

INSPECTORS GUIDE

Protection Program Management



Office of Security Evaluations
Office of Independent Oversight
Office of Health, Safety and Security

October 2009

PROTECTION PROGRAM MANAGEMENT

INSPECTORS GUIDE



October 2009

**U.S. Department of Energy
19901 Germantown Road
Germantown, Maryland 20874**

Preface

As part of an effort to enhance the appraisal process, the Office of Health Safety and Security and the Office of Security Evaluations 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 Independent Oversight Appraisal Process Protocols describe the philosophy, scope, and general procedures applicable to all oversight activities. The Safeguards and Security Appraisal Process Guide describes specific procedures used 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 inspectors, it is made available to the field through the DOE homepage and may be useful to field element and facility personnel who conduct surveys or self-assessments of the protection program management topic.

Periodic revisions to this guide are envisioned in response to changes in DOE program direction and guidance, insights gained from oversight activities, and feedback from customers and constituents. Therefore, users of this process guide are invited to submit comments and recommendations.

This page intentionally left blank.

Contents

Acronyms v

Section 1: Introduction

Purpose 1-1

Organization 1-1

General Considerations 1-1

Characterization of the Protection Program Management Topic 1-2

Inspection Goals 1-3

Compliance vs. Performance 1-3

Inspection Planning Goals 1-3

Planning Decisions 1-4

Using the Topic-Specific Tools 1-4

Validation 1-6

Using the Tools in Each Inspection Phase 1-7

Section 2: Planning Process

References 2-1

General Information 2-1

Common Deficiencies/Potential Concerns 2-4

Planning Activities 2-6

Data Collection Activities 2-7

Section 3: Federal Feedback and Improvement Processes

References 3-1

General Information 3-1

Common Deficiencies/Potential Concerns 3-3

Planning Activities 3-6

Data Collection Activities 3-6

Section 4: Contractor Feedback and Improvement Processes

References 4-1

General Information 4-1

Common Deficiencies/Potential Concerns 4-3

Planning Activities 4-5

Data Collection Activities 4-5

Section 5: Program Integration

Introduction 5-1

Analysis 5-1

Integration 5-5

Integration with Other Topic Teams 5-6

Integration of PPM Subtopical Areas 5-7

Appendix A: Inspection Tool Kit and Forms A-1

This page intentionally left blank.

Acronyms

CAP	Corrective Action Plan
CIC	Classification and Information Control
CMPC	Classified Matter Protection and Control
DBT	Design Basis Threat
DOE	U.S. Department of Energy
ES&H	Environment, Safety, and Health
FOF	Force on Force
GSP	Graded Security Protection
HRP	Human Reliability Program
JCATS	Joint Conflict and Tactical Simulation
JTS	Joint Tactical Simulation
MC&A	Material Control and Accountability
NNSA	National Nuclear Security Administration
OFI	Opportunity for Improvement
PAP	Performance Assurance Program
PEP	Performance Evaluation Plan
PF	Protective Force
PPM	Protection Program Management
PS	Personnel Security
PSS	Physical Security Systems
QRB	Quality Review Board
SECON	Security Condition
SNM	Special Nuclear Material
S&S	Safeguards and Security
SSIMS	Safeguards and Security Information Management System
SSMP	Site Security Management Plan
SSP	Site Security Plan
SSSP	Site Safeguards and Security Plan
TRF	Tactical Response Force
VA	Vulnerability Assessment

This page intentionally left blank.

Section 1: Introduction

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 this 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. When used by an experienced 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. The subtopic sections are further divided into several subelements to assist the reader in understanding subtopic organization:

- Section 2 – Planning
- Section 3 – Federal Feedback and Improvement Processes
- Section 4 – Contractor Feedback and Improvement Processes.

Section 5, Program Integration, provides guidelines for analyzing data and interpreting results in the PPM topic.

The Inspection Tool Kit in Appendix A provides a series of data collection lines of inquiry, 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 470.4, *Safeguards and Security Program*, and its associated manuals. 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 experienced inspectors. Such knowledge can be enhanced and updated as inspection methods improve and 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, these inspection tools provide guidelines for prioritizing and selecting activities, analyzing data, and interpreting results.

Characterization of the Protection Program Management Topic

The overarching purpose of the protection program inspection process is to ensure that DOE tactical doctrine is implemented so that security interests are provided 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 continuous process of conducting activities relating to planning and to feedback and improvement processes. 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 prudently modifying guidance and/or resources. PPM inspections examine the effectiveness of this process.

One or more of the subtopics (i.e., planning process, Federal feedback and improvement processes, and contractor feedback and improvement processes) 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 Process subtopic, planning activities are reviewed to discern management's ability to integrate Departmental security requirements into the site mission. For example, in response to modifications to the Design Basis Threat (DBT) and Graded Security Protection (GSP), data collected in reviewing the Site Safeguards and Security Plan (SSSP) Resource Plan will reflect site efforts to address the resources necessary to meet implementation deadlines and sustain improvements. Similarly, if new equipment and procedures are introduced, inspectors would expect to find modifications in the oversight process as self-inspections, surveys, and performance assurance programs are adapted to provide assurance of the effectiveness of those elements considered essential to the security system. In another example, the inspection of the contractor's performance evaluation program might indicate incentives and awards for timely execution of system modifications that resulted in the successful implementation of tactical doctrine. This final example would require the integration of planning, physical security systems, and protective forces and illustrates how although each inspected element can stand on its own merit, an examination of only one would be insufficient to adequately describe the overall effectiveness of PPM at a facility.

Inspection Goals

The primary inspection goal is to conduct a validated, accurate investigation with a sufficient basis to determine 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 management subsystems 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 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. For example, DOE policy for the submission of deviations requires security processes proposed in lieu of DOE standards to essentially meet the same performance standard. Some sites have developed large numbers of deviations over the years while at the same time, DOE guidance has evolved. As a result, it is neither necessarily deliberate nor uncommon for a site to have a deviation in place that no longer meets DOE performance standards. For example, a barrier built many years ago may not fully comply with the tactical doctrine employment practice because it is not under sensor coverage or observation, or is not included in the protective forces weapons fire plan. Though clearly a compliance issue that must be addressed, the barrier failure is not a sufficient basis to determine whether the overall security system is still able to perform effectively. The compliance versus performance discussion is a central theme for the inspection process because the distinction is critical in helping managers prioritize the elements of the protection program they will address. The compliance versus performance distinction is an essential dialogue that facilitates managers' considerations when they must allocate scarce resources to improve the safeguards and security program.

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 objectives, namely to:

- Understand the character of and gain an appreciation for the inspected, superior, and subordinate protection program organizations, including contractors; their mission, size, and management relationships; and the environment in which the total management system and security program operate.
- Determine any specific areas requiring focus for inspection activities. For example, a research oriented site may require more emphasis on classified matter protection and control (CMPC) than material control and accountability (MC&A). On the other hand, a facility that possesses Category I special

Section 1—Introduction

nuclear material (SNM) and classified matter at the Top Secret level will require extensive emphasis in CMPC, MC&A, and classification and information control (CIC).

- Identify whether data gathering is required at a Headquarters element prior to the conduct phase of the inspection (including interviews, when appropriate).
- Produce the topic inspection plan and other necessary documents.
- Determine specific activities and assessment requirements for each member of the team, including arrival and departure dates, prior to the conduct phase of the inspection.

Planning Decisions

Based on analysis of the information gained from document reviews, 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 (this can be influenced by, among other things, past survey results, changes in DOE policy, changes in the site/facility mission, or changes in the site/facility organizational structure)
- Data required
- Data collection methods, applicable lines of inquiry, and tools to employ
- Headquarters program or other offices to be contacted for possible interview prior to onsite data gathering
- Unique document follow-on review requirements stemming from specific data-call products
- 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 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 a broad basis for evaluating the inspected program and for assigning findings. Refer to the applicable order/manual prior to interviews and tours of facilities to ensure that all relevant information is collected. An additional tool used by the PPM topic is an e-library (disk) of current and previous orders, manuals, policy memoranda, and correspondence between program and policy offices and the field that clarify policy issues or provide additional guidance on site specific concerns, individual deviations, policies, or procedures.

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, examples, and potential concerns before 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 data collection experience and expertise.

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 is acknowledgement from the organization being inspected, it compels both the inspectors and the inspected to review, discuss, and verify collected information frequently, preferably on a daily basis. Validation authenticates inspection results from the very first day of data collection and greatly contributes to the quality and acceptance of the inspection report. To emphasize, the validation process is the mutual agreement by both parties that the information presented is accurate – it is not an acknowledgment that the inspector “is right.”

The validation process ensures that site representatives understand what was observed and understand any potential problems and impacts implied by the observation. 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 additional data in mitigation. Validation also contributes to the defensibility of rating recommendations to the Quality Review Board (QRB) and potential findings discussed with the site. The validation process provides transparency and ensures that information included in the report supports findings and ratings with facts that are not a surprise to site representatives.

There are on-the-spot validations, daily validations, weekly 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 *weekly validation* is recommended at the end of each week of inspection activity, at the end of data collection, with a *summary validation* upon report approval. Ideally, the summary validation is conducted at the security program manager working level. During summary validations, significant information, including items validated previously, is revalidated. Whether validation is done formally or not, it is important that no information should come as a surprise to the inspected facility.

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 all 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 potential 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 that address compliance and performance, 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. Finally, because the purpose of PPM activities is to plan for and provide oversight that enables performance in the other security topics, it is important to assure security managers at all levels that the PPM review process is not complete until the integration of the other topics and an analysis of force-on-force 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 5, Program Integration, 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. Take these guidelines into consideration when assigning tasks to ensure that efforts are not duplicated.
- 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.
- 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.

Section 1—Introduction

- 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 5, Program Integration, after completing each data collection activity to determine whether additional data is needed to evaluate the program. Coordinate with the other topics to determine whether compliance and performance issues in management processes have had an impact elsewhere and vice-versa. For example, the absence of field notes, worksheets, interview summaries, and performance test evidence files may indicate a “compliance centered” feedback program. Coordination with the other topics should address the impact, if any, of a lack of performance testing. If additional activities are needed, inspectors should then determine whether subsequent activities should be re-prioritized.

In the **closure phase**, inspectors:

- Refer to DOE orders and manuals to directly reference requirements, and may use the analysis tables/worksheets in Appendix A, Inspection Tool Kit, to assist in referencing and evaluating findings.
- Use the Program Integration 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.

Section 2: Planning Process

References

DOE Order 470.4A, *Safeguards and Security Program*
DOE Manual 470.4-1A, *Safeguards and Security Program Planning and Management*
DOE Order 470.2B, *Independent Oversight and Performance Assurance Program*
DOE Order 470.3B, *Graded Security Protection Policy*
DOE Policy 470.1, Chg 1, *Integrated Safeguards and Security Management Policy*
DOE Order 226.1A, *Implementation of DOE Oversight*
NA SD 226.1A NNSA Supplement to DOE Order 226.1A (pending)

General Information

DOE safeguards and security program planning is a management function that uses a standardized approach to provide an information baseline for use in integrating Departmental safeguards and security requirements, facilitating management evaluation of program elements, determining resources for needed improvements, establishing a basis for conducting cost-benefit analyses, and for accepting risk. Resulting plans provide a description of the major planning processes and products that are necessary to ensure that major program elements of the overall protection system are robust and support DOE graded security protection strategies and goals.

The primary focus of Independent Oversight inspections is to identify whether security compliance and performance actions are appropriately implemented through site-level plans. This chapter provides an overview of the Department's safeguards and security planning process used to place site-level plans in perspective.

The Role of Planning

Planning is the first step in the safeguards and security management process. It consists of identifying organizational missions, goals, and objectives and deciding how to attain them. Organization and staffing actions, budget activities, and program direction and oversight 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. It is not uncommon for inspection activities to find plans that are outdated because they no longer represent current guidance. It is also common to find plans that meet DOE requirements, yet management has neither followed nor implemented them.

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 both the *where* aspect, namely, where we are now and where we are going, and the *what* aspect, or, the end results expected of the site. These plans 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 site-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. Commonly, the longer the range of a plan, the more general the direction, and the more variable the final execution strategy will be. 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 mission, 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
- Accountability for the organization(s) 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 (change control process) as necessary
- A mechanism for independent review of task accomplishment.

DOE Planning Requirements

Headquarters Level

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 that 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.

Site Level

DOE requires the establishment of methodical approaches for the development of safeguards and security policies and protection strategies. The functions, responsibilities, and authorities associated with resourcing and implementing security programs must be clearly identified and communicated. DOE Manual 470.4-1 provides a systematic vehicle for this process by requiring development of a Site Security Management Plan (SSMP), or its equivalent, that provides detailed information on the assignment of safeguards and security roles, responsibilities, and authorities, as well as the development of budgets and allocation of resources. An effective SSMP is essential to the development of site-level plans.

The Site Safeguards and Security Plan (SSSP) or Site Security Plan (SSP) is the primary site-level strategic planning document that establishes specific levels of protection and acceptable risk levels for the site's security interests. As the cornerstone of protection program planning, the SSSP/SSP is a risk management document and the primary planning document that establishes specific levels of protection and acceptable system effectiveness levels for security interests at DOE field locations. DOE requires that the plan provide a summary of information used to describe the safeguards and security programs, VAs, and system effectiveness analyses at Departmental sites. DOE policy for SSSP/SSP formulation establishes a standard approach for presenting site protection information and VA results that summarize

Section 2—Planning Process

the effectiveness of protection programs. The SSSP/SSP must also identify resource requirements necessary to maintain existing safeguards and security capabilities and implement needed/planned protection program upgrades. The results and conclusions contained in the plan are further intended to guide long-term planning for site safeguards and security operations.

Contractor Level

Contractors are required to maintain thorough backup documentation to support the conclusions and upgrade decisions contained in the SSSP/SSP. 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 external 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 normally provides 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.

Common Deficiencies/Potential Concerns

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 VA techniques underlying many SSPs. 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 of an innovative cost savings plan. Be alert for plans that obtain the Federal Security Managers' approval or higher without an accompanying subject matter expert analysis or assessment.

Lack of Emphasis on Planning

Among the many documents the contractor is obligated to deliver, safeguards and security plans are often not considered 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. Common indicators are plans with current review dates and outdated references, plans with rescinded procedures, or instructions that do not reflect the current operating environment. These plans are often heavy on "boilerplate," weak on accountability, and reviewed via date changes only.

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). Potential signs of less than adequate expertise may be reflected by the analysis of a limited number of scenarios or a failure to adequately address obvious “what ifs” related to an issue.

Lack of Procedures for Updating 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 documentation and tracking system, 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, safeguards and security plans are frequently interrelated; thus, a change in one plan often requires a change in other plans. Without good planning integration and management, a clear understanding of the relationships among the various safeguards and security plans, and the use of a tracking system, plans can become outdated and overlooked until a crisis arises or an inspection is announced. Good self-inspection and survey programs should identify such problems.

Lack of 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 SNM and classified matter generally requires the integration of three protection systems: the 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. One of the most common results from a lack of integration is poor configuration management for vault-type rooms hosted (owned) by one organization but used by another. The tenant organization often changes the interior configuration plans without coordinating with the responsible landlord organization to assure that alarm test plans adequately cover all potential pathways into and within the room. As a result, the vault-type room may end up with pathways that leave its contents vulnerable to theft.

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 protective force posting, training, and contingency planning. Also, the contractor might have learned that it does not pay to spend an inordinate amount of time projecting for

Section 2—Planning Process

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, plans could be appropriately updated, 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 in an appropriate, timely manner. An example of such an error might be associated with the incorporation of a new item of equipment or change of policy, with the item of equipment being fielded or the policy changed before operations personnel are fully trained or prepared to implement the change. Similarly, new weapons may be fielded without the capabilities to sustain training activities, such as a lack of capability for night-time firing or the lack of a long enough firing range.

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, lines of inquiry, and data-gathering forms (see Appendix A).

A good source for descriptive information on the site and its mission is the SSSP/SSP, 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/SSP, for general site information and any upgrades identified during the SSSP/SSP 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. Prior to the onsite review, the topic team should develop and transmit to the site both a request for specific documentation, and a Lines of Inquiry document that defines the scope of the inspection.

The case study approach is one inspection technique that has been used to measure 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. Though not always applicable, for inspections during or following periods of major change it is often productive to find out the program office's expectations (that they have communicated formally) for the site if those expectations differ from DOE requirements. For example, one site was selected as a demonstration platform to test a remotely operated weapon system. The program office believed that their funding had resulted in the new system being fully fielded and operational. They were not aware that the units were still in their shipping crates.

Section 2—Planning Process

B. Inspectors should determine through interviews with site safeguards and security management personnel whether the guidance was received and in what form, whether it was understood, and how it was implemented. It is not uncommon for a program office to issue guidance without coordinating the impact with the appropriate policy office.

