NOT MEASUREMENT SENSITIVE

DOE-STD-1217-2016
February 2016

DOE STANDARD

SAFEGUARDS AND SECURITY SURVEY AND SELF-ASSESSMENT PLANNING, CONDUCT, AND REPORTING

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

AREA SANS

This Page Intentionally Left Blank

TABLE OF CONTENTS

APPENDIX A: SURVEY AND SELF-ASSESSMENT TOOLKIT

FOREWORD

This Department of Energy Technical Standard is for use by all Departmental elements. Beneficial comments (recommendations, additions, and deletions) and any pertinent data that may improve this document should be emailed to mary.gallion@hq.doe.gov or mailed to:

U.S. Department of Energy
Office of Health, Safety, and Security
Office of Security Policy, GTN/AU-51
1000 Independence Ave., SW
Washington, D.C. 20585-1290

Department of Energy Technical Standards do not establish requirements. However, all or part of the provisions in this Technical Standard can become requirements under the following circumstances:

- They are explicitly stated to be requirements in a Department of Energy requirements document (e.g., a purchase requisition).
- The organization makes a commitment to meet a standard in a contract, implementation plan, or program plan.
- This Technical Standard is incorporated into a contract.

Throughout this standard, the word "shall" is used to denote an action that is to be performed if the objectives of this standard are to be met, and the word "should" is used to denote an action that is expected to be performed unless a technically equivalent action is substituted. Goals or intended functionality are indicated by "shall," or "should." However, it is not appropriate to consider that "should" statements would automatically be converted to "shall" statements, as this action would violate the consensus process used to approve this standard.

This Technical Standard was prepared following requirements for due process, consensus, and approval as required by the U.S. Department of Energy Standards Program. Consensus is established when substantial agreement has been reached by all members of the writing team and the Technical Standard has been approved through the Department of Energy directives approval process (REVCOM). Substantial agreement means much more than a simple majority, but not necessarily unanimity. Consensus requires that all views and objections be considered, and that a concerted effort be made toward their resolution.

SAFEGUARDS AND SECURITY SURVEY AND SELF-ASSESSMENT PLANNING, CONDUCT, AND REPORTING

1. SCOPE. This document provides the Department of Energy (DOE) with a standard methodology for adapting the Department's requirements for Safeguards and Security (S&S) surveys and self-assessments to organization-specific needs in a coherent, consistent, and repeatable fashion. It describes a consistent and acceptable approach to planning, conducting, and reporting the results for S&S surveys and self-assessments.

2. PURPOSE. The purpose of this Technical Standard is to provide Federal and contractor personnel who have S&S oversight responsibilities with an accepted, compliance and performance based process to conduct the S&S surveys and self-assessments prescribed in DOE O 470.4B.

3. APPLICABILITY. This Technical Standard is intended for use by Federal and contractor S&S organizations conducting either S&S surveys or S&S self-assessments.

4. REFERENCES.
   a. DOE Policy 470.1A, Safeguards and Security Program, December 29, 2010.

   b. DOE Order 470.3B, Graded Security Protection (GSP) Policy, August 12, 2008.

   c. DOE Order 470.4B Administrative Change 1, Safeguards and Security Program, July 21, 2011.

   d. DOE Guide 414.1-1C, Management and Independent Assessments Guide, March 27, 2014.

   e. DOE Order 226.1B, Implementation of Department of Energy Oversight Policy, April 25, 2011.

   f. DOE Order 413.3B, Program and Project Management for the Acquisition of Capital Assets, November 29, 2010.

   g. DOE Order 142.3A, Unclassified Foreign Visits and Assignments Program, October 14, 2010.

   h. DOE Order 452.8, Control of Nuclear Weapon Data, July 21, 2011.

   i. DOE Order 470.6, Technical Security Program, September 2, 2015.

   j. DOE Order 471.3, Administrative Change 1, Identifying and Protecting Official Use Only Information, April 9, 2003.

