operations meet existing standards and policies.
DOE Order 471.2A, 5.b.(8).(c)	(Heads of field elements) Conduct appropriate surveys and self-assessments to ensure effective implementation.
DOE Order 471.2-1C,7.e	(CMPC Managers) Observing and reporting (e.g., security incidents involving classified information, inspection and survey results, self-assessment results, unauthorized disclosures, standards reports, etc.); developing standards and criteria for self-assessments; evaluating both the CMPC program and the program employees; conducting self-assessments; measuring results; and developing and completing corrective actions.
SAGD[1] 3.3.2	The self-assessment tracking system should account for all deficiencies and ideally be integrated into a sitewide or organizational tracking system.
3.3.5	Corrective action verification and validation shall be tracked on a formal system. Issue status reports of corrective actions periodically and present them to top management.

[1] DOE *Self-Assessment Tool Kit*.

Tool 6-4

CONTROL SYSTEMS
SUMMARY ANALYSIS TABLE

ORGANIZATIONAL LEVEL	N/A*	A	M	I	REMARKS
PROGRAMS FOR CONTROL SYSTEMS IN PLACE					
Site Office					
Operating Contractor					
Pro-Force Contractor					
EFFECTIVE CRITICAL ISSUE TRACKING SYSTEM					
Site Office					
Operating Contractor					
Pro-Force Contractor					
CONTROL SYSTEM FEEDBACK PROPERLY REVIEWED					
Site Office					
Operating Contractor					
Pro-Force Contractor					
CONCLUSION: Are the control systems adequate?					_____ YES _____ MARGINAL _____ NO

* N/A = Not Applicable A = Adequate M = Marginal I = Inadequate

This page intentionally left blank.

DATA COLLECTION FORM

DATA COLLECTION FORM (U)

(U) Date: _____ **(U) Team Member**_____

(U) Site-Year-Topic-Sequence Number _____
(U) (example: SRS-01-PS-001)

(U) Subject: *Identify* the topic sub-element that these results are related to (planning, organization and staffing, budget process, program direction, or control systems).

(U) Results: *Briefly* summarize the data collected during a specific data collection activity, i.e., interview, document review, file reviews, or performance test. This ***should not be a verbatim*** account of data collection results, but a roll-up of the collected facts—**an initial analysis**.

(U) Impact: *Briefly* discuss the potential impact on this element of protection program management as it contributes to the overall protection program. If a series of issues that could impact ratings have been identified, then their collective impact should be discussed here.

(U) Need for Additional Information: *Briefly* state the need to collect additional information and what data collection activity will be conducted to meet this need. If none, then state accordingly.

This page intentionally left blank.

INSTRUCTIONS FOR COMPLETING AN ISSUE FORM

INSTRUCTIONS FOR COMPLETING AN ISSUE FORM (U)

(U) The purpose of this form is to convey the inspection team's understanding of a concern that could impact the rating, to solicit site management's position on this concern, and to describe actual/proposed mitigating actions. The form may also be used to assist in resolving other communications problems. Issue Forms can be of any length. Portion markings are required when the form contains classified information. Portion markings have been provided but may need to be modified depending on the classification of the text. Topic Team Leaders and applicable site personnel are responsible for ensuring the completion of a classification review by an authorized derivative classifier. The pre-existing portion markings may be lined through when the form contains no classified information.

(U) Date:_____ (U) Site-Year-Topic-Sequence Number _____ (U) (example: RL-03-PS-001)

PART A (U)
1. (U) Issue: State in sufficient detail to convey to the site how and why we believe an observed condition is an issue, and state the applicable reference supporting the issue.
2. (U) Impact: Clearly state the immediate or potential impact that exists because of the issue.
(U) Approval: Topic Team Leader_____Date_____ (U) Inspection Chief_____Date_____
PART B (U)
1. (U) Site Response: The response should include the site's position on the issue and its immediate or potential impact. Supporting or additional information should be provided to substantiate this position.
2. (U) Action Taken, if appropriate: Describe any actions taken to mitigate immediate impacts or actions under consideration for future implementation. Include the rationale for these actions.
(U) Approval: Site Representative_____Date_____
(U) Receipt Acknowledged: (U) SP-41 Representative_____Date_____

This page intentionally left blank.

REPORT PREPARATION

REPORT PREPARATION

The integration of protection program management (PPM) subtopics and all other topic results should be one of the PPM topic team's primary goals throughout the inspection effort. Management should be able to read the PPM annex (i.e., the last appendix of the overall inspection report) and clearly understand the relationship between their activities and S&S program performance. The following steps will be used in the preparation of the protection program management topic appendix.

1. Throughout the draft report preparation phase, these objectives will be kept in mind:

   - Make sure the narrative supports the conclusion and is not just a catalog of the results (system description).

   - Minimize or omit issues (positive or negative) that do not support the overall conclusion.

   - Use results-oriented sub-headers to assist the reader.

   - List strengths first and then weaknesses throughout the report.

2. The assigned "principal writer" will prepare the appendix by combining the separate submissions into "one voice"; the team leader will review and make final edits.

3. Team members will provide input to the principal writer primarily in writing and verbally as requested. Data collection sheet(s) should not cover more than one subtopic or element (as needed) and must fully characterize each collection activity, the results of accumulated data, and a full analysis. Team members should prepare their assigned portions of the appendix as though writing a final product for the review board. Data for the PPM topic is often collected throughout both the planning and data collection inspection phases. Data includes:

   - Planning (VA and Performance Assurance Program)
   - Resources (Budget and Staffing, Training and Qualifications)
   - Feedback Mechanisms (Survey Program, Self-Assessment Program, and Resolution of Findings)
   - ISSM.

   The principal writer will normally complete data collection for the assigned sub-topic and begin the report draft by Wednesday of the exercise week. The other topic team members should complete their contributions by Thursday of the exercise week.

   Preparation of the draft report will be accomplished in the following manner:

Onsite Planning Phase

- Daily: The team collects data and meets to identify PPM strengths and weaknesses, and conclusions on overall effectiveness of the PPM.

Offsite Follow-up Phase

- When access to appropriate classified word processing is available, the principal writer begins drafting the report immediately after the completion of the planning phase by developing an outline of the entire report (introduction, subtopic sections, conclusion, rating, and opportunities for improvement), text for the introduction, and text for the PPM subtopic section.

- When possible, the initial draft is shared (via fax or email) with the other topic team members in sufficient time in advance of the data collection phase to allow for a revision of the draft report prior to the beginning of the data collection phase.

Onsite Data Collection Phase

- Daily: team meets to identify program strengths and weaknesses, and conclusions on overall effectiveness of the individual programs.

- Thursday: using the results of these daily meetings and data collection sheets, the principal writer begins the finalization (beginning with developing text for the principal's assigned subtopic section) of the draft report.

- Thursday: the remaining topic team member(s) continue data collection.

Onsite Close-out Phase

- Daily: team meets to identify program strengths and weaknesses, and conclusions on overall effectiveness of the individual programs.

- Thursday: using the results of these daily meetings and data collection sheets, the principal writer begins the finalization (beginning with developing text for the principal's assigned subtopic section) of the draft report.

- Thursday: all other subtopic inputs are due to the principal writer by close of business.

- Saturday: finalize the draft report, team members review for content and one team member proofreads.

- Monday: final proof reading and correction prior to submission to the management review board; the principal writer and team leader will be the primary spokespersons during the review board.

Each team member contributes to the remaining deliverables to include the list of interviews conducted, documents reviewed, data collection sheets, opportunities for improvement, and out-brief slides and bullet lists for the Inspection Team Leader and Deputy.