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

SSMP Evaluation

D. The SSMP contains descriptions of the function, roles and responsibilities of, as a minimum, Federal site staff. Contractor roles and responsibilities may also be included. In addition the SSMP links Headquarters level goals and objectives to site operations and provides a macro-level view of site resource planning. Inspectors should review the SSMP and/or equivalent documents to determine the roles and responsibilities of Federal and contractor staff. In addition, the review of the SSMP should identify whether and how well the site staff met the requirement to identify associated resources and the documented impact/vulnerability associated with budget changes/shortfalls.

SSSP/SSP Evaluation

E. 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. Sites that have no Category I and II quantities of SNM will have an SSP. Inspectors should determine whether the inspected site has an SSSP/SSP and whether it is current. The physical security systems, protective force, and MC&A topic teams will all be evaluating various aspects of the details of the SSSP/SSP. 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/SSP is a major PPM team interest item.**

F. Inspectors should conduct DOE Headquarters and site office interviews to identify pre-approval review procedures. Inspectors should review the SSSP/SSP 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 SSP, and the projected date for approval of a revised SSSP/SSP, and conduct interviews with those responsible for preparing, reviewing, and approving the SSSP/SSP.

Vulnerability Assessment Evaluation

G. The Department's process of conducting a VA requires gathering data that describes the physical and operational characteristics of a safeguards and security system, assigning values to such parameters as delay and detection, and analyzing the results to determine the relative effectiveness in conjunction with applicable threat and/or security protection levels. Specifically, VAs must account for adversary threats as identified in applicable DOE policy (i.e., DOE Order 470.3A *Design Basis Threat (DBT) Policy* or the GSP policy), which defines adversary numbers, characteristics, and capabilities (i.e., weapons, munitions, and materials available to the adversary). The Department further requires that trained analysts must use the DBT/GSP to define the threat scenarios to the protection system and to evaluate the effectiveness of the system in detecting, interdicting, and neutralizing the threat.

DOE policy also requires that critical systems elements must be identified and analyzed for every target or asset that requires a VA. These critical system elements must be specifically delineated so that performance tests can be conducted to determine the ability of the individual protection measures to perform their intended function. Additionally, performance tests must be documented and the results must be analyzed to provide a credible validation for each element's effectiveness. 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, accurate data and/or validated expert opinion.

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

SECON Plan Evaluation

Security Conditions (SECON) Plans should be designed to enhance the site's security posture in response to "actionable information" developed by law enforcement and/or intelligence agencies. It is critical that the site's SECON Plan describe specific, but flexible actions to be taken in response to changes in the SECON level that are tailored specifically to the site.

H. Inspectors should review the SECON Plan, coordinate closely with the protective force topic team to determine whether the actions defined in the SECON Plan are integrated into protective force operations and post orders, etc. In addition, inspectors should determine whether the site has conducted exercises related to changing SECON levels and coordinated with local law enforcement and site personnel. Inspectors should also determine whether the site has evaluated the effectiveness of defined SECON measures, as well as the cost and operational impact of maintaining heightened SECON status. Finally, inspectors should determine whether the site has established procedures for periodically reviewing local/site-specific threat indicators.

Tactical Doctrine Implementation

The Department established a tactical doctrine (DOE Manual 470.4-1, Change 1, Part 1, Section A, Appendix 2) governing the defense of sensitive national security assets to ensure the uniform application of effective security measures throughout the DOE complex. This tactical doctrine provides a fundamental approach for protecting nuclear weapons and components, SNM, or targets subject to radiological or toxicological sabotage. DOE tactical doctrine further establishes requirements for the development of higher protection force training and fitness standards and the employment of aggressive small-unit tactics within the bounds of a well-defined and constructed area defense that is supported by fixed strong points, strategically emplaced obstacles/barriers that are covered by fire, advanced intrusion detection and assessment technologies, coordinated fire planning, enhanced weapons systems, and armored vehicles. Consequently, DOE field sites are expected to configure critical protection elements using the Department's tactical doctrine – to the greatest extent possible – in order to achieve a concentric arrangement of intrusion detection systems, robust barriers, and response capabilities to detect, delay, and neutralize the adversary as far from the target as possible. This doctrine integrates physical security

systems (intrusion detection/assessment and barriers), protective force (tactics, training, and equipment), and VAs.

I. Inspectors should coordinate with the physical security systems and protective force topic teams, particularly with the team members involved with performance testing, to evaluate whether the site has implemented DOE tactical doctrine to the extent possible given site characteristics and environment. The review should address the use of extended detection/assessment and delay, the ability of the site to channel/direct the adversary's movements, the status of security police officer training and qualification, and the ability of the protective force to employ advanced weapons and tactics in defense of the site. In addition, inspectors should determine whether the site has evaluated the effectiveness of its protection strategy through both analysis and performance testing.

GSP Implementation Plan

The GSP is the performance standard for the protection of the Department's assets, expressed in terms of protection effectiveness. When protection effectiveness is unacceptable, sites are expected to identify and implement cost/effective enhancements to the protection program to improve protection effectiveness and to develop an implementation plan that includes a schedule and a method for monitoring progress.

J. Inspectors should review the GSP Implementation Plan to determine whether the plan includes all required actions and the site's progress toward full implementation of the GSP.

Deviations

DOE Manual 470.4-1 establishes specific procedures for characterizing deviations from Departmental requirements, processes for identifying and implementing risk mitigation measures, and requirements for obtaining appropriate approval from DOE safeguards and security program directive requirements. There are three categories of deviations: variances, waivers and exceptions. All three categories of deviations require a specific level of approval, depending on the type of security interests being protected and subject of the requested deviation, before being implemented. Variances may be approved for an indefinite time and are granted under circumstances that involve no additional risk. Supplemental to DOE approval requirements, waivers require an appropriate analysis of vulnerability with implementation of mitigating or compensatory measures and must not be approved for periods exceeding two years. Exceptions require a higher level of approval that involves formal risk acceptance; they must not be approved for periods exceeding three years, and the need for continuation of the exception must be validated annually.

K. Inspectors should compare the list of deviations included in the SSSP/SSP with both site records and the Safeguards and Security Information Management System (SSIMS) to determine whether they are the same. SSIMS is the list of record.

L. Inspectors should also review individual deviation request packages to ensure that they are complete, are approved at the appropriate level, and include a risk statement supported by VA or performance test data.

Procedures for Plan Development

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

M. Inspectors should determine whether the site’s 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

N. 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.

O. 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, functions and responsibilities manuals, program and corrective actions plans) are available to management for holding contractors and individuals accountable for their assigned responsibilities.

P. Inspectors should review award fee appraisals against contracts to ensure contractors are meeting established planning goals. Assignments within functions and responsibilities manuals should be verified to ensure the existence of specified planning documents. Corrective action plans can be reviewed to determine whether specified document or procedural revisions are being accomplished according to the plan schedule.

Consistency Among Plans and Procedures

Q. 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/SSP 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 VA Evidence Files

R. The risk acceptance in the SSSP/SSP 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.

S. 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 and Integration

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/SSP) and planning documents associated with their topic areas (e.g., operations security plan, MC&A plan). Meet with the other topic teams on a daily basis to review that day's activities with the intent of discovering issues that require integration. Expect that topic teams will inspect their topical areas to determine the effectiveness of plans in those areas. Draw heavily on the experience, expertise, and ongoing inspection activities of the other teams.

Section 3: Federal Feedback and Improvement Processes

References

DOE Order 470.1, Chg 1, *Safeguards and Security Program*
DOE Manual 470.4-1A, *Protection Program Management*
DOE Order 226.1A, *Implementation of DOE Oversight Policy*
DOE *Self-Assessment Kit*

General Information

A subsystem of safeguards and security management provides feedback and improvement functions for safeguards and security activities through surveys, reviews, inspections, self-evaluations/assessments, reporting, and corrective action. Programs to provide feedback and foster continuous improvement are essential for assessing the adequacy of measures and controls, improving the definition and planning of work, and ensuring that best practices and lessons learned are shared. DOE requires that these programs be established at local levels and that they be integrated to foster a work process that facilitates defining and planning work, formally identifying and analyzing risk, developing and implementing measures and controls, performing work, and monitoring and assessing performance feedback and improvement. As part of this feedback and improvement process, DOE requires that sites develop robust Performance Assurance Plans (PAPs) and programs that ensure the operability, effectiveness, and continuity of essential protection elements. Similarly, surveys conducted by the cognizant security authority and self-assessments conducted by contractors must provide a means for identifying programmatic strengths and weaknesses and facilitate line management's prioritization of decisions regarding site safeguards and security programs, including allocation of resources, acceptance of risks, and mitigation of vulnerabilities. Departmental requirements also dictate that line management at sites and facilities develop and implement formal corrective actions where safeguards and security shortfalls are identified during feedback and continuous improvement efforts.

For inspection purposes, these functions are the documented organizational and procedural measures implemented by Departmental and contractor management that evaluate and communicate the status of program compliance and performance in accordance with DOE Headquarters and line management policies and procedures. Safeguards and security management includes those personnel and offices at all DOE/National Nuclear Security Administration (NNSA) and contractor levels of organization that are assigned responsibilities for managing and implementing the protection program.

Survey Program

The survey program is a major topical area for inspections; the PPM topic team evaluates the detailed implementation of the Federal program and how effectively line managers use the information developed by this feedback system. This section focuses on Federal feedback and improvement processes. DOE requires site offices to conduct surveys that effectively communicate the contractor's level of compliance and performance in the safeguards and security program. In addition, the site office must conduct a self-assessment in which they review their internal processes. DOE permits site offices to conduct the review of themselves as either a survey or self-assessment as long as they examine the execution of their own security responsibilities and actions. The last element of the Federal review is the effectiveness of the

Performance Evaluation Plan (or similarly named process) through which the site office communicates expectations and provides rewards or levies penalties for security contract performance.

Survey Planning

DOE Manual 470.4-1A, Section G, prescribes requirements for the conduct of surveys. This program is a primary method 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. The primary documentation from this program are the individual topic survey plans, performance test reports, and field notes of interviews and observations used to develop annual facility survey reports. Survey reports are distributed to all organizations with a registered activity at the surveyed facility and to applicable Headquarters elements. These survey reports and associated documentation provide critical information to management and to inspection elements.

Federal Self-Assessments

A self-assessment program is a management process with the major objective of measuring the status of internal compliance and performance 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 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 site offices are expected to implement a self-assessment program that provides coverage for all elements of the protection program. While addressing any direct security responsibilities they may have, the Federal self-assessment must also evaluate the implementation and effectiveness of the oversight they provide to the contractor in all topics. The effectiveness of the program at all levels is of significant importance to the PPM topic team.

Internal Oversight

Managers may establish additional internal, self-directed feedback 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 these measures are the normal reporting systems inherent in line management operations, such as integration boards; change control processes; information management systems; and mandatory or regularly scheduled observations, walkdowns, and other (deliberate or incidental) documented operational awareness activities. Documentation of these activities is essential if management intends to include them in formal feedback processes. For example, a working group that is chartered to assure that the survey program is integrated with and takes credit for all oversight activities, such as the contractor's performance award evaluations, would be regarded as potentially more effective than a survey program that is not integrated. The PPM topic team should become aware of these measures and determine their contribution to the feedback process.

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 actions for identified issues are as important as the 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, risk and cost-benefit analysis, the development of actions to address the deficiency, the assignment of responsibility for completion of corrective action, and a trend analysis of results. The 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 in a manner that precludes recurrence.

Locally Developed Feedback Systems

Various reporting and information systems might have a secondary use as feedback mechanisms. 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 system include budget program reviews, reports of security infractions, personnel status reports, the SSSP/SSP development process, and personal observations. Inspectors must address these activities to the extent that they promote effective performance.

Common Deficiencies/Potential Concerns

Ineffective Survey Programs

One purpose of the survey program is to grant facility approval before permitting safeguards and security interests on the premises. Once a facility is operating, the primary purpose of the survey program is to provide documented assurance of the status of security program compliance and performance with DOE requirements and objectives. The survey program develops information that may be used for other purposes as well, such as award fee requirements, and also provides an interface between the surveying office and surveyed sites. The survey program should be examined by management to ensure that program results are used to the best advantage. Experience has shown trends in weaknesses that inspectors should be aware of.

Management may have delegated responsibility for the survey program to a level where the prescribed program may be run effectively, but where 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 feedback systems that duplicate the capability of the survey program.

Vague or Ineffective Survey/Self-Assessment Guidance and Plans

- Site offices must develop survey and self-assessment guidance and plans.
- Often, procedures or plans to implement the program are incomplete, do not include all DOE requirements or contain vague descriptions of the tasks and functional elements to be assessed.
- Procedures and performance-oriented criteria may be absent.
- Requirements for Corrective Action Plans (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 use a term other than “finding.” Another variation of this deficiency is when guidance provides a definition of a “finding” that differs from that approved by DOE.
- 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.

Ineffectively Implemented Survey/Self-Assessment Programs

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

- The assessments and surveys vary significantly in depth of coverage and many do not include adequate performance testing, often because insufficient resources have been made available to implement these programs successfully.
- Personnel performing self-assessments or surveys generally focus on their specific areas 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, so 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.

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 feedback systems. Sites often develop additional 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 walkdowns” during which mid- and senior-level managers were given specific topics to evaluate, depending on what area the 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.

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.

Reactive Organizational Oversight

In the absence of internal oversight 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 oversight subsystems are required to keep management informed.

Unsupportive Award Fee Processes

A primary mechanism for adding emphasis to a program and ensuring 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. In one example, a site that had converted from a “university” model to an incentive-oriented “for profit” contract had no fee for safeguards and security performance. Award fee properly

Section 3—Federal Oversight

allocated to safeguards and security has been shown to be an extremely effective oversight measure, and the information gathered for the award fee process may be used for other elements of management.

A common deficiency in award fee processes is that award fee is tied to easily achieved goals or incentives that simply expect the contractor to do the work as stated in the contract. For example, a site had over a million dollars in award fee tied to “obtaining the highest ratings possible during Independent Oversight Cyber, Security, and Emergency Management inspections.” However the highest rating these inspections provide is “meets expectations”. Similarly, sites have linked performance award to “satisfactory” performance in annual surveys, even though Satisfactory is the minimal level expected of all programs – not a difficult-to-achieve benchmark.

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

- Is fee awarded despite significant safeguards and security failures?
- Is fee awarded based on a documented program review or on the contractor’s assertions? It is not uncommon to find award fee programs that include a requirement for the contractor to provide their own appraisal, which the site office then approves.

Planning Activities

During planning, inspectors identify the feedback and improvement 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

Records

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

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

B. During the review of records, 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 oversight systems that are in effect at each level of management
- Informal feedback systems that are not necessarily institutionalized but are relied upon as a control measure
- Internal, self-directed feedback measures.

C. Inspectors should review the 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 those 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 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.

Survey Program

E. Inspectors should first determine whether an approved Federal survey program is in place at the site office safeguards and security organizational level and whether management has published survey/self-assessment guidance. Inspectors should review the guidance and/or plan to determine whether it contains all DOE requirements, including appropriate assignment of responsibilities and adequate instructions and procedures for assessing all aspects of the protection program. Inspectors also need to coordinate any integration with other topic teams that normally assess the effectiveness of the survey program in their respective areas.

F. 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.

G. 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. Specific lines of inquiry related to surveys are provided in Appendix A.

Federal Self-Assessment Program

H. Inspectors should evaluate the overall self-assessment program to determine how the results of the program are 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 an oversight 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. Additional information related to lines of inquiry for self-assessments is provided in Appendix A.

Internal Oversight

I. Inspectors can determine by interview and document review whether other internal feedback measures (in addition to self-assessments, which are discussed 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.

J. Inspectors should check for duplication of effort and for appropriate interfaces between internal and external oversight and feedback systems. For example, if the self-assessment and survey programs are capable of providing the manager with the required information, other internal measures might not be necessary. The most effective managers 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 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.

Corrective Action Plans

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

K. Inspectors should review system effectiveness by following an issue from identification to resolution by selecting findings from previous 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.

L. There is no prescribed system and no direction that an issue-tracking system must be automated. However, effective managers 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 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.

Award Fee Determination Plan

M. Inspectors should determine whether cost-plus award fee contracts exist for site safeguards and security contractors. 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, focusing 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 award 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 management for safeguards and security system feedback?

Locally Developed Feedback Systems

N. 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 to monitor safeguards and security program status. 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

O. 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 the status of individual findings
- Magnitude of deficiencies unknown
- Trend analysis not conducted
- Root cause analysis not conducted.