   k. DOE Manual 471.3-1, Administrative Change 1, Identifying and Protecting Official Use Only Information, April 9. 2003.

l. DOE Order 471.5, Special Access Programs, March 9, 2011.

m. DOE Order 471.6, Administrative Change 2, Information Security, Ju 29, 2011.

n. DOE Order 472.2, Change 2, Personnel Security, July 21, 2011.

o. DOE Order 473.3, Protection Program Operations, June 29, 2011.

p. DOE Order 475.1, Counterintelligence Program, December 10, 2004.

q. DOE Order 475.2B, Identifying Classified Information , October 3, 2014.

r. DOE Order 580.1A, Administrative Change 1, DOE Personal Property Management Program, March 30, 2012.

s. Title 32 Code of Federal Regulations, Part 2001—Classified National Security Information.

t. Title 32 Code of Federal Regulations Part 2004 – National Industrial Security Program Directive Number 1.

u. Title 10, Code of Federal Regulations Part 824, Procedural Rules for the Assessment of Civil Penalties for Classified Information Security Violations.

Some external sources of useful reference materials include:

http://energy.gov/cio/downloads/doe-f-4708 (Current version of Survey Form)
http://www.efcog.org/guides/ (EFCOG Self-assessment Tool Kit)

5. ACRONYMS AND DEFINITIONS. Definitions and acronyms commonly used in the Safeguards and Security Program can be found in the Environment, Health, Safety and Security Policy Information Resource located at https://pir.doe.gov/. Definitions that have unique meanings in this Technical Standard include:

   a. Observation. An item for management attention noted in a survey or self-assessment report that identifies a potential deficiency if not addressed or a possibility for program enhancement that should be further studied before implementation.

   b. Opportunity for Improvement. A term used by some oversight activities to identify an item for management attention noted in a survey or self-assessment that identifies a possibility for program enhancement that should be further studied before implementation.

   c. Suggestion. A term used by some oversight activities to identify an item for management attention noted in a survey or self-assessment that identifies a possibility for program enhancement that should be further studied before implementation.

6. DUTIES, RESPONSIBILITIES, AND TRAINING

a. Survey Team Leader

For a survey of a facility with an importance rating of "A" or "B," the survey team lead shall be a Federal employee appointed by line management of the DOE cognizant security office. For other facilities, the survey team lead may be a contractor acting under the supervision of a Federal employee designated by line management of the DOE cognizant security office. The survey team lead is responsible for the successful completion of the survey. This person must have a comprehensive understanding of safeguards and security (S&S) programs, have previous survey experience (preferably as a topic lead or survey team lead), and be especially capable of integrating topical area results into a comprehensive assessment of facility security. It is highly desirable that the survey team lead has completed training courses offered by the National Training Center on survey conduct and management.

The survey team lead is responsible for managing the efforts of the survey team and for keeping the participants informed of all matters affecting the team and/or the facility during the survey. The survey team lead is responsible for team planning and logistics, coordination of team activities, focusing the activities of the team, ensuring that deliverables are prepared and provided according to the schedule, promoting integration among topic teams, and acting as a team spokesperson during meetings and briefings. In particular, the team lead needs to ensure that all pertinent elements of the S&S program are reviewed, that analysis is particularly focused upon the most critical elements, and that any concerns or deficiencies identified are fully supported by documented and validated data.

b. Survey Topical Lead

A topical lead for each topic to be surveyed should either be appointed by the same authority appointing the survey team lead or, alternately, be designated by the survey team lead. For surveys of facilities with an importance rating of "A" or "B", the topical lead should be a Federal employee. The topical lead shall be an expert in his or her assigned topic. In some cases, it may be necessary to select a contractor as topic lead because of his or her outstanding technical qualifications, with the understanding that a contractor cannot supervise the work of Federal employees. The topical leads work closely with the survey team lead to complete pre-planning, to ensure that each topic team collects the data required for preparation of the survey report, and to ensure that written and verbal deliverables assigned to the topical teams are of high quality and are delivered according to the schedule. Each topical lead conducts, with the assistance of the topical team, a topical analysis of results, and recommends topical and sub-topical ratings to the survey team leader. It is highly desirable that topical leads have completed the training courses offered by the NTC on survey conduct and management.