Section 3—Federal Oversight

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

P. There is no minimum standard or “correct” percentage of an award fee that should be allocated to safeguards and security. Field experience suggests that between 1 to 10 percent of an award fee for management and operations contractors is generally allocated to safeguards and security. If the safeguards and security award fee appears to be inadequate, inspectors should question 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 oversight system is effective for safeguards and security. Inspectors should consider these frequently cited factors in determining the allocation percentage:

- History of the contractor’s safeguards and security performance
- Need for emphasis on safeguards and security as determined by the operations/site office
- Adequacy of other oversight 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. The PPM team should consider these indications for applicability because experience indicates that the integration of other topic team observations is especially applicable to the feedback 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 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, is normally 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 oversight system; either the feedback 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 other topic teams’ observations for their impact on PPM, it might find that adequate feedback systems are in place, but that other factors (e.g., non-availability of resources, human error, and management’s judgment) might have been the cause of the problem.

When problems indicating a potential feedback system deficiency are discovered by another topic team, it is essential that the PPM team coordinate with that team to gain their observations on the effectiveness of the feedback systems. If the systems at the PPM level are at fault, problems are typically evident in more than one topic.

This page intentionally left blank.

Section 4: Contractor Feedback and Improvement Processes

References

DOE Order 470.1, Chg 1A, *Safeguards and Security Program*
DOE Order 470.2B, *Independent Oversight and Performance Assurance Program*
DOE *Self-Assessment Kit*

General Information

A subsystem of contractor safeguards and security management provides feedback and improvement data for safeguards and security activities through inspections, self-evaluations/assessments, reporting, and corrective actions. For inspection purposes, contractor feedback and improvement systems are the organizational and procedural measures implemented by 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 contractor 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 for each primary site contractor and whether management has published self-assessment guidance. Inspectors should review the guidance and/or plan to determine whether it complies with DOE requirements and contains adequate descriptions of responsibilities, instructions, and procedures for assessing all aspects of the protection program. Inspectors should then coordinate with other topic teams to determine the scope, depth, and quality of the topical area self-assessments. The lines of inquiry in Appendix A of this Guide may be used to facilitate assessment of the adequacy of site self-assessment programs.

Self-Assessments

A self-assessment program is a management system with the major objectives of establishing accountability and excellence at the grassroots level, thereby involving people who are the most familiar with the processes being assessed. 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 elements of the safeguards and security program (e.g., CIC 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 Feedback

Managers may establish their own internal, self-directed feedback 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 are the normal reporting systems inherent in line management operations. Although the inspection process focuses on the formal self-assessments and performance assurance programs required by DOE as the basis for the inspection results, the PPM topic team should become aware of any additional feedback measures and give credit for their contribution to the overall feedback process if they are effective.

Performance Assurance Program

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

DOE requires that performance testing be documented in the site's PAP, which is an integral part of the SSSP/SSP. The PAP must describe the program and its administration by identifying essential protection elements for the protection of SNM and Top Secret matter and describe how the performance of these elements is to be ensured. Additionally, the PAP must address how deficiencies identified during performance assurance activities are to be corrected. The primary objective of DOE PAPs is to assure the effectiveness of the protection provided to Departmental safeguards and security interests by systematically evaluating all essential protection program elements. DOE requires that PAPs must provide for both operability testing (e.g., function/serviceability checks) and effectiveness testing (e.g., limited-scope performance tests and/or force-on-force tests) of each essential protection program element or component. The Department further requires that PAPs must provide for evaluation of operational continuity of all essential system elements and assure that new (or recently repaired) essential elements are validated through acceptance testing before operational deployment.

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 identified essential safeguards and security elements. It is most important for inspectors to determine whether a performance assurance program exists and whether the site has developed an essential element list. Finally, the PPM team is very interested in whether the tests that are run under a performance assurance program are able to measure the effectiveness of the protection element. The PPM team should provide the other topical teams with both the information they find regarding the elements that should be candidate essential elements and the specific type of performance they need in order to validate VA data inputs. Specific lines of inquiry for evaluating performance assurance programs are included in Appendix A of this Guide.

Corrective Action Plan Program

Subsystems and processes used by management to develop and track corrective action on identified issues are as important as the feedback systems used to initially identify issues. It is essential to have an effective system for developing and tracking corrective actions 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. The tracking system normally records the status of milestones, 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 Feedback Systems

Various reporting and information systems might have a secondary use as a feedback 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 feedback system include management walkdowns, budget program reviews, reports of security infractions, personnel status reports, the SSSP/SSP development process, and personal observations.

Common Deficiencies/Potential Concerns

Vague or Ineffective Self-Assessment Plans

Most contractor 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, identification of root causes for findings, tracking, and trend analysis 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 may be spurious, undocumented, and without appropriate causal analysis, tracking or trending.

Ineffectively Implemented Self-Assessment Programs

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

- The assessments vary significantly in depth of coverage and many do not include adequate performance testing, often because insufficient resources have been made available to implement these programs successfully.
- Personnel performing self-assessments generally focus on their specific areas of responsibility without considering the impact of closely related functions. Self-assessment reports do not support the conclusions reached.
- CAPs generated as a result of a self-assessment fail to identify applicable causal factors and/or fail to include actions that will address the identified deficiency.

Section 4—Contractor Oversight

- Deficiencies found during self-assessments are not always characterized as findings, so no corrective action takes place.
- Results of previous inspections, surveys, or assessments are not used when conducting self-assessments to ensure that similar deficiencies do not exist.
- Personnel assigned responsibility to conduct self-assessments do not have the background, training, or expertise to effectively evaluate program status.

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 feedback and improvement systems. Sites often develop additional feedback and improvement 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 walkdowns” during which mid- and senior-level managers were given specific topics to evaluate, depending on what area the 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.

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 for monitoring progress and early identification of schedule slippage; 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.

Reactive Organizational Oversight

In the absence of internal feedback 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 feedback subsystems are required to keep management informed.

Planning Activities

During planning, inspectors identify the feedback and improvement systems used at all echelons of management. This information will help establish priorities and task assignments to team members.

Data Collection Activities

Records

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

- SSPs or SSSPs
- Organization and functions manual(s)
- Mission statement
- Self-assessment program plan and procedures
- Performance assurance program plans
- Procedures for CAPs.

B. During this review, inspectors should identify which facilities and 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 feedback systems that are in effect at each level of management
- Internal, self-directed feedback measures
- Informal control systems that are not necessarily institutionalized but are relied upon as a feedback measure.

Self-Assessment Program

C. Inspectors should evaluate the overall self-assessment program to determine how the results of the program are 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 documentation necessary to assess the compliance and performance 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.

Section 4—Contractor Oversight

D. Inspectors should review the 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 the local DOE surveys and those from the General Accounting Office and the DOE Office of the Inspector General, and review as appropriate.

E. 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 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.

F. Inspectors should review system effectiveness by following an issue from identification to resolution by selecting findings from previous 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.

Impact of Deficient Corrective Action Process

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
- Magnitude of deficiencies unknown
- Management not aware of the status of individual findings
- Root cause analysis not conducted
- Trend 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.

G. There is no prescribed system and no direction that an issue-tracking system must be automated. However, effective managers 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 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.

Internal Feedback

H. Inspectors can determine by interview and document review whether other internal feedback measures (in addition to self-assessments, which are discussed in activities C through E, 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.

I. Inspectors should check for duplication of effort and for appropriate interfaces between internal and external oversight and feedback systems. For example, if the self-assessment and survey programs are capable of providing the manager with the required information, other internal feedback measures might not be necessary. The most effective managers 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 feedback 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.

Locally Developed Feedback Systems

J. 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 should be credited for their contribution to feedback data. 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.

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. The PPM team should consider these indications for applicability because experience indicates that the integration of other topic team observations is especially applicable to the feedback 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 topic teams can also provide valuable data to determine the status of findings and corrective actions in their topic areas. This information, along with that already gathered by the PPM topic team, is normally 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 oversight system; either the oversight 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 other topic teams' observations for their impact on PPM, it might find that adequate oversight systems are in place, but that other factors (e.g., non-availability of resources, human error, and management's judgment) might have been the cause of the problem.

When problems indicating a potential feedback program deficiency are discovered by another topic team, it is essential that the PPM team coordinate with that team to gain their observations on the effectiveness of the management oversight systems. If the feedback systems at the PPM level are at fault, problems are typically evident in more than one topic.

Section 5: Program Integration

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 one location, the metric they used to measure protective forces management effectiveness was the reduction of *unscheduled overtime* over the previous year. Under this metric, protective force 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 number of overtime hours, but that the *unscheduled* overtime had been 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. Federal management failed to properly define the expected overtime reduction and protective force management masked the fact that overall overtime had not been reduced.

Analysis

The analysis process involves the PPM team's critical consideration of all inspection results, including the results from other topical areas. Analyses should lead to logical, supportable conclusions regarding how well the protection program is managed and whether it 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 the subtopics on each other; and 2) the overall status of the topic. Following the analysis of PPM topic indicators, results from other inspection topics can be used, much as a 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 of a survey program can indicate whether or not a team leader has been appointed, a schedule has been written, and all areas have been surveyed, and whether the survey was based largely on document reviews or was performance-based. If a number of these example elements are missing (no-go), the resultant analysis will have a more objective basis and better support possible descriptions of the qualitative nature of the program. Conversely, inspectors must avoid the pitfall of automatically treating all issues as *ultimately management failures*

Section 5—Program Integration

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 identified 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 topical 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 in this analysis 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 performance.

The relationship of all topical 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. Topics frequently ask the PPM topic to address an issue in the PPM section "because it is a management topic." When considering whether the PPM team should address a particular issue, the first question the inspector should ask is "Is the issue a compliance or performance deficiency that resulted in a finding?" If not, it will generally not warrant elevation to a PPM finding. Even if it did not rise to the level of a finding, it may still be relevant if similar observations in other topics indicate a trend that is of significance to PPM. For example, poor training in one topic, accompanied by the assertion that "Management knew it was a problem," might not indicate a PPM issue, but a need for training that led to findings in *three* areas might. 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 that should significantly impact the PPM area?
- Would timely management actions have precluded the deficiency?
- Do analyses of ratings and issues from the other topic teams reveal a systemic PPM problem?

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 topical 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 external 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.

Section 5—Program Integration

- 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 does not, in itself, indicate a management failure, but may indicate overall PPM planning effectiveness, which must be factored into the overall PPM picture by the topic team. Answering the following questions¹ 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?
- Are the following plans approved and current and do they contain appropriate documentation?
 - The SSMP, or equivalent documents
 - The SSP or SSSP, as appropriate
 - The SECON plan
 - The PAP.
- Is the SSP/SSSP supported by an accurate, current, and validated VA?
- Do the VA evidence files provide adequate support for the assumptions and decisions made in the analysis?
- Are deviations from Departmental safeguards and security requirements appropriately developed, analyzed, and processed?
- 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?

Feedback and Improvement Programs

Effective feedback and improvement programs at all levels of management are fundamental to managing a protection program. Each level requires different 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

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

failure in establishing and implementing adequate feedback and improvement mechanisms could result in management making decisions based on insufficient or inaccurate information.

The bottom line for the inspector is to determine whether both Federal and contractor feedback and improvement programs provide managers with useful data on the status of protection program elements. If the answers to the following questions are all affirmative, the inspector should generally consider feedback and improvement processes 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, correcting, and bringing to timely closure deficiencies noted in surveys, inspections, self-assessments, and self-directed control systems?
- Are timely reports provided to the appropriate organizational level to ensure proper management attention?

Including Results from Other Topic Teams

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 longstanding deficiencies in protective force and physical security systems should be appropriately addressed under feedback and improvement; the subtopic under which it is addressed depends on whether it was assessed and rated as part of the self-assessment, survey, or performance assurance program. As another example, still within the feedback and improvement area, the lack of clear and appropriate corrective action procedures may result in a failure to properly identify the cause of deficiencies and may result in inadequate corrective actions, thus allowing recurrent errors. Other issues should be placed under appropriate subtopics in PPM according to an 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.

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 inspection report and combines with other unique attributes to strengthen the overall 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 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 the management of their topics, 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, DOE tactical doctrine is addressed within the PPM topic area; however, the PPM team requires information from the physical security and protection force topic teams to adequately assess the effectiveness of the implementation of that doctrine. While the PPM team can identify the overall intent, priorities, and defensive schemes associated with site defensive plans, the other topical teams must provide critical information on how well line management supported and executed the plans and whether or not the results of testing verified that the plans effectively implemented current doctrine. The details of such implementation can only be accurately evaluated by those with extensive knowledge and experience within the applicable topic area.

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 topic 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 an excessive number of false or nuisance alarms with a given intrusion detection system, it might

indicate a design flaw, a maintenance weakness, a training and qualification flaw or other issue that could have been identified by the performance assurance program. 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 that have 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 Subtopical Areas

The PPM topic is divided into the two broad subtopical areas; planning, and feedback and improvement. It also includes an assessment of the overall integration of safeguards and security policy across all topical areas.

The planning subtopic addresses the site management infrastructure, strategic planning and risk management, directives implementation, and contingency planning. The review of the SSMP focuses on both Federal and contractor protection program management infrastructure and the overall budgeting process. Strategic planning and risk management are assessed through the review of the SSSP/SSP, associated VAs, and implementation of the Department's tactical doctrine. Directives implementation is addressed through the deviations process review, which assesses both Federal and contractor management methods for implementing necessary modifications to Departmental safeguards and security requirements. Finally, contingency planning is addressed through the SECON Plan review.

The feedback and improvement subtopic focuses on the processes implemented by the protection program management staff to control the overall safeguards and security program by maintaining a constant understanding of protection program status, and identifying and correcting deficiencies in a timely manner. The Federal survey program and the Performance Evaluation Plan focus on the effectiveness of Federal oversight in ensuring that contractor safeguards and security programs comply with Departmental requirements. The review of both Federal and contractor self-assessment programs focuses on each entity's ability to self-identify strengths and weaknesses in protection programs. The review of the corrective action program focuses on the ability of site management to correct identified weaknesses in a timely manner, with minimal potential for re-occurrence. The performance assurance program review focuses on how the site assures that the most important elements of the protection program continue to perform as expected.

Planning Process

The PPM team depends on other topic teams to confirm much of the data included in VAs, including the placement and effectiveness of protective force assets, electronic intrusion detection/assessment systems, and access control systems. In addition, the individual topic teams are better equipped to evaluate the effectiveness of a site's non-standard measures to meet Departmental directives.

Feedback and Improvement Programs

Inspection teams for each inspection topical area must determine and evaluate the feedback and improvement programs in effect for their topic. If any topic team finds that these systems are inadequate, they should identify the requirements that have not been met as a result of insufficient oversight and the compliance and/or the performance impact. Normally, if the issue does not result in a finding in a given topic, this is an indication that it is a compliance issue that does not systemically affect performance. If the issue rises to the level of a finding in a topic, this is a generally reliable indicator of performance impact that should be addressed for PPM implications/integration. Similar significant issues in two topics, or less-significant (limited to compliance) issues in three or more topics, may indicate a program-wide PPM issue, such as insufficient oversight.

By communicating topic team observations among topic teams and the PPM team, a pattern of deficiencies might be identified in more than one topical area, and thus be indicative of a systemic 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.

Appendix A: Inspection Tool Kit

Protection Program Management Performance Evaluation	A-1
Office of Independent Oversight Inspection Plan/Notification Letter (Example)	A-11
Inspection Schedule (Example).....	A-15
Information Request/Data Call (Example)	A-17
Protection Program Management Detailed Inspection Plan (Example).....	A-21
Protection Program Management Inspection Process Matrix	A-25
Protection Program Planning Weekly Schedules (Examples).....	A-33
Tools Related to Section 2, Planning Process	
Tool 2-1: Planning Worksheet	A-37
Tool 2-2: Document Checklist	A-38
Tool 2-3: Plan Evaluation Worksheet.....	A-40
Tool 2-4: Safeguards and Security Plan Detailed Review	A-42
Tool 2-5: Vulnerability Assessment Report Detailed Review	A-45
Tool 2-6: ASSESS/ATLAS Facility Characterization Files Detailed Review	A-48
Tool 2-7: ASSESS/ATLAS Outsider Analysis Detailed Review	A-51
Tool 2-8: ASSESS/ATLAS Insider File Detailed Review.....	A-53
Tool 2-9: JTS/JCATS Neutralization Analysis	A-55
Tool 2-10: Tabletop/Qualitative Evaluations	A-58
Tool 2-11: Vulnerability Assessment Summary Analysis Table.....	A-62
Tool 2-12: Deviations Assessment	A-66
Tools Related to Sections 3 and 4, Federal and Contractor Oversight	
Tool 3-1: Lines of Inquiry	A-69
Tool 3-2: Survey and Self-Assessment Reports Review.....	A-75
Tool 3-3: Topical Team Survey and Self-Assessment Evaluation	A-78
Tool 3-4: Topical Team Performance Assurance Program Evaluation	A-81
Tool 3-5: Overall Performance Evaluation for Oversight.....	A-82
Additional Forms and Instructions	
Data Collection Form	A-85
Instructions for Completing an Issue Form	A-86
Report Preparation	A-87
Oversight, Deviations, and Performance Assurance Assessment Worksheets.....	A-89
Deviations Assessment	A-90
Classified Cyber Facilities Survey/Self-Assessment Review	A-91
Unclassified Cyber Facilities Survey/Self-Assessment Review	A-92
IM/CMPC Facilities Survey/Self-Assessment Review.....	A-93
NMC&A Facilities Survey/Self-Assessment Review.....	A-94
PERSEC Facilities Survey/Self-Assessment Review	A-95
Pro Force Facilities Survey/Self-Assessment Review	A-96
Physical Security Systems Facilities Survey/Self-Assessment Review.....	A-97
PPM Facilities Self-Assessment Reviews.....	A-98
PPM Facilities Survey Review	A-99
PPM Feedback Survey	A-100
PPM Summary Validation Worksheet	A-102

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 EVALUATION**

PROTECTION PROGRAM MANAGEMENT PERFORMANCE EVALUATION

The inspection of PPM will include: Protection Program Planning, Feedback and Improvement, and Safeguards and Security Program Implementation. In addition, an evaluation of the site's progress to implement applicable DOE Tactical Doctrine and Policy will be performed. The primary focus under protection program planning will be the SSSP and the vulnerability assessments underlying them. PPM will also evaluate the extent to which the site has successfully addressed planning issues identified in previous Independent Oversight inspections. Coupled with this review is a large-scale, force-on-force performance test conducted to confirm the implementation of DOE Tactical Doctrine and vulnerability assessment results.

The review of performance assurance activities will address whether there is sufficient integration of critical system elements and the SSSP/SSP; the influence, if any, of current and pending deviations; how the performance of one system affects another; whether all critical system element operational and performance assurance tests are appropriately scheduled and completed; whether there are mechanisms in place to address system failures; and whether adequate analysis of tests is accomplished to develop appropriate lessons learned. Oversight related inspection actions will focus on the leadership and oversight provided for the SSSP/SSP effort and site office effectiveness in providing safeguards and security program direction to site contractors, including the review and processing of deviation requests. The review of feedback and improvement will include the Performance Evaluation Plan (PEP), the Federal survey program, contractor self-assessment programs and issues identified by outside reviews, surveys, and independent assessments. This review will include the approval and monitoring of corrective actions taken at the site office and by site contractors in response to issues identified by assessments from any source.

Finally, the results of all other topical team assessments will be analyzed to determine the extent to which site management systems result in the integration and implementation of all S&S topic areas.

PLANNING

The objective of the inspection process with regard to safeguards and security (S&S) planning is to assess the effectiveness of the site's planning in complying with Departmental planning requirements as described in DOE Manual 470.4-1, Change 1, and subsequent updates. The primary areas of evaluation are: the Safeguards and Security Management Plan (SSMP); the Site Safeguards and Security Plan (SSS) or Site Security Plan (SSP) and supporting vulnerability assessments (VAs); the process for addressing necessary deviations to Departmental requirements; implementation of the Department's Tactical Doctrine; and implementation of the Graded Security Policy (GSP).

Safeguards and Security Management Plan:

- Is there a specific SSMP or are the concepts incorporated in other equivalent documents?
- Does the SSMP provide a description of the implementation of S&S policy?
- Does the SSMP describe the organization structure and the functions, roles, responsibilities, and authorities of each position?

- Does the SSMP document the development of budgets and allocation of resources?
- Does the SSMP describe the resources that are necessary to both maintain the current S&S program and implement enhancements to either reduce risk or improve operational cost effectiveness?
- Is the SSMP updated annually (at least every 12 months)?
- Do the strategic planning assumptions that are used to support the S&S program meet site mission requirements and objectives?
- Does the SSMP document how the cognizant security authority will assess the implementation of the S&S program and the organization's progress toward meeting established missions/goals?
- Does the SSMP cover both the Federal and contractor elements?

Security Condition (SECON) Plan:

- Is there an approved documented SECON Plan?
- Is the SECON Plan integrated into protective force (PF) operational plans?
- Are site responses defined for changes in SECON levels?
- Has the site documented/tested predetermined employee responses (i.e., evacuation, shelter in place) to SECON changes?
- Does the SECON Plan include appropriate interaction with Headquarters elements?
- In this event, are the Headquarters Operations Center and Departmental elements notified of the SECON level?
- Has the site developed a process to periodically review local/site-specific threat indicators?
- Does the site have a record of specific SECON measures currently in place?
- Has an assessment been made of the site's ability to sustain specific SECON measures?
- Does the SECON Plan have a provision for seeking Headquarters-approved relief from the requirements of its plan?

Site Safeguards and Security Plan/Site Security Plan:

- Does the Site Safeguards and Security Plan (SSSP) or Site Security Plan (SSP) meet DOE format and content requirements?

- Does the process for preparing the SSSP or SSP provide for reasonable input from all concerned parties?
- Does the description of the operations include all current activities?
- Does the description of the protection measures accurately reflect those implemented?
- Have other topic teams identified concerns over the protection programs described in the SSSP/SSP?
- Does the site office play a part in the review and approval of each SSSP/SSP?
- Does the review, comment, and approval process for the SSSP/SSP meet requirements?
- Are elevated risks appropriately reported to senior management?
- Is the SSSP/SSP current and approved at a level consistent with the amount of risk being accepted?
- Are S&S essential protection elements and systems identified for evaluation under the performance assurance program (PAP)?
- Do the results of VAs depict the existing condition of site protection programs?
- When the Design Basis Threat (DBT)/GSP performance standard cannot be met, are VAs used to establish priorities and resource requirements for the necessary improvements?
- Does the Resource Plan identify near- and long-term resource requirements needed to ensure the integrity of existing and planned S&S upgrades?
- Is there a process to communicate the impact of the inability to fund identified upgrades?
- What is the status of SSSP/SSP-identified upgrades?
- When there are elevated levels of risk, does the SSSP/SSP provide a cost-effective plan for reducing the level of risk in a reasonable timeframe?
- Is the SSSP/SSP supported by reliable VAs?

Vulnerability Assessments:

- What is the baseline threat document?
- Do VAs portray a threat appropriate for the operations?

- Are there assumptions made that unreasonably limit adversary actions or capabilities?
- Do VAs meet the conditions of the scoping agreement?
- Does the set of site VAs represent the total site operating environment?
- Do the adversary strategies and tactics evaluated reflect the best choices for the adversaries under the prevailing assumptions?
- Did the site analyze the potential use of onsite hazardous materials as an adversary force multiplier?
- Do PF strategies and tactics reflect those actually trained for and used by the site?
- Were the representative adversary scenarios approved by the scenario development review process, and do they address the requirements of the GSP?
- Are the methods used to evaluate protection effectiveness adequate to evaluate adversary and site actions and responses?
- What effectiveness methodologies are used for the VAs?
- Are the effectiveness methodologies used correctly?
- 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 and probability of kill file for Joint Tactical Simulation (JTS)/Joint Conflict and Tactical Simulation (JCATS) tactical models?
- How are adversary timelines and task requirement times determined?
- 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?
- 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?
- Does the site have an adequate set of tools to conduct the required analyses (e.g., adequate numbers of terminals and facilities for JCATS simulations, or the capability to update terrain models)?
- Do evidence files provide adequate support for assigned figures of merit?
- Were evidence files readily available for review?
- Have the results of the VAs been portrayed correctly in the SSSP/SSP?

- What is the status of SSSP/SSP identified upgrades?
- Does the VA report address all of the data requirements of DOE Manual 470.4-1, Part 1, Section E, Appendix 5?
- Does the VA approval process meet the requirements of DOE Manual 470.4-1, Part 1, Section E?
- Were critical protection system elements identified and included in the PAP Plan?

Deviation Process:

- Does the Federal oversight office have a documented process for evaluating and approving deviation requests?
- Does the contractor have a documented process for developing deviation requests?
- Do deviation requests meet Departmental format and content requirements?
- Are deviations appropriately characterized (i.e., variance, waiver, exception)?
- Are results of vulnerability analyses and performance tests conducted on proposed alternatives included?
- Are deviations from S&S program directive requirements appropriately approved before implementation?
- If approved, has an evaluation of the risks associated with the deviation been conducted?
- Are approved deviations documented in the SSSP/SSP and site procedures as appropriate?
- Are deviations approved out of cycle with the SSSP/SSP approval process documented as an attachment to the applicable plan until the next annual update?

Tactical Doctrine:

- Has the site implemented the Department's tactical doctrine in a manner that addresses the site's specific environment?
- Are protection strategies implemented as specified in either the DBT or GSP policy?
- Is the overall protection strategy consistent with DOE doctrine?
- Are PF resources positioned so that there is little or no delay in responding to critical targets?
- Are PF resources positioned to interdict and neutralize the adversary threat as far as possible outside the boundaries of the target location?

- Are physical protection systems used to maximize and enhance PF effectiveness?
- Is there a well-defined area defense?
- Are aggressive small-unit tactics employed within the bounds of a well-defined and constructed area defense?
- Is the defense supported by fixed strong points and obstacles/barriers?
- Are there advanced detection and assessment capabilities in the defined area of defense?
- Is the defined area of defense supported by coordinated fire planning, updated weapon systems, and armored vehicles?
- Does the tactical response force (TRF) consist of highly trained, motivated, and skilled tactical units/teams positioned on, or in proximity to, each target?
- Are there documented and approved plans to accomplish the recapture, recovery, and pursuit missions?
- Are the TRF trained to accomplish the recapture, recovery, and pursuit missions?

GSP Implementation:

- Has the site developed a schedule for addressing the requirements of the GSP?
- Is the site meeting its schedule?
- If not, what are the barriers it is facing, and how is the site addressing these issues?

Determine whether an effective mechanism is in the contract to reward or penalize contractor performance by asking:

- Are all deviations correctly characterized as variances, waivers, and/or exceptions?
- What mechanisms exist in site contracts?
- 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 to 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. Also, determine whether effective management processes are in

place to 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. The following lines of inquiry can be used to determine the effectiveness of the performance assurance, Federal survey, performance evaluation, contractor self-assessment, and resolution of findings programs at the inspected site.

Performance Assurance Program:

- Is there a formal PAP Plan?
- Does it describe the PAP efforts associated with assuring the protection of Category I quantities of special nuclear material (SNM) and Top Secret data?
- Does the PAP describe how deficiencies identified during performance assurance activities are to be corrected?
- Does the PAP Plan identify compensatory measures for essential protection program elements whose performance does not meet expectations?
- Has the site documented the essential elements of all protection programs?
- If so, are essential elements of the protection program security systems and subsystems whose failure would reduce protection to an unacceptable level tested at frequencies that provide high assurance of operability and reliability?
- Are testing frequencies documented for each essential protection program element (system and subsystem)?
- Does the PAP use detailed performance test plans, with objective and measureable performance criteria?
- Do performance tests result in formal reports? If so, is there a results tracking and trending capability?
- Are the PAP performance test results factored into the VA process?
- Does the PAP differentiate between operability, continuity, and reliability testing?
- Does the PAP require an annual integrated performance test for each Category I facility?

Federal Survey Program:

- Has the site office developed and approved comprehensive survey procedures, and are they consistent with DOE guidance?
- Are they followed?
- Is there an annual schedule of survey activities?

Appendix A—Inspection Tool Kit

- Are all topical and sub-topical areas surveyed annually?
- Is there evidence that sufficient expertise is included on survey teams to provide a valid review?
- Is sufficient time allowed for a survey to support a valid review?
- Are survey reports published in a timely manner, and are findings entered into the Safeguards and Security Information Management System (SSIMS) promptly and updated quarterly?
- Do survey report narratives support the conclusions reached in the report?
- Do survey reports comply with Departmental format and content requirements?
- Do identified deficiencies result in findings?
- What other mechanisms does the site office use to identify protection program weaknesses or opportunities for improvement?
- Does the site office incorporate the results of other governmental agency activities into the survey requirements?
- Does the site office maintain evidence files consisting of data collection sheets, performance test plans, and inspection plans to support survey report narratives?
- Do survey activities include a performance testing component?
- Are survey exit briefings conducted?

Performance Evaluation Plan (PEP):

- Do contractor PEPs include appropriate weight to effective performance/compliance for S&S programs?
- Do contractor PEPs address all applicable S&S topical areas?
- Do contractor PEPs adequately define:
 - Minimum S&S program performance?
 - Expected S&S program performance?
 - Realistic performance incentives?

Contractor Self-Assessments:

- Has the contractor(s) developed detailed self-assessment procedures?
- Are the contractor procedures being followed?

- Have the contractor self-assessment schedules and procedures been approved by the local DOE cognizant security authority?
- Do self-assessment reports meet DOE format and content requirements?
- Are all applicable S&S topics/sub-topics assessed between annual surveys?
- Is there an annual schedule of self-assessment activities?
- Is there evidence that sufficient expertise is included on self-assessment teams to provide a valid assessment?
- Do assessment reports comply with Departmental format and content requirements?
- Are assessments comprehensive enough to identify program weaknesses?
- Do report narratives support the conclusions reached in the report?
- Do identified deficiencies result in findings?
- Are assessment reports published in a timely manner, and are findings entered into an appropriate corrective actions tracking system?
- Does the contractor maintain evidence files consisting of data collection sheets, performance test plans, and inspection plans to support assessment report narratives?
- Do assessment activities include a performance testing component?
- Are exit briefings conducted?
- What other mechanisms does the contractor use to identify weaknesses or opportunities for improvement?
- Are findings and other items of note entered into a tracking system?

Resolution of Findings:

- Have both the site office and the contractor(s) developed formal procedures for resolving survey, self-assessment, and inspection findings?
- Are corrective action plans (CAPs) for findings submitted within 30 working days of the date of the exit briefing?
- 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?
- Are effective root cause analysis and cost-benefit analysis conducted?
- Is effective risk assessment performed?
- Are corrective actions completed on schedule?
- Are corrective actions adequately validated?
- Are corrective actions completed in a timeframe commensurate with the impact of the protection weakness?
- Are quarterly reports of the status of corrective actions for each finding provided to the appropriate cognizant security authority?
- Are there mechanisms to track and trend the resolution of findings?

Protection program management activities do not occur in a vacuum. They are intended to provide management with the data to effectively manage the S&S program. As a result, both significant strengths and significant weaknesses in the “operational” aspects of the S&S program impact the overall evaluation of the management of the S&S program.

Integration of Overall Safeguards and Security Program Implementation:

- Do the results of the other topical discipline reviews reflect effective protection program planning?
- Do the results of the other topical discipline reviews reflect effective use of appropriate oversight and feedback mechanisms?

**OFFICE OF INDEPENDENT OVERSIGHT
INSPECTION PLAN/NOTIFICATION LETTER
(EXAMPLE)**

**U.S. DEPARTMENT OF ENERGY
OFFICE OF HEALTH, SAFETY AND SECURITY
OFFICE OF INDEPENDENT OVERSIGHT
PLAN FOR THE SAFEGUARDS AND SECURITY
INSPECTION OF NAME OF SITE**

XXXX Inspection 200X

I. INTRODUCTION

This document outlines activities currently planned by the Office of Independent Oversight, within the Office of Health, Safety and Security, for evaluating line management of safeguards and security programs at the **NAME OF SITE**. Additionally, Independent Oversight will inspect activities at the site that directly support site security programs. Inspection activities will be conducted according to U.S. Department of Energy (DOE) Order 470.2B, *Independent Oversight and Performance Assurance Program*, which establishes the foundation for evaluation of program effectiveness. While this plan outlines projected evaluation activities, it should be understood that changes to specific activities and inspection focus areas will be made in response to emerging concerns and requests from key Headquarters managers. Site representatives will be kept informed of significant changes in proposed activities and inspection focus areas.

II. SCHEDULE

In order to minimize impact to the site, emphasis is placed on limiting the onsite evaluation efforts to only those activities that cannot be accomplished at Headquarters. The Headquarters planning stage includes line management interviews, documentation review, team orientation, and performance test coordination.

The inspection team will participate in an onsite planning visit from the dates of, **INSERT DATES**, during which time initial data gathering will also occur. Primary data collection activities, to include interviews, document and record reviews, limited-scope performance testing, and other performance observations, will be conducted during the periods of **INSERT DATES**. Other inspection activities, including large-scale, force-on-force performance tests, final data collection, validating inspection results, conducting factual accuracy reviews, finalizing a draft report, and conducting close-out activities, will be conducted during the period **INSERT DATES**. At the completion of the onsite inspection, a draft report will be issued and key managers and senior staff will be briefed on the inspection results consistent with Independent Oversight protocols.