c. Survey Team Members

Selection of survey team members should be coordinated among the survey team leader, topical leads, and the organizations for which the individuals work. Team members should be selected for technical competence, professionalism, and maturity, with particular emphasis on interpersonal skills that will allow them to interact with facility personnel to collect and analyze data without creating an unnecessary burden on operations or controversy with facility personnel. Team members should have previous experience and demonstrated expertise in the topical or sub-topical area to which they are assigned, unless they are specifically selected for the purpose of training and/or furthering their professional development. Team members selected for training or professional development should perform under the direct supervision of an individual with previous experience and demonstrated expertise in the topical or sub-topical area. Unless they are specifically selected for training or professional development, it is highly desirable that survey team members have completed training courses offered by the National Training Center on survey conduct and management.

d. Self-assessment Team Leads and Members

Self-assessment team leaders, topical leads, and team members should be chosen using the same criteria as listed above for survey team leaders, topical leads, and team members. However, as self-assessments are a contractor activity, it is not necessary to have Federal employees as survey and topical team leaders.

7. SURVEY AND SELF-ASSESSMENT OVERVIEW

Without an adequate S&S survey program, line managers cannot effectively manage the S&S programs for which they are responsible. Surveys compare planned S&S program performance to the actual achievement. The survey report presents accumulated data and provides an analysis of S&S program effectiveness for the areas surveyed/assessed at the surveyed location. The survey activity provides two vital components to the Federal management of an S&S program – measurement of the degree to which actual implementation matches planned implementation, and feedback indicating actions needed to make program implementation match program planning and/or needed changes to program planning and implementation to better achieve mission objectives. Management support and commitment to the S&S survey program are critical to ensuring the time and resources required to produce a useful survey product are available.

To provide the best possible information for management consideration, the S&S survey needs to include a significant sample of the elements of the local S&S mission and the resulting report needs to contain a logical and thorough presentation of the survey results, accompanied by a complete and logical analysis of those results that leads to conclusions regarding the status of program implementation, reflected in the ratings awarded, and identification of needed actions. These conclusions regarding the status, accompanied by measurements and analysis supporting the conclusions, inform not only local Federal management, but also line management at higher levels about the current status of the S&S program at the surveyed site or facility.

S&S programs have traditionally been considered to be logically divided into topical areas and, within each topical area, sub-elements known as sub-topics. While this organizational structure might be considered to be somewhat arbitrary, it forms a useful way to organize data collection and to report the results of a survey or self-assessment. This division into topics and sub-topics is reflected in the DOE Form 470.8, *Survey/Inspection Report Form* (see Appendix A, Section 5.5), and this topical and sub-topical structure will be used in discussion of the survey and self-assessment process to follow. In addition to providing a structural reference for this technical standard, the form is often used to provide a means of summarizing the results of a comprehensive survey or self-assessment and is the appropriate data entry form for entering survey and self-assessment data into the Safeguards and Security Information Management System (SSIMS).

Self-assessments provide the same management information to local contractor managers on a more frequent basis than the survey or at a time between surveys. The need for documentation of self-assessment activities leading to a periodic comprehensive report is no less than for surveys. The benefits of these self-assessments are several:

- Local managers receive notification of program weaknesses on a more timely basis, thereby allowing them to address and correct the issues sooner than might be possible using only an external review;

- Local S&S personnel are encouraged to be self-critical, allowing them to be more proactive in providing adequate security to local assets; and,

- Employees who have security duties but are not security professionals are provided a more comprehensive view of the security program.