III. INSPECTION TEAM RESPONSIBILITIES AND ASSIGNMENTS

The team leader, Acting Director, Office of Security Evaluations, will be the senior DOE official managing the evaluation activities as the inspection leader and also the senior Independent Oversight point of contact. He will be assisted by a deputy inspection team leader, technical specialists, and administrative support personnel. The inspection leader and his staff will ensure evaluation activities are conducted in accordance with approved procedures.

The evaluation team will be subdivided into subject areas. These areas will include Protection Program Management (PPM), Classified Matter Protection and Control (CMPC), Personnel Security (PS), Physical Security Systems (PSS), Protective Force (PF), Material Accountability and Control (MC&A), and Classification and Information Control (CIC).

DOE Order 470.2B assigns responsibility to the Heads of Field Elements to assist Independent Oversight in performing an effective and valid evaluation. This responsibility includes the provision of (1) access and support, (2) points of contact, and (3) validation of the factual content of the inspection data and report.

IV. INSPECTION PROCESS

Independent Oversight is charged with the independent oversight of safeguards and security; cyber security; emergency management programs; and environment, safety, and health (ES&H) throughout the Department. Independence is assured by a direct reporting relationship to the Office of the Secretary of Energy (i.e., outside any line management reporting chain) through the Chief Health, Safety and Security Officer. Further, Independent Oversight does not have any direct responsibility for facility operations, PPM, information systems management, or policy formulation.

Independent Oversight exercises independence in the conduct of inspections. Scheduling of inspections is independent of line management although valid concerns of site and DOE management are accommodated, whenever possible. Evaluations are based upon performance-based assessments of how sites implement the requirements established in DOE orders and directives with an emphasis on the effectiveness of the program elements. Independent Oversight also provides feedback on the effectiveness of orders and directives and whether they adequately establish effective program requirements. Consequently, Independent Oversight will employ the professional judgment of experienced inspectors to provide an overall evaluation of safeguards and security program status, including the impact of orders and directives governing implementation.

Emphasis on DOE Line Management and Self-assessment Processes

The primary purpose of Independent Oversight's assessment activities is to provide timely information to the Secretary of Energy and other senior Departmental managers on the status of Departmental safeguards and security; cyber security; emergency management; and ES&H programs. This information must be presented in a manner that supports and facilitates Secretarial-level actions to address identified shortcomings. Therefore, emphasis is placed on evaluating management performance, particularly DOE management direction and guidance for program implementation. Evaluation of the adequacy of DOE and contractor management assessment and self-assessment processes (feedback and improvement) is an important aspect of Independent Oversight's emphasis on management effectiveness, and is thus a major focus of the inspection. At the same time, the most fundamental management performance measure is the extent to which programs are effectively implemented. Thus, a central feature of Independent Oversight's inspections is the consideration of program effectiveness through performance testing, performance observations, and analysis of program documentation. While Independent Oversight's assessments provide a "snapshot in time" of performance, the analysis of inspection results will highlight program trends and provide evidence of progress or decline in overall performance, whenever such trends and evidence are discernable.

“Top-Down” Approach

Independent Oversight's role is not to duplicate surveys and assessments of safeguards and security, cyber security, emergency management, and ES&H topics that are conducted by other organizations. Rather, Independent Oversight's role is to provide an independent review of program effectiveness, which gives line management essential feedback on program status and direction. This leads to a "top-down" approach to evaluation planning that focuses on overall program effectiveness across the breadth of the program. However, as part of this approach, Independent Oversight recognizes the need to conduct carefully targeted, in-depth reviews of particular aspects of program implementation to effectively evaluate performance. Independent Oversight inspections are designed to balance the need for breadth and depth.

V. SCOPE OF THE EVALUATION

The Independent Oversight inspection will evaluate performance of line management responsible for safeguards and security programs at **NAME OF SITE**.

The major focus of the safeguards and security portion of the assessment is the evaluation of measures in place for the physical protection of special nuclear materials. Independent Oversight will pay particular attention to the effectiveness of site management in comprehensively and systematically addressing actions needed to correct findings identified during special reviews, surveys, self-assessments, and inspections.

As part of its overall program of protective force performance tests, Independent Oversight will conduct a series of large-scale, force-on-force tests designed to generate data with respect to individual and team tactical performance, command, control, communications, and other aspects of tactical response. Independent Oversight conducts such performance tests against the terrorist adversary capability defined by the DOE Graded Security Protection (GSP) Policy.

The inspection will also assess the protection that the site provides to classified and sensitive unclassified information. As part of the safeguards and security portion of the assessment, the following topical areas will be evaluated by Independent Oversight:

- Protection Program Management
- Classified Matter Protection and Control
- Classification and Information Control
- Personnel Security
- Physical Security Systems
- Protective Force Program
- Material Control and Accountability.

A common emphasis for the safeguards and security evaluation will be the performance of DOE line management, both in the field and at Headquarters, and also the effectiveness of feedback and improvement mechanisms such as surveys and self-assessments and their associated corrective action mechanisms. Although the focal point for reporting results in these areas will be the PPM appendix of the inspection report, this emphasis will incorporate data collection across all topical areas.

The inspection will be conducted according to formal protocols and procedures described in the *Office of Independent Oversight and Performance Assurance Appraisal Process Protocols*. This document

provides the general framework for the work processes used by Independent Oversight for conducting inspections. This general framework will be further supplemented by a variety of subordinate protocol documents including office-specific appraisal process guides, *Composite Adversary Team Standard Operating Procedure*, the relevant topical inspectors guides, and the Department’s protocols for conducting Protective Force Performance tests and exercises.

This plan outlines the overall scope and conduct of the inspection. Team members will develop individual schedules of onsite activities that supplement this overall plan. Appendix C contains detailed topical area scope and lines of inquiry.

VI. EVALUATION SAFETY

Independent Oversight considers safety to be of primary importance in all inspection activities. Special emphasis is placed on the safe conduct of safeguards and security performance tests, particularly force-on-force performance testing and protective force limited-scope performance tests. All performance tests will be carefully planned to minimize safety risks while achieving acceptable levels of realism. The performance test safety planning process includes a determination of potential safety hazards associated with anticipated performance tests and, where indicated, the preparation of written performance test safety plans designed to address these potential hazards. All routine evaluation activities will be conducted in accordance with site safety procedures.

VI. CORE INSPECTION TEA COMPOSITION

VII.

<u>Management Team</u>	Insert NAMES and TELEPHONE Numbers
<u>Program Management</u>	Insert NAMES and TELEPHONE Numbers
<u>Protective Force</u>	Insert NAMES and TELEPHONE Numbers
<u>Performance Testing</u>	Insert NAMES and TELEPHONE Numbers
<u>Physical Security Systems</u>	Insert NAMES and TELEPHONE Numbers
<u>Personnel Security</u>	Insert NAMES and TELEPHONE Numbers
<u>Classified Matter Protection and Control</u>	Insert NAMES and TELEPHONE Numbers
<u>Material Control & Accountability</u>	Insert NAMES and TELEPHONE Numbers
<u>Classification Information and Control</u>	Insert NAMES and TELEPHONE Numbers

Note: The core inspection team will be supported by an administrative support component, a performance testing component, augmentees from DOE and National Nuclear Safety Administration (NNSA) sites, and other members of the Office of Independent Oversight brought in for limited roles. These names will be provided to the site as part of normal coordination activities.

Inspection Schedule (Example)

Planning and Data Collection Visit – January 11 – January 16, 2009

January 11, 2009	Team Members Travel
January 12, 2009	
7:30 a.m. – 8:30 a.m.	Badging
8:30 a.m. – 9:30 a.m.	In-Brief (Proposed)
9:30 a.m. – 10:30 a.m.	Training (Proposed)
10:30 a.m. – 5:00 p.m.	Planning, Data Collection, Document Review, and Interviews
January 13-15, 2009	
8:00 a.m. – 5:00 p.m.	Planning, Data Collection, Document Review, and Interviews
5:00 p.m. – 6:00 p.m.	Team Meeting
January 16, 2009	Team Members Travel Home

Data Collection Visit – January 25 - 30, 2009

January 25, 2009	Team Members Travel
January 26 - 29, 2009	
8:00 a.m. – 5:00 p.m.	Planning, Data Collection, Document Review, and Interviews
5:00 p.m. – 6:00 p.m.	Team Meeting
January 30, 2009	Team Members Travel Home

Performance Testing, Data Collection, Validation and Closeout Activities – February 22 – March 6, 2009

February 22, 2009	Team Members Travel
February 23 - 28, 2009	
8:00 a.m. – 5:00 p.m.	Data Collection, Performance Testing, Report Writing, and Validation
5:00 p.m. – 6:00 p.m.	Team Meeting
March 2, 2009	
8:00 a.m. – 5:00 p.m.	Quality Review Board
March 3, 2009	
8:00 a.m. – 5:00 p.m.	Quality Review Board
March 4, 2009	
8:00 a.m. – 5:00 p.m.	Comment Resolution
March 5, 2009	
TBD	Out-brief
March 6, 2009	Team Members Travel Home

This page intentionally left blank.

**(EXAMPLE)
INFORMATION REQUEST
OFFICE OF INDEPENDENT OVERSIGHT
SAFEGUARDS AND SECURITY INSPECTION OF
XXXXXX
(Inspection timeframe ENTER DATES)**

The requested documentation is required to support the inspection activities. Please provide the documents as appropriate. In general, requested documentation should be made available for review by the Inspection Team in the team work space at the beginning of the planning visit to be held during the week starting (ENTER DATE) and throughout the onsite portion of the inspection. The exact titles and terminology of documents may differ; if the request is unclear, please contact the Independent Oversight point of contact. Some documents are being requested prior to the beginning of the onsite inspection. Those documents are specifically identified along with the requested dates for submittal. The documents represent a departure point for inspection planning, data collection, and performance testing. Depending upon the availability and results of initial document reviews and interviews, other data and documentation may be requested.

Documentation provided to the team space may be in paper form. Any documentation sent to the topic leads, or their alternates, prior to the inspection should be provided in electronic format, where possible. In addition, please provide an inventory of provided documentation, indexed according to the numbering scheme used by each topic. Requested information or procedures that have not been developed, are not available, or are not provided, should be identified as “Not Available.”

Any classified information must be transmitted to Headquarters, Germantown, according to U.S. Department of Energy (DOE) directives for mailing classified information or retained at the site for review upon arrival.

Contact the designated Independent Oversight topic leaders if there are questions or if clarifications are necessary.

Protection Program Management

Questions regarding the data call for Protection Program Management should be addressed to Team Leader’s Name at His/her phone number or through e-mail at email_address@hq.doe.gov. The following items should be sent to HS-61, Headquarters, Germantown, care of “Team Leader” no later than (ENTER DATE). Documents of a size that make shipping to Germantown prohibitively expensive (specifically, original paper copies of evidence files for surveys, self-assessments, and corrective actions) should be made available in the work space at the beginning of the inspection. Please note that a series of briefings have been requested to facilitate addressing planning, tactical doctrine, and both Federal and contractor oversight processes. If requested plans have recently been changed, please include the plans of record for the review period. For example, if the survey guidance was recently changed, also include the survey guidance of record used for the previous survey period.

Planning Documentation

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

2. Vulnerability Assessment (VA) and Site Safeguards and Security Plan (SSSP) or Site Security Plan (SSP) development process protocol documents. Examples include:
 - a. Process for developing adversary strategies/tactics
 - b. Process for evaluating insider adversaries, both working alone and in collusion with the outsider
 - c. Process for conducting Joint Conflict and Tactical Simulations (JCATS) analyses and developing neutralization values
 - d. Process for developing and evaluating upgrade packages
 - e. Presentation of chronological efforts and events leading up to the current/approved SSP (include VAs, validations, peer reviews, Headquarters visits, etc.)
3. Data from protective force performance testing that supports the most recent vulnerability analysis or protective force performance assumptions made in the VAs requested above, particularly any performance tests included in the calculation of the probability of neutralization.
4. Most recently approved SSP, the most current draft of each SSP (if revisions are underway), and the catalog listing of evidence files supporting the approved SSSP/SSP and supporting VAs.
5. A listing of Adversary Time Line Analysis System (ATLAS) and Analytic System and Software for Evaluating Safeguards and Security (ASSESS) files used to develop the above listed VA reports, and the associated evidence files for the following types of data:
 - a. modeling inputs
 - b. protective force response
 - c. adversary capabilities
 - d. blast effects
 - e. sabotage data (if appropriate)
 - f. timeline data
 - g. neutralization data
 - h. special weapons effectiveness.
6. If tabletop/qualitative methods were used, copies of any meeting notes and supporting documentations for ratings.
7. SECON Implementation Plans, including an index to the appropriate protective force plans and associated security/operations procedures.
8. Most recent Design Basis Threat (DBT) Implementation Plan and status.
9. List of deviations from DOE requirements and application packages.
10. SSSP/SSP Resource Plan.
11. Records that indicate progress towards the emerging General Protection Strategy model for VAs.
12. A “Vulnerability Assessment Process” briefing should be prepared for presentation during the first week of the inspection that reflects the implementation of DOE planning requirements and how they are integrated in planning, equipment selection and utilization, barrier placement, and protective force organization and training, and what mechanisms provide VA analysts with performance-tested validation of VA assumptions and values.

Tactical Doctrine

13. Documents that reflect the implementation of DOE Tactical Doctrine in planning, equipment selection and utilization, barrier placement, and protective force organization and training.
14. A “Tactical Doctrine Implementation” briefing should be prepared for presentation during the first week of the inspection that reflects the implementation of DOE Tactical Doctrine in planning, equipment selection and utilization, barrier placement, and protective force organization and training. This briefing normally describes how the detection system, barriers, and neutralization processes are integrated and also addresses efforts to mitigate legacy issues concerning terrain or other limiting factors (if necessary).

Performance Assurance Plan

15. Performance Assurance Plan (guidance), performance assurance test schedule, and results of tests for the past two years (ENTER DATES).
16. Listing of critical and essential elements. Indicate their location in the SSSP if appropriate.
17. Performance Assurance Test Plans for critical systems and elements.

Safeguards and Security (S&S) Management Plan (or equivalent as permitted)

18. Organizational charts for all elements, Federal site office and contractor (including significant S&S subcontractors), that have S&S responsibilities. Where S&S topical and sub-topical responsibilities are apportioned among organizations, provide an overall organization chart indicating the interrelationships of all topics/parties in the conduct of the S&S program.
19. Provide the Federal site office and contractor missions and function manuals or other reference materials that describe the roles and responsibilities of current site organizations, including deliverables and accountability within the S&S program.

Feedback, and Improvement Documentation

Federal Survey Program

20. Documents describing the implementing procedures, individual topic survey plans, evidence files including performance (based) test plans from individual surveys, and schedules for the Federal site office surveys and the Federal self-assessment program.
21. Copies of individual topic survey assessment activities and self-assessment reports (evidence files) conducted during the past three years.
22. Federal site office procedures for addressing external inspection, survey, and self-assessment issues, findings, concerns, observations, and/or other action items related to the mitigation of identified Federal site office weaknesses in the S&S program.

23. Corrective action plans for all inspection, survey, and self-assessment issues, findings, concerns, and/or observations for the last two years.
24. Records (other than the Safeguards and Security Information Management System or SSIMS) that reflect DOE verification, validation, and closure of issues, findings, concerns, and/or observations for the past two years.
25. A “Federal Oversight” briefing should be prepared for presentation during the first week of the inspection that reflects the implementation of DOE Manual 470.4-1 and DOE Order 226.1A requirements for integrated oversight.

Contract Performance Evaluation Plan/Program

26. The portion(s) of the Federal guidance and site contract that describe the Performance Evaluation Plan measures and performance award measurement process associated with contractor performance in S&S. Include documents that reflect the real dollar and percentage values in relation to the total site contract value, total fixed/award/stretch fee amounts.
27. Copies of the contractor’s performance assessments of themselves (if part of the award fee process) and the narratives of Federal assessments of the contractor for the last two reporting periods.

Contractor’s Self-Assessment Program

28. Documents and a briefing during the first inspection week describing the contractor S&S self-assessment program. Indicate how/if the contractor has elected to integrate the performance assurance program, testing and maintenance results, protective force limited-scope performance tests, training, alarm response and assessment performance tests, etc., to accomplish the self-assessment program objectives.
29. Copies of self-assessment reports conducted during the last two years.
30. Provide the location (not copies) of the individual assessment plans and evidence files of individual completed assessments for each assessment topic.
31. Contractor procedures for addressing inspection, survey, and self-assessment issues; findings; concerns; observations; and/or other action items related to the mitigation of identified contractor weaknesses in the S&S program.
32. Corrective action plans for all inspection, survey, and self-assessment issues; findings; concerns; and/or observations identified during the last two years.
33. Records (other than SSIMS) that reflect DOE and contractor verification, validation and closure of issues, findings, concerns, and/or observations for the last two years.
34. A “Contractor Oversight” briefing should be prepared for presentation during the first week of the inspection that reflects the implementation of DOE Manual 470.4-1 and DOE Order 226.1A requirements for integrated oversight.