8. SURVEY AND SELF-ASSESSMENT PLANNING

Survey and self-assessment planning consists of two components – cyclic program planning and planning for a survey of a particular facility or a particular self-assessment. Effective planning requires the planner to fully understand the assets at each facility to be reviewed during a planning period, the operations and characteristics of each facility, the safeguards and security directives that apply at each facility, and the past performance of each facility on previous surveys, facility self-assessments, and recent external reviews.

a. Cyclic Planning for Surveys and Self-Assessments

Comprehensive planning is key to the success of a survey or self-assessment program. Review activities may be scheduled around a one-time evaluation, ongoing observations during the reporting interval, or a combination of the two. Each activity conducting surveys or self-assessments should establish a planning cycle that best allows the allocation of resources and assures that surveys or self-assessments are scheduled to meet the requirements of DOE O 470.4B. A survey or self-assessment plan shall be prepared for the selected planning cycle to reflect the approach used for data collection and report preparation, a schedule of planned surveys or self-assessments during the planning period, and an initial assessment of personnel and other resources required to complete the planned activities. Personnel requirements, both the number of personnel and their skills, will be a function of the particular facilities scheduled for that planning period. Planning shall include an identification of the information needed to conduct a comprehensive evaluation at each facility, including the identification of topics and sub-topics required. If information is to be collected over an extended period, for example by observing particular operations during the time period, the plan will need to consider whether the information collected remains completely reliable or is somewhat degraded by the passage of time between the observation and final report preparation. Planning should identify sampling or verification methods that ensure perishable information gathered early in a survey or self-assessment planning period remains valid at the time the report is completed.

b. Planning a Facility Survey or Self-Assessment.

Survey and comprehensive self-assessment planning involves gathering and analyzing large amounts of information from many sources, making decisions based on the analysis, and preparing survey activities based on the decisions. Because there is only a limited amount of time available onsite to collect the data necessary to characterize the status of the programs being surveyed, planning should focus on determining what program elements to review and how best to survey those elements to help ensure the most effective use of that time. In particular, the plan shall identify program elements that will be fully or partially evaluated based upon sampling activities during a survey cycle (such as the results of surveillances or shadowing). For those elements the plan shall specify the additional data necessary to assess the applicability and accuracy of data obtained from periodic sampling during the final

phase of survey conduct. Planning activities also include identifying personnel and other support requirements for all phases of the survey.

(1) Pre-planning.

Pre-planning includes determining the scope and objectives of the review. Information such as the facility importance rating, S&S interests, and security contract requirements provide the basis for the scope and objectives of the assessment, but other factors such as previous performance, recent site operational changes, and new missions are also important in establishing the scope of the review. The team leader develops an initial schedule and considers whether a preliminary visit is needed. Throughout the planning process, the team leader is responsible for obtaining any necessary management approvals of decisions and actions.

(2) Preliminary Coordination.

Before data collection begins, the team leader's responsibilities should include:

- Coordinating the proposed schedule with the facility and other responsible parties;
- Identifying basic information needed in the data collection, such as a site or facility security plan, assessment/ inspection reports, approved deviations (including equivalencies/exemptions for DOE policy and deviations from national policy), and contract data;
- Sending the notification letter or other agreed upon notification;
- Team member selection and coordination with members' management;
- If a data call is deemed necessary to support a team planning meeting, determining the documents needed, preparing a list, and requesting the listed documents from their respective sources.
- Conducting a team planning meeting;
- Establishing a schedule and topic assignments;
- Gathering facility data (e.g., location, S&S interests, queries of SSIMS, EFOCI, and other data bases to obtain information regarding the facility clearance, importance rating, key positions, assets, current S&S plans, and active deviations);
- Establishing protocols, including a schedule for team meetings, a procedure for communicating schedule changes or additional support requirements, a process for managing classification concerns and issues, a determination of the validation

process to be used, a consolidated document call, a report outline reflecting the desired format for the report, and a compilation of logistical information (travel dates, hotel arrangements, rental cars, site access, in-briefing time/location);

- Providing the format for plans, reports, findings, process improvements, and corrective actions;

- Providing official notification; and,

- Preparing an overall plan for the survey or self-assessment.