**PROTECTION PROGRAM MANAGEMENT
DETAILED INSPECTION PLAN (EXAMPLE)**

PROTECTION PROGRAM MANAGEMENT DETAILED INSPECTION PLAN (EXAMPLE)

The lines of inquiry 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
<p><u>PLANNING:</u></p> <ol style="list-style-type: none"> 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? <p><u>IMPACT:</u> 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.</p>			
<p>Management: Personal competence and training are maintained by management making adequate resources available to perform all security program functions.</p>	<p>Are resources (staffing and budget) planned to adequately support the structure; do they demonstrate timely completion of functional requirements?</p>	<ol style="list-style-type: none"> 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. 	<p>pre-planning</p> <p>pre-planning and onsite</p> <p>pre-planning</p>

PERFORMANCE MEASURE	CRITICAL CRITERIA/LINES OF INQUIRY	DATA COLLECTION ACTIVITIES	REMARKS
<p>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.</p> <p>Management ensures that security plans, policies, and priorities are adjusted to meet changing threat situations.</p>	<p>1. Are security concerns adequately addressed in the site operational and security planning processes?</p> <p>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?</p> <p>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?</p>	<p>1. Interview managers and security professionals to determine the extent to which security professionals participate in planning meetings, budget discussions, and management-level decisions.</p> <p>2. Review the SSSP/SSP and other security and operational planning documents to determine the manner in which security concerns are addressed.</p> <p>3. Review site policies to determine whether security program officials are in a position to ensure compliance.</p> <p>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).</p> <p>5. Review site security program procedures to determine whether they are accurate and comprehensive.</p> <p>6. Interview managers to determine what incentives are used to encourage good performance.</p>	<p>onsite</p> <p>pre-planning</p> <p>pre-planning</p> <p>onsite</p> <p>pre-planning</p> <p>onsite</p>
<p>Management: Feedback and improvement is supported by effective self-assessment and corrective action programs.</p>	<p>1. Has the self-assessment program identified significant program weaknesses that, when addressed, would materially enhance program implementation?</p> <p>2. Does the corrective action process include all the required elements (i.e., analyze root cause and prioritize actions, establish corrective</p>	<p>1. Review past self-assessments to determine whether they reflect thorough coverage of the security program and are conducted on a regular basis.</p> <p>2. Review records to determine who conducts the self-assessments and their qualifications.</p> <p>3. Review records to determine whether concerns</p>	<p>pre-planning</p> <p>pre-planning</p> <p>pre-planning</p>

PERFORMANCE MEASURE	CRITICAL CRITERIA/LINES OF INQUIRY	DATA COLLECTION ACTIVITIES	REMARKS
	action schedule that will allow monitoring 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?	<p>identified during self-assessments are entered into a central tracking system.</p> <p>4. Review procedures to determine whether the corrective action process contains all the required elements.</p> <p>5. Review records to determine whether some form of independent verification of closure of findings is in place.</p>	<p>pre-planning</p> <p>pre-planning</p>

**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. <i>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.</i>
Review site protection strategy, VAs/SSSP/SSP 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 the 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 sub-topic 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/sub-topic 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

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
<p>Collect data, Tuesday-Thursday</p> <ul style="list-style-type: none"> -Interview security program officials and specialists. -Complete reviews and record results on file review form. <p>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).</p>		Team
<i>Must keep Team Leader informed of location and phone number (may be done via administrative support personnel).</i>		Team
Daily , prepare data collection forms (personal preference: either complete before the daily team meeting, or 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 Issue Forms (when required) and the inspection report.		Team

Distribute to Deputy Inspection Chief and Administrative Coordinator.		
When required, prepare Issue Forms.		Team Member
Review Issue Forms and provide to inspection management.		Team Leader
Resolve site comments.		Team Leader and Member
<p>Topic team discusses results of data collection, leading to the drafting of evening bullets, and confirms/revises schedule (should occur briefly before the daily meeting, over the phone if necessary).</p> <p>*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.</p> <p>*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).</p> <p><i>Assign a team member the responsibility to capture on an Issue Form any issues that could impact the rating.</i> (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.)</p>		Team Leader
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: <ul style="list-style-type: none"> - 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 (<i>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</i>). - 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 a summary of initial results and to schedule future data collection activities for HRP, safeguards and security awareness, and unclassified foreign visits and assignments, Thursday		Team
Identify and destroy unwanted papers; return pagers, keys, and dosimeters to administrative support personnel, Thursday		Team
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
<p>Collect data, Tuesday through Thursday</p> <ul style="list-style-type: none"> - Follow up on any issues related to the security program. <p>Validate data (as team will be split, each team member will validate data as it is collected and then summarize with the attending field points of contact when a data collection activity is completed).</p> <p>*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.</p> <p>*Issues that could impact the topic rating should normally be discussed in the evening meeting only after:</p> <ul style="list-style-type: none"> - 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). 		<p>Team</p> <p>Team</p> <p>Team Leader</p> <p>Team Leader</p>

<i>Assign a team member to prepare an Issue Form as soon as such an issue has been identified.</i>		
<i>Must keep Team Leader informed of location and phone number (do not rely on administrative support personnel).</i>		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
Principal writer continues work on the draft appendix by completing work on security program sub-section, Wednesday		Principal Writer
Sub-topic 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		Team

that might obscure the presentation of the key points – Findings – Policy issues – Proposed rating		
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
Address QRB/site comments (inform QRB 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

**PROTECTION PROGRAM PLANNING
WEEKLY SCHEDULES**

(EXAMPLES)

PROTECTION PROGRAM MANAGEMENT PLANNING SCHEDULE-WEEK 1 (EXAMPLE)

Day	Time	Activity	HS-61 Participants	Site Participants
Monday	7:30 – 11:30	In-brief & Site Training		
	Afternoon	Survey/Self-assessment Programs Deviations Security planning/VA Oversight Briefing-location TBD		
	1530 1630 1700	Daily Validation w/site PPM Bullets Integration Topic Integration Meeting		Fed/Site managers
Tuesday	Morning	Survey/Self-assessment Programs Deviations Security Planning/VA		
	Afternoon 1530 1630 1700	Survey/Self-assessment Programs Daily Validation w/site PPM Bullets Integration Topic Integration Meeting		Fed/Site managers
Wednesday	Morning	Survey/Self-assessment Programs Performance Assurance Program GSP/SECONS		
	Afternoon 1530 1630 1700	Daily Validation w/site PPM Bullets Integration Topic Integration Meeting		Fed/Site managers
Thursday	Morning	Survey/Self-assessment Programs Performance Assurance Program GSP/SECONS		
	Afternoon	Survey Program Performance Assurance Program PPM Summary Bullets 1 st Week Summary Validation		Fed/Site managers

Appointment locations to be determined.

Daily and weekly summary validation appointments will be conducted to assure that managers are aware of what strengths and weaknesses have been validated/will be validated with Federal and contractor staffs during that day/week.

PPM will assess Tactical Doctrine and provide PF and FOF HS-61 Test Director with the results of the assessment as related to VA's, the SSSP, and PAP.

-Topical writing assignments are the same as those assigned for data collection.

-OFI's - ALL

PROTECTION PROGRAM MANAGEMENT PLANNING SCHEDULE WEEK 2 (EXAMPLE)

Day	Time	Activity	HS-61 Participants	Site Participants
Monday	Morning	S&S Management Plan Performance Assurance Program		
	Afternoon	Performance Assurance Program Writing		
	1530 1630 1700	Daily Validation w/site PPM Bullets Integration Topic Integration Meeting		Fed/Site managers
Tuesday	Morning	Tactical Doctrine Senior Manager Interviews		
	Afternoon 1530 1630 1700	Daily Validation w/site PPM Bullets Integration Topic Integration Meeting		Fed/Site managers
Wednesday	Morning	Writing		
		Topical Integration Section		
	Afternoon 1530 1630 1700	Daily Validation w/site PPM Bullets Integration Topic Integration Meeting		Fed/Site managers
Thursday	Morning	Tactical Doctrine Integration Writing		PF/PSS/Testing/VA
	Afternoon	PPM Weekly Summary 2 nd Week Summary Validation		Fed/Site managers

This page intentionally left blank.

TOOLS RELATED TO SECTION 2, PLANNING PROCESS

Tool 2-1: Planning Worksheet.....	A-37
Tool 2-2: Document Checklist.....	A-38
Tool 2-3: Plan Evaluation Worksheet	A-40
Tool 2-4: Safeguards and Security Plan Detailed Review.....	A-42
Tool 2-5: Vulnerability Assessment Report Detailed Review	A-45
Tool 2-6: ASSESS/ATLAS Facility Characterization Files Detailed Review	A-48
Tool 2-7: ASSESS/ATLAS Outsider Analysis Detailed Review	A-51
Tool 2-8: ASSESS/ATLAS Insider File Detailed Review	A-53
Tool 2-9: JTS/JCATS Neutralization Analysis.....	A-55
Tool 2-10: Tabletop/Qualitative Evaluations	A-58
Tool 2-11: Vulnerability Assessment Summary Analysis Table	A-62
Tool 2-12: Deviations Assessment.....	A-66

Tool 2-1

**PLANNING WORKSHEET
FOR
PROTECTION PROGRAM MANAGEMENT**

Facility/Site: _____

Sub-topic: _____ Issue: _____

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

Tool 2-2

DOCUMENT CHECKLIST

Facility/Site: _____ Date of Evaluation: _____

TOPIC AREA	DOCUMENT	EXISTS?	ADEQUATE?	REVIEWER COMMENTS
Protection Program Planning	Site Safeguards and Security Plan or Site Security Plan	<input type="checkbox"/> Yes <input type="checkbox"/> No	<input type="checkbox"/> Yes <input type="checkbox"/> No	
	Performance Assurance Program Plan	<input type="checkbox"/> Yes <input type="checkbox"/> No	<input type="checkbox"/> Yes <input type="checkbox"/> No	
	GSP Implementation Plan	<input type="checkbox"/> Yes <input type="checkbox"/> No	<input type="checkbox"/> Yes <input type="checkbox"/> No	
	SECON Plan	<input type="checkbox"/> Yes <input type="checkbox"/> No	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Protection Program Management	SSMP or equivalent	<input type="checkbox"/> Yes <input type="checkbox"/> No	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Protection Program Feedback	Survey Program Procedures	<input type="checkbox"/> Yes <input type="checkbox"/> No	<input type="checkbox"/> Yes <input type="checkbox"/> No	
	Survey Program Reports	<input type="checkbox"/> Yes <input type="checkbox"/> No	<input type="checkbox"/> Yes <input type="checkbox"/> No	

TOPIC AREA	DOCUMENT	EXISTS?	ADEQUATE?	REVIEWER COMMENTS
	Self-assessment Procedures	<input type="checkbox"/> Yes <input type="checkbox"/> No	<input type="checkbox"/> Yes <input type="checkbox"/> No	
	Self-assessment Reports: Individual Topics? Annual Roll-up?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Yes <input type="checkbox"/> No	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Yes <input type="checkbox"/> No	
	Corrective Action or Issue Management Plans	<input type="checkbox"/> Yes <input type="checkbox"/> No	<input type="checkbox"/> Yes <input type="checkbox"/> No	
	Issue Tracking/Trending Process	<input type="checkbox"/> Yes <input type="checkbox"/> No	<input type="checkbox"/> Yes <input type="checkbox"/> 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			<input type="checkbox"/> Sufficient <input type="checkbox"/> Insufficient	
General Approach			<input type="checkbox"/> Sufficient <input type="checkbox"/> Insufficient	
Task Definition			<input type="checkbox"/> Sufficient <input type="checkbox"/> Insufficient	
Priority of Tasks			<input type="checkbox"/> Sufficient <input type="checkbox"/> Insufficient	
Task Linkages			<input type="checkbox"/> Sufficient <input type="checkbox"/> Insufficient	
Identification of Resources			<input type="checkbox"/> Sufficient <input type="checkbox"/> Insufficient	

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

Tool 2-4

**SAFEGUARDS AND SECURITY PLAN
DETAILED REVIEW**

SSSP/SSP DATA COLLECTION QUESTIONS		YES	NO
1.	Has the SSSP/SSP 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 SSP?		
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/SSP 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/SSP accurately describe the site’s mission as well as the mission of listed facilities?		
	If not, explain:		
7.	Does the SSSP/SSP accurately describe and reflect the status of the site’s S&S program?		
	If not, explain:		

SSSP/SSP DATA COLLECTION QUESTIONS		YES	NO
8.	Does the SSSP/SSP 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/SSP describe the current level of system effectiveness (risk) for each key facility and target?		
	If no, explain:		

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

Tool 2-5

VULNERABILITY ASSESSMENT REPORT
DETAILED REVIEW

Facility: _____

VULNERABILITY ASSESSMENT QUESTIONS		YES	NO
1.	Are VAs based on the current Graded Protection Policy Order?		
	<ul style="list-style-type: none"> If not, why? 		
2.	Adversary Acts:		
	<ul style="list-style-type: none"> Theft of SNM? 		
	<ul style="list-style-type: none"> Radiological sabotage? 		
	<ul style="list-style-type: none"> Critical mission curtailment? 		
	<ul style="list-style-type: none"> Weapons of Mass Destruction? 		
	<ul style="list-style-type: none"> Other: 		
3.	Do VAs address the following aspects of the DBT:		
	<ul style="list-style-type: none"> Terrorists acting alone? 		
	<ul style="list-style-type: none"> Terrorists colluding with a passive insider? 		
	<ul style="list-style-type: none"> Terrorists colluding with an active insider? 		
	<ul style="list-style-type: none"> Terrorists colluding with a violent insider? 		
	<ul style="list-style-type: none"> Criminals acting alone? 		
	<ul style="list-style-type: none"> Criminals colluding with a passive insider? 		
	<ul style="list-style-type: none"> Criminals colluding with an active insider? 		
	<ul style="list-style-type: none"> Criminals colluding with a violent insider? 		
	Explain any outsider threats that were not analyzed:		
	<ul style="list-style-type: none"> Active non-violent insiders? 		
	<ul style="list-style-type: none"> 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.	Were Representative Scenarios approved through the Scenario Development Review process?		
	• If no, provide rationale.		
11.	Do the Representative Scenarios adequately evaluate the site’s protection program, and are the following types of attacks addressed? If not, why?		
	• 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:	<i>Describe Concern</i>
• Dimensions	
• Characteristics	
• Passage	
- Vehicles	
- Personnel	
- Materials	
• Safeguards	
- Access Control	
Evidence Files	<u>File/Document Name:</u> <u>Date:</u> <u>Location:</u> <u>Comment:</u>
- Contraband Detection	
Evidence Files	<u>File/Document Name:</u> <u>Date:</u> <u>Location:</u> <u>Comment:</u>
- SNM Detection	
Evidence Files	<u>File/Document Name:</u> <u>Date:</u> <u>Location:</u> <u>Comment:</u>
- Material Transfers	
Evidence Files	<u>File/Document Name:</u> <u>Date:</u> <u>Location:</u> <u>Comment:</u>

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

Tool 2-7

ASSESS/ATLAS OUTSIDER ANALYSIS
 DETAILED REVIEW

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

FACILITY:	FILE NAME:
RFT:	ADVERSARY:
STATE:	STRATEGY:
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:		
•			

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?			

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:			
	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 to the attack in a coordinated fashion?		
	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:		

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:			
10.	Was the Adversary appropriately aggressive?		
	If not, explain:		
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?						
	<u>File/Document Name:</u> <u>Date:</u> <u>Location:</u> <u>Comment:</u>						

FACILITY:	STATE:	DATES OF EVALUATION:		
ADVERSARY OBJECTIVE:				
TYPE OF ADVERSARY:	NUMBER OF ADVERSARIES:	NUMBER OF PRO-FORCE:	PRO-FORCE RESPONSE STRATEGY:	
QUESTIONS			YES	NO
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 Adversary Capabilities List?			
	If not, explain:			
8.	Does the amount and type of ammunition assigned to each unit seem reasonable?			
	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
9.	Were Pro-Force tactics consistent with training?			
	If not, explain:			
10.	Did the Pro-Force respond to the attack in a coordinated fashion?			
	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:			

FACILITY:	STATE:	DATES OF EVALUATION:		
ADVERSARY OBJECTIVE:				
TYPE OF ADVERSARY:	NUMBER OF ADVERSARIES:	NUMBER OF PRO-FORCE:	PRO-FORCE RESPONSE STRATEGY:	
QUESTIONS			YES	NO
13.	Was the Adversary attack well planned and coordinated?			
	If not, explain:			
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					
Non-violent Insider					
- Personnel Characterization					
- Assumptions					
- Strategies					
- Capabilities					
- User-defined Settings					

	N/A*	A	M	I	REMARKS
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					
Protective Force Tactics					
- Compatibility w/existing tactical response plans					
- Use of resources					
- Compatibility w/normal operations and training					

	N/A*	A	M	I	REMARKS
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?					<input type="checkbox"/> YES <input type="checkbox"/> MARGINAL <input type="checkbox"/> NO

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

Tool 2-12

DEVIATIONS ASSESSMENT

The purpose of this questionnaire is to assist individual topic teams in their evaluation of the pending and approved deviations to the requirements for their topic. This data will assist the PPM topic in identifying the overall site compliance with requirements for deviations and help identify potential trends among topics. These questions are derived from the requirements in DOE Manual 470.4-1, Change 1, Section M. PPM normally assesses only approved deviations and comments on pending deviations as necessary. Users should use care to preclude creating a potentially classified work sheet.