The level of pre-planning required for a survey or self-assessment that includes ongoing data collection such as surveillances or shadowing of key activities will be even more stringent, since specific measures for validation of such data will need to be identified, and methods for inclusion of these data sets into the analysis leading to topical area ratings and facility ratings will need to be specified.

9. SURVEY AND SELF-ASSESSMENT CONDUCT

Valid sampling and accurate evaluation should be the focus of all survey and self-assessment activities during the conduct of the review. This focus should be apparent during all phases of the review activity so that, as far as possible, the review is a joint exercise between reviewer and reviewed to identify and correct program issues, with the goal of improving the local S&S program. Methodologies typically used to measure performance include, but are not limited to, document review, testing, observation, interviews, data collection, and data analysis and validation.

a. In-Briefing.

A formal in-briefing has traditionally been the initial on-site activity of the type of review that one might call a "snapshot in time," during which all data is collected in a relatively brief interval – one day to a few weeks depending on the complexity of the site. More recently, comprehensive survey and self-assessment reports have often been based, partially or completely, upon data collected over an extended period, perhaps as long as a year. Even in the case of the more extended data collection effort, an in-briefing at the beginning of the review period should be conducted to assist in establishing and maintaining effective communication with the site. A carefully prepared in-briefing can ensure a positive start for the assessment, create a good first impression, and provide an opportunity to reduce the stress and tension associated with the survey or self-assessment. Items to be covered during the facility in-briefing should include (but are not limited to):

- Survey or self-assessment scope and objectives;

- Survey or self-assessment approach and methodology (with respect to data-collection methods), including whether all data will be collected during one site

visit, whether the final report will be based on a set of observations conducted throughout the assessment cycle, or some combination of these approaches;

- For surveys, the level of reliance on the contractor assurance system and how data derived from the contractor assurance system will be verified by the survey team and included in the analysis of survey data;
- General introductions of team members; and,
- Schedule of survey or self-assessment activities.

b. Maintaining Communication

The team leader and topical leads should plan on meeting frequently during the course of the survey or self-assessment. The frequency of the meetings will be partially dictated by the assessment approach – snapshot or extended – but are vital to ensure that the team leader and topical leads understand the status of data collection toward meeting the selected lines of inquiry, understand information that is of interest in their respective topics that has been identified by other teams, and maintain an awareness of emerging areas of concern.

The team also should emphasize communication with the assessed site. Again, the frequency of planned communications with site points of contact and site management will depend on the pace of data collection. However, it is vital to effective communication with the site, and therefore to the success of the assessment, that the points of contact and site management remain informed concerning the progress of data collection and have early notice of potential issues, particularly as they relate to rolling or shadow assessments if these techniques are a portion of the survey or self-assessment procedure.

c. Data Collection

All members of the survey or self-assessment team work to collect data. Members of one topical area often collect data that supports other topical areas and should share such data with other interested topical area teams. For example, data collected about physical security systems could also be useful to the analysis of protective force and nuclear material control, as they are each elements of the overall protection design. Data collection efforts as well as analysis efforts must always remain focused on the effectiveness of the entire S&S program in providing appropriate security for national security assets.

The selected lines of inquiry always guide data collection. Within a line of inquiry, data collection can be prioritized to allow schedule adjustments if complications or unforeseen events do not permit completion of all planned activities. If this occurs, the team can concentrate on gathering the data deemed most critical. High-priority data-collection activities should be scheduled early in the process to ensure that they

are accomplished. When a full line of inquiry is endangered by data collection issues, the team leader will decide the best course of action.

All working papers and data-collection records, notes, checklists, and other documentation accumulated during data collection should be retained as backup documentation to the final report. Ensure that all items are either reviewed by an Authorized Derivative Classifier and appropriately marked and protected, or are protected and marked at a level and category specified by the team lead until review by an Authorized Derivative Classifier can be performed. Working papers are used to support the validity of findings and as a source of information for future reviews. These papers also can be used for assessing the progress of the review, especially if an extended data collection methodology is employed. Working papers are maintained at least until the completion of the following survey or self-assessment. If deemed useful for extended tracking and trending of issues, they may be retained for longer periods.