1. Are deviations appropriately characterized as variances, waivers, or exceptions based on:
 - Variance: Equivalent but different method to comply (for example, iron bar fence in lieu of required chain link) with DOE requirements without compensatory measures
 - Waiver: Requires compensatory measures to preclude real or potential vulnerabilities
 - Exception: Inability to meet requirement that creates vulnerabilities for which there are no adequate compensatory measures?

Please provide examples using the site deviation number and describe the deficiency.

2. Are deviations documented in the SSSP/SSP?
3. Are deviations implemented prior to approval?
4. Are deviations approved at the appropriate level of authority?
5. Do deviation requests fully and accurately describe associated vulnerabilities?
6. Are the results of VAs and tests documented in the deviation request?
7. Do compensatory measures appear adequate? If not, please suggest workable alternatives.
8. Are compensatory measures monitored by the Departmental element?

This page intentionally left blank.

TOOLS RELATED TO SECTIONS 3 and 4, FEDERAL AND CONTRACTOR OVERSIGHT

Tool 3-1: Lines of InquiryA-69
Tool 3-2: Survey and Self-Assessment Reports ReviewA-75
Tool 3-3: Topical Team Survey and Self-Assessment Evaluation.....A-78
Tool 3-4: Topical Team Performance Assurance Program Evaluation.....A-81
Tool 3-5: Overall Performance Evaluation for OversightA-82

Tool 3-1

**LINES OF INQUIRY
Federal and Contractor Oversight**

Inspectors may use the following lines of inquiry to validate the comprehensiveness of activities supporting a site’s performance assurance, survey, self-assessment, and resolution of findings programs:

Lines of Inquiry Concerning Performance Assurance Programs (PAPs)
<ul style="list-style-type: none"> • Has the PAP been developed, managed, and implemented to ensure that S&S programs and protection program elements protect security interests and activities?
<ul style="list-style-type: none"> • Does the PAP describe the program and its administration and implementation by: <ol style="list-style-type: none"> 1. Identifying ESSENTIAL protection elements for the protection of Category I and II special nuclear material (SNM) and Top Secret matter? 2. Describing how the performance of these elements is to be ensured, including the manner in which credit is taken for activities performed by external oversight organizations? 3. Identifying how deficiencies identified during performance assurance activities are to be corrected?
<ul style="list-style-type: none"> • Does the PAP validate the operability and performance effectiveness of all essential S&S elements and components?
<ul style="list-style-type: none"> • Is there a management and planning process to achieve integrated, site-specific testing of critical essential protection program elements?
<ul style="list-style-type: none"> • Is the management and planning process based on a graded approach that implements the integrated concepts of deterrence, prevention, detection, and interdiction/neutralization?
<ul style="list-style-type: none"> • Do PAP operability tests verify the integrity of all elements of a component or system to confirm operability?
<ul style="list-style-type: none"> • Do PAP performance tests provide comprehensive assurance that all elements of a layered S&S system are performing as designed and provide the required levels of protection?
<ul style="list-style-type: none"> • Are limited-scope performance tests and force-on-force (FoF) exercises used to meet specific performance assurance testing requirements?
<ul style="list-style-type: none"> • Do performance tests ensure that approved protection strategies of denial, containment, recapture, recovery, and pursuit can be accomplished by the PF?
<ul style="list-style-type: none"> • Is the PAP evaluated as part of the facility survey and self-assessment program?
<ul style="list-style-type: none"> • Are new protection program essential elements and components validated through acceptance testing before operational use?
<ul style="list-style-type: none"> • Are essential protection program elements that have been repaired or undergone maintenance validated through testing before resumption of use?
<ul style="list-style-type: none"> • Is the PF performance tested both individually and in small tactical units?
<ul style="list-style-type: none"> • Do the performance tests ensure that approved protection strategies of denial, containment, recapture, recovery, and pursuit can be accomplished by the PF?
<ul style="list-style-type: none"> • Are essential elements of the protection program security systems and subsystems whose failure would

reduce protection to an unacceptable level tested at frequencies that provide high assurance of operability and reliability?
<ul style="list-style-type: none"> • Are testing frequencies documented for each essential protection program element (system and subsystem)?
<ul style="list-style-type: none"> • Is there an integrated performance test encompassing all essential protection elements associated with a comprehensive site or facility scenario that is conducted at least every 365 days?
<ul style="list-style-type: none"> • Do Category I facilities requiring denial protection strategies conduct integrated performance testing on a quarterly (at least every 3 months) basis?
OR
<ul style="list-style-type: none"> • Do sites with multiple Category I facilities requiring denial protection strategies rotate quarterly performance testing so that at least one facility is tested on a quarterly basis (at least every 3 months) with an integrated performance test for all Category I facilities accomplished at least once every 365 days?
<ul style="list-style-type: none"> • Are the results of PAP tests documented?
<ul style="list-style-type: none"> • Does the record keeping system provide an audit trail for performance assurance activities and reports?
Lines of Inquiry Concerning Federal Surveys and Contractor Self-assessments
<ul style="list-style-type: none"> • Do the survey and self-assessment programs provide assurance that S&S interests and activities are protected at the required levels?
<ul style="list-style-type: none"> • Do the survey and self-assessment programs provide compliance and performance-based documentation of the evaluation of the S&S program?
<ul style="list-style-type: none"> • Are the survey and self-assessment procedures approved by the appropriate cognizant security authority?
<ul style="list-style-type: none"> • Does the contractor conduct self-assessments between the periodic surveys conducted by the DOE cognizant security authority?
<ul style="list-style-type: none"> • Do the surveys and contractor self-assessments include all applicable facility S&S program elements and provide an integrated evaluation of all topical and sub-topical areas to determine the overall status of the S&S program?
<ul style="list-style-type: none"> • Is any decision not to use all sub-topical areas documented in a local procedure?
<ul style="list-style-type: none"> • Does the scope of the activities and methods used for the survey and self-assessment programs include the following: <ol style="list-style-type: none"> 1. Compliance – are applicable statutes, regulations, policies, plans, and other directives appropriately followed? 2. Performance – do the elements of the S&S self-assessment program meet the objectives of the protection program based on operational testing of program elements? 3. Comprehensiveness – does the self-assessment program evaluate the adequacy and effectiveness of programs and [reflect] a thorough examination of the implementation of policies, practices, and procedures to ensure compliance and performance with requirements?
<ul style="list-style-type: none"> • Do Federal and contractor survey and self-assessment team members possess qualifications, experience, and training sufficient to review and inspect the topical/sub-topical areas being assessed?

<ul style="list-style-type: none"> • Are surveys and self-assessments planned, scheduled, and conducted in an integrated manner and if topical and sub-topical area evaluations are performed separately, are results documented and integrated into a single (periodic) report that includes a composite rating?
<ul style="list-style-type: none"> • Are the results of surveys and self-assessments validated by document reviews, performance testing, interviews, analyses, and observations?
<ul style="list-style-type: none"> • Are all open findings from previous assessments [from any source/agency] reviewed to validate the status of corrective action and to evaluate the impact on the existing S&S program?
<ul style="list-style-type: none"> • Are findings that may have programmatic impact on vulnerability to national security, classified information or matter, nuclear materials, or Departmental property immediately reported to the Departmental element and contractor line management?
<ul style="list-style-type: none"> • Are findings corrected during a survey or self-assessment identified in the report with a description of the closure/validation performed by the survey or self-assessment team?
<ul style="list-style-type: none"> • Are ratings based on the effectiveness and adequacy of the program and do they reflect a balance of performance and compliance results as well as the impact of the deficiency/deficiencies and mitigating factors?
<ul style="list-style-type: none"> • Are the following topical and sub-topical ratings used:
<ol style="list-style-type: none"> 1. Satisfactory – meets protection objectives or provides reasonable assurance that the objectives are being met.
<ol style="list-style-type: none"> 2. Marginal – partially meets protection objectives or provides questionable assurance that the objectives are being met.
<ol style="list-style-type: none"> 3. Unsatisfactory – does not meet protection objectives or does not provide adequate assurance that objectives are being met.
<ul style="list-style-type: none"> • Do overall survey ratings reflect – “Effective Performance,” “Needs Improvement,” or “Significant Weaknesses”?
<ul style="list-style-type: none"> • Are ratings based on existing conditions at the end of the survey or assessment and not on future or planned corrective actions or conditions?
<ul style="list-style-type: none"> • Are ratings based on the impact of all open deficiencies, regardless of source?
<ul style="list-style-type: none"> • Are less-than-satisfactory ratings in any topical area based on validated weaknesses in the S&S system or deficiencies in performance?
<ul style="list-style-type: none"> • Are repeat topical area marginal ratings for consecutive survey or assessment periods assigned an unsatisfactory rating unless one of the following conditions applies:
<ol style="list-style-type: none"> 1. The current assessment of the topical area results in a satisfactory rating.
<ol style="list-style-type: none"> 2. The previous assessment that resulted in a marginal rating identified different deficiencies and reasons for the rating.
<ol style="list-style-type: none"> 3. The deficiencies and reasons that were the basis of the previous marginal rating were related to the completion of a line item construction project or upgrade program. In that case, acceptable interim measures must have been implemented, physically validated pending completion of the project, and documented in the assessment report.
<ul style="list-style-type: none"> • Do survey and self-assessment reports include the following items:
<ol style="list-style-type: none"> 1. A completed DOE Form 470.8 or equivalent?
<ol style="list-style-type: none"> 2. An executive summary containing:

<ul style="list-style-type: none"> The scope, methodology, period of coverage, duration, and date of the exit briefing.
<ul style="list-style-type: none"> A brief overview of the facility, function, scope of operations, and contractual information (e.g., contract number, award and expiration dates, contract type, identification of security clauses, identification of the security, and overall scores assigned to the most recent contract appraisal).
<ul style="list-style-type: none"> A brief synopsis of major strengths and weaknesses that impact the effectiveness of the facility’s overall S&S program, including the identification of any topical areas rated less than satisfactory.
<ul style="list-style-type: none"> The overall composite rating with supporting rationale.
<ul style="list-style-type: none"> A reference to the list of findings identified during the self-assessment.
<p>3. An introduction containing:</p>
<ul style="list-style-type: none"> The scope, methodology, period of coverage, duration, and date of the exit briefing to management.
<ul style="list-style-type: none"> A description of the facility, its function and scope of operations, security interests, and contractual information (e.g., contract number, award and expiration dates, contract type, identification of security clauses, identification of the security, and overall scores assigned to the most recent contract appraisal).
<p>4. A narrative for each rated topical and sub-topical area that includes:</p>
<ul style="list-style-type: none"> A description of the site’s implementation of the program element.
<ul style="list-style-type: none"> The scope of the evaluation.
<ul style="list-style-type: none"> A description of activities conducted.
<ul style="list-style-type: none"> The evaluation results and associated issues (including other Departmental and Other Government Agency reviews or inspection results related to the topic/sub-topic that were included).
<ul style="list-style-type: none"> The identification of all findings, including new and previously identified open findings, regardless of source and their current corrective action status.
<ul style="list-style-type: none"> An analysis that provides a justification and rationale of the factors responsible for the rating.
<p>5. Attachments, including:</p>
<ul style="list-style-type: none"> A copy of the current DOE Form 470.2, <i>Facility Data and Approval Record</i>.
<ul style="list-style-type: none"> A listing of all active DOE Form 470.1, <i>Contract Security Classification Specification</i>, or DD Form 254, <i>Contract Security Classification Specification</i>.
<ul style="list-style-type: none"> A listing of all new findings from the survey or self-assessment.
<ul style="list-style-type: none"> A listing of all previously identified findings that remain open, including the current status of corrective actions.
<ul style="list-style-type: none"> A listing of team members, including names, employers, and their assigned area(s) of evaluation.
<ul style="list-style-type: none"> A listing of all source documents used to support the survey or self-assessment conduct and results (e.g., Government Accounting Office, Inspector General, and similar assessment documents).
<ul style="list-style-type: none"> Are surveys and self-assessment reports distributed to the applicable senior managers and other personnel responsible for corrective actions and other personnel, as deemed appropriate?

<ul style="list-style-type: none"> • Within 15 days of an overall marginal composite survey or self-assessment rating, is line management notification made and does the notification include: <ol style="list-style-type: none"> 1. A statement identifying the vulnerability and rationale for the rating. 2. A description of the corrective action/compensatory measures taken to date. 3. A statement acknowledging physical validation of the adequacy of items identified in the corrective action/compensatory measures.
<ul style="list-style-type: none"> • Within 24 hours of an overall composite unsatisfactory survey or self-assessment rating, the cognizant security authority must coordinate with the DOE cognizant security authority, who must in turn coordinate with the Departmental element to take the following actions: <ol style="list-style-type: none"> 1. Suspend the activity and/or recommend suspension of the facility clearance pending remedial action. 2. Provide justification for continuing operations to the DOE cognizant security authority. In addition to providing the rationale, the cognizant security authority must evaluate those immediate interim corrective actions being taken to mitigate indentified risks or vulnerabilities.
<ul style="list-style-type: none"> • Are records and documentation of the conduct of surveys and self-assessments retained in accordance with local procedures and appropriate records inventory disposition schedules?
<ul style="list-style-type: none"> • Are any process improvements resulting from the annual evaluation of the survey or self-assessment processes incorporated into the Federal survey or contractor self-assessment processes?
<p>Lines of Inquiry Concerning Resolution of Findings</p>
<ul style="list-style-type: none"> • Are corrective action plans developed for all open survey and self-assessment findings?
<ul style="list-style-type: none"> • Are corrective action plans for surveys and self-assessments submitted within 30 working days of the date of the exit briefing?
<ul style="list-style-type: none"> • Are quarterly reports of the status of corrective actions for each finding provided to the appropriate cognizant security authority?
<ul style="list-style-type: none"> • Are all survey and self-assessment corrective actions: <ol style="list-style-type: none"> 1. Based on documented root cause analyses, risk assessments, and cost benefit analyses to ensure that the survey/self-assessment program objectives are met? 2. Reported, entered, tracked, and updated until completed, validated, and closed in the Safeguards and Security Information Management System (SSIMS) or a local corrective action tracking system, as appropriate?
<ul style="list-style-type: none"> • Is documentation associated with the conduct of surveys and self-assessments retained in accordance with local procedures and appropriate inventory disposition schedules?
<ul style="list-style-type: none"> • Is trending used in the resolution of findings to determine if systemic and systematic causal factors exist within the S&S program?
<ul style="list-style-type: none"> • Are negative trends analyzed to ensure corrective actions address root causes and the need for continuous improvement?

Lines of Inquiry Concerning Performance Evaluation Plans
<ul style="list-style-type: none">• Do contractor performance evaluation plans include appropriate weight to S&S programs?
<ul style="list-style-type: none">• Do contractor performance evaluation plans address all applicable security topic areas?
<ul style="list-style-type: none">• Do contractor performance evaluation plans adequately define:
<ul style="list-style-type: none"><ul style="list-style-type: none">• Minimum S&S program requirements?
<ul style="list-style-type: none"><ul style="list-style-type: none">• Expected S&S program requirements?
<ul style="list-style-type: none"><ul style="list-style-type: none">• S&S program goals?
<ul style="list-style-type: none">• Do contractor performance evaluation plans adequately define the costs and rewards related to S&S performance requirements, expectations, and goals?

Tool 3-2

**SURVEY AND SELF-ASSESSMENT REPORTS REVIEW
Federal and Contractor Oversight**

One of the first things an inspector can do in regards to surveys or self-assessments is to review existing reports. The inspector should assess the reports' content to identify whether all appropriate topical and sub-topical areas were assessed and whether the information in the report reflects an adequate, thorough review of those topics and sub-topics. In short, the report should be reviewed to determine whether it represents a "stand-alone" assessment of the status of the safeguards and security programs at the site and whether the analysis that resulted in the report was based on an appropriately in-depth review of the programs. The worksheet on the following page can be used to capture the methodology used by the site to arrive at the report conclusions. This worksheet will assist the inspector in identifying potential areas for further review.