Data collection methods and techniques are chosen based upon their utility in addressing the selected lines of inquiry. Each method and technique has an associated purpose and cost (both to the team and the facility). It is important to know when and where to use each method. For example, running an expensive force-on-force (FOF) performance test would not be cost-effective if the data were available through an interview, observation, or limited scope performance test (LSPT). An essential step that should be accomplished in the planning phase is to associate data collection methods with each line of inquiry chosen.

The results of previous Federal and contractor reviews, including facility description, security interests examined, and findings and suggestions, shall be considered as a valuable data source. The corrective action plans and resolution of the previous findings also are indicative of the quality of the program and level of management support the program receives. In particular, the review of past findings can reveal significant indicators of the effectiveness of S&S program management. Concerns about open or repeat findings or the inability to establish and implement effective corrective action plans in a particular topical area should be discussed with the entire team. The determination of whether similar concerns exist in other topical areas will give those performing the program management evaluation important indicators as to whether the issues extend beyond the topical area in which they were first identified.

It is always desirable to minimize impacts to the facility. For example, procedures, such as special nuclear material (SNM) transfers, security alarm preventive maintenance checks, or portal monitor checks, should, whenever possible, be observed during regularly scheduled times rather than at the team's request for a special demonstration. However, the need for data to inform the analysis of a line of inquiry is primary. For example, if an operation such as a nuclear material inventory is not scheduled during the survey or assessment and observing the operation is critical to evaluating system operations, then initiating an inventory through a performance test is appropriate.

d. Performance Tests

Performance testing is a key data collection technique deserving special mention. While compliance with specific directive requirements is one of the primary interests of a review team, the actual performance of processes, personnel, and systems in providing protection to national security assets should be measured to provide an appropriate level of assurance that assets are adequately protected. Performance tests are typically onsite exercises of the personnel, equipment, and/or procedures of selected portions of S&S systems to determine system effectiveness. Performance tests are not limited to the systems protecting special nuclear material or classified matter; they can be conducted to assess any portion of the facility security design. In all cases, they should focus on the elements of a topic or sub-topic that are essential to the effectiveness of that topic or sub-topic. Performance tests will not necessarily reflect the overall state of security at a facility because the observed result of a performance test usually reflects only on the security element tested, not the full protection system. Further, the outcome of a single performance test can reflect temporary or unusual conditions existing at the time of the test. Therefore, while the results of a single performance test are valid data, performance test data should be placed in context with other findings, observations, and conclusions.

Performance tests shall be designed to provide objective data to assist the team in determining whether:

- Personnel know and follow procedures;
- Procedures are effective;
- Plans and procedures accurately describe operations conduct;
- The processes described in procedures produce the expected product;
- Personnel know how to operate equipment;
- Personnel and equipment interact effectively;
- Equipment is functional, operational and effective;
- Equipment has adequate sensitivity; and/or,
- Equipment meets design objectives.

If the facility has a program for conducting performance tests, the team should consider requesting that the facility conduct one of its performance tests rather than, or in addition to, one designed by the team. Observing the facility conduct a performance test provides information concerning the facility's own assessment program as well as providing the needed data about the protection element being

tested. An additional source of performance data is the routine documentation maintained in the course of implementing an S&S program. Performance data reflected in facility documentation such as inventory records, files, classified documents, reports, and access logs are useful in assessing the effectiveness of control processes.

e. Data Validation

An essential component of data collection is data validation. When any data is collected, it is imperative that the data collector determine whether site personnel observing the same event perceive the same outcome as the data collector. If they do not, it is essential to understand why not and to inform the site observer why the data collector has a different perception. It is also essential to share this perception because of the limited sample set that is collected during a review. If site personnel understand that the data collector perceives the result of an observation differently than they do, it provides them an opportunity to supply additional data that provides a fuller context to the data collector's view of the result.

Similarly, it is important for the team to share perceptions with site management on a periodic basis. Site management should be informed when the assessment team is moving toward a conclusion in a particular area, whether that conclusion is positive or negative. Again, site management might be able to offer additional information that would modify the team's view of the situation.

When final conclusions are reached in the survey or self-assessment report, they shall be based upon a set of facts agreed to by both the review team and the site. However, the analysis of those facts, and the subsequent assessment of site protection effectiveness, is always the sole prerogative of the review team.

f. Data Analysis

After all data is collected and verified to be current and accurate, it should be compiled and analyzed to determine the effectiveness of protection by overall facility, by topical area, and/or by sub-topical area, as appropriate. The facts established during the data collection and validated by the site and the team's analysis of those facts form the basis for observations and findings in the final report. Even when no findings or observations are made, the presentation of validated data and the logical interpretation of that data is a valuable contribution to management understanding of site status and should never be neglected in the final report. Key facts and the team analysis of them should be documented in the report immediately before an observation or finding is made and additional supporting information, if any, should be contained in the retained working papers. The logical path from facts to the finding or observation needs to be clear in the final report, even if some detail is omitted. Findings and observations shall be clearly identifiable in the final report and shall be highlighted during the close out briefing. It is often helpful to repeat all findings and observations from all topical areas in a single appendix or attachment to the report. Tracking and trending of results is enhanced by the assignment of a unique tracking number to a

finding or observation, especially findings, to assist in tracking and reporting on actions taken in response. For findings in particular, since they must be entered into the SSIMS database, a tracking number is needed that conforms to the SSIMS finding format. An example would be 13-NOV-01-HQ-0123-SSIS-PM-001, where 13-NOV-01 is the date of the survey, HQ is the cognizant security office, 0123 is the facility code for the surveyed facility, SSIS is the type of survey (see DOE O 470.4B, Appendix A, Section 2, paragraph 3), PM is the topical area in which the finding is made, and 001 is a sequential number of the finding within the topical area.

The terms finding, observation, suggestion, opportunity for improvement, and others are used in surveys and self-assessment reports to indicate issues that require management attention. The term finding is defined in DOE policy and is always used to identify any validated program deficiency (a failure to meet a performance or compliance requirement derived either from internal or external directives or the approved site/facility security plan.) The term observation is used to identify areas where the review team perceives a need for particular management attention, even if DOE requirements and security plan performance elements have been met. Observations also may be used to identify potential areas for program enhancement. In some cases, survey and self-assessment programs have used the terms suggestion or opportunity for improvement. These are similar in intent to an observation, but are used to clearly separate potentially positive results from potentially negative ones. Usually this distinction is made when management believes both findings and observations are indicators that program improvements are needed whereas a suggestion or an opportunity for improvement indicates that the review team has identified a potential program improvement which local security management might consider. Findings, observations, suggestions, opportunities for improvement, or any other conclusion reached during data analysis shall be based upon validated data collected during the various activities comprising the review.

g. Ratings

Upon completion of survey or self-assessment data collection, a recommended rating for each sub-topical and topical area reviewed shall be determined, usually by the topical team members. When considering a topical rating, the topical team should consider the results from each sub-topical area and the relative contribution of each sub-topical area to the success of the overall topic within the local context. The logic and determinations supporting the recommended ratings should be included in the draft survey or self-assessment report to support the topical rating proposed to the team leader.

The team leader, in consultation with topic leads and team members, shall determine the composite facility rating and the topical and sub-topical ratings, based upon the results of the survey or self-assessment. The team leader shall ensure that the basis for the rating determinations is explained in the survey or self-assessment report. A composite facility rating shall be based upon the topical and sub-topical ratings and an analysis of the relative importance of each topical and sub-topical area in the overall protection design of the site/facility. As with each of the topical and sub-topical

ratings, the logic and considerations leading to the award of the composite facility rating should be explicitly addressed in the survey report.

The ratings listed below are used for all surveys (except termination), reviews, and self-assessments. Does Not Apply (DNA) and Not Rated (NR) shall also be used in lieu of a rating when appropriate.