The following definitions apply to the use of this worksheet:

DR: The report reflects that within a topic or sub-topic area various documents were reviewed to identify if they were current and accurate.

Obs: The report reflects that activities within a topic or sub-topic were observed as part of the assessment.

Int: The report reflects the results of interviews with various line managers and operators responsible for actions within the topic or sub-topic area.

Test: The report reflects the results of various test or product reviews.

Within the above categories, the report may imply something was done or may include specifics or examples of what was done. The variation can be indicated by the use of an "S" or an "I".

"S" means that the report included specifics or examples of how the "DR," "Obs," "Int," and/or "Test" were accomplished.

"I" means that the report implied that "DR," "Obs," "Int," and/or "Test" were accomplished but gave no specific examples.

If a topic or sub-topic was not assessed, it should be assigned an "X" rating to reflect that the report contained no information to support that it was assessed or that the report specified that the topic or sub-topic was not assessed. If a topic or sub-topic was not assessed, the "X" can be placed in the "DR" column and there will be no "S" or "I" entries related to that topic or sub-topic.

This worksheet can also be used to identify whether the report identifies the overall assessment results of "Satisfactory," "Needs Improvement," or "Unsatisfactory," and the number of "Findings," "Observations," "Suggestions/Opportunities for Improvement," or "Noteworthy Practices" identified within the report.

When completed, the worksheet can provide an inspector with a quick reference to support how complete and thorough the contents of a report may be. It will also provide a departure point for further analysis of the overall survey or self-assessment program.

Site/Facility: _____

Date of Assessment: _____

	DR	Obs	Int	Test		DR	Obs	Int	Test
PMS Prot Pro Mgmt					C Cyb Ldr, Resp, A				
PMS Prog M&A					C Cyb C&A, Risk,Plg				
PMS Res & Budget					C Cyb Pol, Guid, Proc				
PMS Per Dev Trng					C Cyb Tech Imp				
PMS S&S Planning					C Cyb Perf, Fdbk, CI				
PMS Surv & SA					Telecom Sec				
PMS PAP					U Cyb Ldr, Resp, A				
PMS Res Findings					U Cyb C&A, Risk,Plg				
PMS Inc Rptg					U Cyb Pol, Guid, Proc				
PMS Prg Wd Spt					U Cyb Tech Imp				
PMS Fac App & Reg					U Cyb Perf, Fdbk, CI				
PMS FOCI									
PMS Sec Mgmt Con					PS Acc Auth				
					PS HRP				
PF Mgmt					PS Class Visits				
PF Training					PS S&S Aware				
PF Duties									
PF Fac & Equip					UVA Spnsr Prg Mgmt				
					UVA CI Rqts				
PS Acc Controls					UVA Exp Cont/ Tech				
PS IDS					UVA Sec Rqts				
PS Bar & Delays					UVA Apps & Rpts				
PS Test & Maint									
PS Com					MCA Prog Admin				
					MCA Mat Account				
IP Basic Rqt					MCA Mat Control				
IP TSCM									
IP OPSEC									
IP Class Guide									
IP CMPC Cont Class									
IP Cont Class									
IP SAP									

DR = Doc, Plan, Proc, Record Review

Obs = Observation of work or product

Int = Interview

Test = Performance and/or Knowledge Test

S= Stated

I= Implied

X= Not Assessed

Summary Results: Satisfactory

Needs Improvement

Unsatisfactory

Findings

Observations

Suggestions/Opportunities for Improvement

Noteworthy Practices

Tool 3-3

Topical Team Survey and Self-Assessment Evaluation
Federal and Contractor Oversight

TOPIC: _____

SITE: _____

The purpose of this questionnaire is to assist individual topic teams (non-PPM) in their evaluation of the surveys and self-assessments conducted for their topic. This data will also assist the PPM team in identifying the overall effectiveness of the self-assessment process and potential trends in oversight. These questions are derived from the requirements in DOE Manual 470.4-1, Change 1, Section G. PPM normally evaluates the oversight assessments conducted since the last inspection (up to three years worth).

1. Self-Assessments:

a. Do self-assessments address compliance and performance and all the key/essential elements for the topic area as identified on DOE Form 470.8?

- Current Year (ENTER YEAR) _____ Yes _____ No _____
- Last Year (ENTER YEAR) _____ Yes _____ No _____
- Prior Year (ENTER YEAR) _____ Yes _____ No _____

Comments:

b. Are self-assessments performance based with well-developed pass/fail criteria when possible, or are reports characterized by document reviews and program descriptions?

- Current Year (ENTER YEAR) _____ Yes _____ No _____
- Last Year (ENTER YEAR) _____ Yes _____ No _____
- Prior Year (ENTER YEAR) _____ Yes _____ No _____

Comments:

c. Were meaningful findings issued as a result of self-assessments, or do report narratives consistently describe compliance or performance failures without issuing a finding?

- Current Year (ENTER YEAR) _____ Yes _____ No _____
- Last Year (ENTER YEAR) _____ Yes _____ No _____
- Prior Year (ENTER YEAR) _____ Yes _____ No _____

Comments:

2. Surveys:

a. Do surveys address compliance and performance and all the key/essential elements for the topic area as identified on DOE Form 470.8?

- Current Year (ENTER YEAR) _____ Yes _____ No _____
- Last Year (ENTER YEAR) _____ Yes _____ No _____
- Prior Year (ENTER YEAR) _____ Yes _____ No _____

Comments:

b. Are surveys performance based with well-developed pass/fail criteria when possible, or are reports characterized by document reviews and program descriptions?

- Current Year (**ENTER YEAR**) _____ Yes _____ No _____
- Last Year (**ENTER YEAR**) _____ Yes _____ No _____
- Prior Year (**ENTER YEAR**) _____ Yes _____ No _____

Comments:

c. Were meaningful findings issued as a result of surveys, or do report narratives consistently describe compliance or performance failures without issuing a finding?

- Current Year (**ENTER YEAR**) _____ Yes _____ No _____
- Last Year (**ENTER YEAR**) _____ Yes _____ No _____
- Prior Year (**ENTER YEAR**) _____ Yes _____ No _____

Comments:

d. Were findings against the Federal site office from the last Independent Oversight inspection adequately addressed, and do site office corrective action plans for external and self-assessment findings include root cause analyses and address issues in a manner that precludes recurrence?

- Current Year (**ENTER YEAR**) _____ Yes _____ No _____
- Last Year (**ENTER YEAR**) _____ Yes _____ No _____
- Prior Year (**ENTER YEAR**) _____ Yes _____ No _____

Comments:

3. Corrective Actions:

a. Were findings assessed to the contractor(s) from the last Independent Oversight inspection adequately addressed? If not, please describe the deficiency.

b. Were findings assessed to the site office from the last Independent Oversight inspection adequately addressed? If not, please describe deficiency.

c. Do contractor corrective action plans for survey and self-assessment findings include root cause analyses and address issues in a manner that precludes recurrence?

- Current Year (**ENTER YEAR**) _____ Yes _____ No _____
- Last Year (**ENTER YEAR**) _____ Yes _____ No _____
- Prior Year (**ENTER YEAR**) _____ Yes _____ No _____

Comments:

d. Do Federal corrective action plans include root cause analyses and address issues in a manner that precludes recurrence?

4. Compliance/Performance Issues.

Has this inspection identified compliance or performance issues that recent survey/self-assessment activities rated satisfactory or failed to identify?

Issue: _____

Issue: _____

Issue: _____

Tool 3-4

**Topical Team Performance Assurance Program Evaluation
Federal and Contractor Oversight**

The purpose of this questionnaire is to assist individual topic teams (non-PPM) in their evaluation of the performance assurance requirements for their topic. This data will also assist the PPM team in identifying the overall effectiveness of the performance assurance program and potential trends among topics. These questions are derived from the requirements in DOE Manual 470.4-1, Change 1, Section F. PPM normally assesses the performance assurance activities conducted since the last inspection (up to three years worth).

1. Has the site identified essential elements for this topic, including those for Category I facilities, MC&A, and Top Secret? If so, please list them or provide a document reference.

2. What activities have been accomplished to assure the operability and effectiveness of this topic's essential elements?

- Current Year (**ENTER YEAR**)

- Last Year (**ENTER YEAR**)

- Prior Year (**ENTER YEAR**)

Comments:

3. Do performance tests of topical essential elements use objective, measurable pass/fail criteria?

Comments:

4. What happens if there is a test failure?

5. For new technologies, weapons, assessment tools, or processes that have been implemented or are being field tested/demonstrated by the site, what was the acceptance testing process used to permit the new program element to be placed in service (regardless of whether any credit is taken for effectiveness, detection, assessment, interdiction, or neutralization)? Please describe and provide a document or staff reference.

Tool 3-5

OVERALL PERFORMANCE EVALUATION FOR OVERSIGHT
Federal and Contractor Oversight

Person Interviewed: _____

Interviewer: _____

Organization: _____

Date: _____

<p>SPECIFIC QUESTIONS <i>(Performance Criteria)</i></p>	<p>NOTES</p>
<ul style="list-style-type: none"> • Are survey, inspection, and self-assessment programs in place to determine the effectiveness of the S&S program on a recurring basis? <ul style="list-style-type: none"> – <i>Documented and promulgated?</i> – <i>Responsibility and accountability clear?</i> – <i>Personnel understand responsibilities?</i> – <i>Programs comply with DOE orders?</i> – <i>Provide adequate feedback?</i> – <i>Organization and staffing adequate?</i> 	
<ul style="list-style-type: none"> • 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? <ul style="list-style-type: none"> – <i>Is there a tracking system?</i> – <i>Properly implemented and effective?</i> – <i>Provides timely and useful information?</i> – <i>System properly documented?</i> – <i>Contains all necessary information?</i> – <i>Accountability is assigned?</i> – <i>Integrated to prevent redundant reporting?</i> 	

SPECIFIC QUESTIONS <i>(Performance Criteria)</i>	NOTES
<ul style="list-style-type: none">• Are reports developed by the control systems provided to the appropriate organizational level to ensure proper management attention?<ul style="list-style-type: none">– <i>Positive identification of S&S issues?</i>– <i>Thorough internal distribution of reports?</i>– <i>Priorities assigned by system?</i>– <i>Format clear, concise, and effective?</i>– <i>Reports distributed to permit use in correcting common problems?</i>– <i>Reports reviewed by top management when appropriate?</i>	

This page intentionally left blank.

ADDITIONAL FORMS AND INSTRUCTIONS

Data Collection Form.....	A-85
Instructions for Completing an Issue Form.....	A-86
Report Preparation	A-87
Oversight, Deviations, and Performance Assurance Assessment Worksheets	A-89
Deviations Assessment	A-90
Classified Cyber Facilities Survey/Self-Assessment Review	A-91
Unclassified Cyber Facilities Survey/Self-Assessment Review	A-92
IM/CMPC Facilities Survey/Self-Assessment Review.....	A-93
NMC&A Facilities Survey/Self-Assessment Review.....	A-94
PERSEC Facilities Survey/Self-Assessment Review	A-95
Pro Force Facilities Survey/Self-Assessment Review	A-96
Physical Security Systems Facilities Survey/Self-Assessment Review.....	A-97
PPM Facilities Self-Assessment Reviews.....	A-98
PPM Facilities Survey Review	A-99
PPM Feedback Survey.....	A-100
PPM Summary Validation Worksheet	A-102

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 (i.e., 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.

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) Inspection Representative:	_____ Date: _____

REPORT PREPARATION

The integration of protection program management (PPM) sub-topics 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 PPM 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 sub-topic 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 (Safeguards and Security Management Plan, Site Security Plan(s), VA, Deviations, and GSP Implementation Plan)
 - Feedback Mechanisms (Survey Program, Self-assessment Program, Performance Assurance Program, and Resolution of Findings).

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, sub-topic sections, conclusion, rating, and opportunities for improvement), text for the introduction, and text for the PPM sub-topic section.
- When possible, the initial draft is shared (via fax or email) with the other topic team members in advance of the data collection phase with sufficient time to allow for a revision of the draft outline prior to the beginning of the data collection phase.

Onsite Data Collection Phase

- Daily: The 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 sub-topic section) of the draft report.
- Thursday: The remaining topic team member(s) continue data collection.

Onsite Close-out Phase

- Daily: The 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 sub-topic section) of the draft report.
- Thursday: All other sub-topic inputs are due to the principal writer by close of business.
- Saturday: The draft report is finalized, and team members review for content and one team member proofreads.
- Monday: Final proof reading and correction is completed 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.

OVERSIGHT, DEVIATIONS, AND PERFORMANCE ASSURANCE ASSESSMENT WORKSHEETS

The purpose of this assessment tool is to assist individual topic teams in organizing the evaluation and identification of the oversight, deviations, and performance assurance requirements for their topic. The attached worksheets are for your *optional use by exception* to methodically identify potential strengths and weaknesses associated with protection program management requirements that impact your safeguards and security program area. On the oversight worksheet, individual facilities and sub-topic areas within each topic are identified as referenced on DOE Form 470-8. Not all will apply to your inspection process for every site/facility. The questions are derived from the requirements in DOE Manual 470.4-1; Change 1; Sections G, F, and M.

This data will also assist the PPM topic in identifying the overall effectiveness of the safeguards and security program, potential trends among topics, and potentially significant strengths or weaknesses that should be considered for inclusion in the PPM section of the report. Your assistance and suggestions are welcomed to improve these worksheets.

Deviations Assessment

Deviation Number	In SSSP	Implemented Prior to Approval	Approval Level	Characterized appropriately	Accurate Description of Risk	VA Results Included	Adequate Compensatory Measures	Compensatory Measures Monitored
	Yes No	Yes No	Yes No	Yes No	Yes No	Yes No	Yes No	Yes No
	Discussion:							
	Yes No	Yes No	Yes No	Yes No	Yes No	Yes No	Yes No	Yes No
	Discussion:							
	Yes No	Yes No	Yes No	Yes No	Yes No	Yes No	Yes No	Yes No
	Discussion:							
	Yes No	Yes No	Yes No	Yes No	Yes No	Yes No	Yes No	Yes No
	Discussion:							

PPM Feedback Survey

Please evaluate the following topics using the scale 1 = Strongly Disagree – 5 = Strongly Agree.

Process	
Topics provided adequate feedback and validation.	1 2 3 4 5
Inspectors listened to better understand our program.	1 2 3 4 5
The inspection provided value to our program.	1 2 3 4 5
Results reflected compliance and performance.	1 2 3 4 5
Results were based on requirements.	1 2 3 4 5
Results were based on differences in opinion.	1 2 3 4 5
Differences in policy interpretation led to problems.	1 2 3 4 5
Conclusions were fully supported.	1 2 3 4 5
Validations kept management informed.	1 2 3 4 5
The inspection process was carried out as a partnership.	1 2 3 4 5
Inspectors were professional at all times.	1 2 3 4 5
Inspectors strived to be accurate instead of “right.”	1 2 3 4 5
Report	
Factual accuracy comments were considered in the report.	1 2 3 4 5
There were no surprises in the report.	1 2 3 4 5
The report was balanced.	1 2 3 4 5

1. What items in the data call required additional communication to understand what information was being requested?
2. If any, what were the issues that could have been better described and how?
3. If any, what were the issues identified without clarifying their importance in terms of whether they were compliance issues, performance issues, or both?
4. If any, what inspection results and findings reflected differing interpretations of policy?
5. The inspection process would be improved by the addition of, deletion of, or a change to:
6. In relation to the cost and benefits of the feedback the site received, the inspection scope and team size was:
7. Did the inspection process and report appropriately address site efforts to effectively manage risk where the site believed risk was unavoidable?

PPM Summary Validation Worksheet (U)

(U) Topic:

(X) Recommended Rating:

- Effective Performance
- Needs Improvement
- Significant Weakness

Program Strengths: (U)

(X) 1.

Program Weaknesses: (U)

Findings (U)

(X) 1. Finding # and Text

- (U) a. Site Response: Accepts Rejects
- (X) b. Significant Comments:
- (X) c. Expectations: No further comments Ten day comment

Additional Weaknesses and Opportunities for Improvement (OFI) (U)

(X) 1. Weakness or OFI text:

- (U) a. Site Response: Accepts Rejects
- (X) b. Significant Comments:
- (X) c. Expectations: No further comments Ten day comment

Status of Previously Identified Findings: (U)

(X) 1. Previous Finding # and Text

- (X) a. Current Status: Corrected Not Corrected
- (U) b. Site Response: Accepts Rejects
- (X) c. Significant Comments:
- (X) d. Expectations: No further comments Ten day comment

Conclusion: (U)

- (U) 1. Site Response: Accepts Rejects
- (X) 2. Significant Comments:
- (X) 3. Expectations: No further comments Ten day comment