- Satisfactory. The element being evaluated meets protection objectives or provides reasonable assurance that protection objectives are being met.

- Marginal. The element being evaluated partially meets protection objectives or provides questionable assurance that protection objectives are being met.

- Unsatisfactory. The element being evaluated does not meet protection objectives or does not provide adequate assurance that protection objectives are being met.

A topic or sub-topic should be rated **Satisfactory** if all aspects of the topic or sub-topic are found to be as depicted in the approved security plan, including any approved equivalences or exemptions, and observed performance is sufficient to provide assurance that the topical or sub-topical elements are providing the level of protection assumed in the approved site/facility security plan. In particular, any security element within the topic or sub-topic that is identified as an essential element shall demonstrate performance at least equal to that required to support overall security effectiveness, as documented in the approved security plan. A topic or subtopic should also be rated Satisfactory if, for any measure not met, documented and approved compensatory measures are in place to provide comparable protection and action is either under way to return the security elements comprising the topic or sub-topic to full capability or an approved plan to restore the security elements is being satisfactorily pursued. In some instances, a topic or subtopic might be rated Satisfactory when some component element fails to meet an applicable measure but, in the judgment of the topical area experts and the survey team leader, the impact of that shortfall does not erode the contribution of the topic or sub-topic to the effectiveness of S&S under the approved security plan. The logic underlying such a decision shall be included in the survey report. Notwithstanding the Satisfactory rating, however, the component should be brought to full effectiveness as soon as possible in all cases.

Noncompliance with one or more requirements of the approved security plan shall result in a rating of **Marginal** or **Unsatisfactory** for a survey or self-assessment topic or sub-topical area when the observed shortcoming(s) reduces the assurance that the S&S program, as depicted in the approved security plan, represents the actual S&S practices at the site or facility. If performance testing indicates that a significant question regarding adequate protection exists, even when the site/facility is in full compliance with the approved security plans, a topic should be rated no higher than Marginal.

Assignment of one or more subtopic ratings of Marginal or Unsatisfactory shall lead the topical area team to carefully analyze the seriousness and multiplicity of findings

in a sub-topical area against the definitions for Marginal or Unsatisfactory before assigning a rating to a topic. If less-than-satisfactory sub-topical ratings exist within a topical area rated Satisfactory, the survey or self-assessment report shall explain why the impact of these sub-topical ratings do not justify a reduced topical rating.

A topic or subtopic shall be rated **Unsatisfactory** if limited compliance with the approved security plan and/or performance testing results indicate that the topical or sub-topical contributions to the approved security plan fall short of the performance required to protect security assets. Performance should consider the adequacy of any compensatory measures in place when the rating is determined, since adequate compensatory measures supported by a plan to restore the planned functionality can result in a satisfactory rating. However, an unsatisfactory rating shall also be awarded if no plan exists for restoring security element function and removing current compensatory measures, even if the compensatory measures provide a temporary mitigation of the security concern.

After ratings have been assigned to all sub-topics and topics, a rating shall be assigned to the site/facility. While the same three ratings are available – Satisfactory, Marginal, and Unsatisfactory – the context is somewhat different. The site/facility rating shall be based upon an integrated view of the entire security program, taking into consideration the topical ratings. The site/facility rating is the team leader's certification to the appointing official regarding the security status of the site/facility. A Satisfactory rating indicates that the site/facility is operating in accordance with the approved security plans and that the demonstrated S&S performance is at least equal to that required to adequately protect all site/facility security assets. A Marginal rating indicates that action is needed to advance the site/facility toward compliance with the approved security plans and/or to fully achieve the performance anticipated when the security plans were approved. An Unsatisfactory rating conveys the team's judgment that immediate management attention is needed to ensure continued protection of one or more of the national security assets located at the site/facility or to ensure that adequate progress will be maintained toward achieving a satisfactory status.

h. Exit Briefing

At the conclusion of the survey or self-assessment, an exit briefing should be conducted with management officials of the organization reviewed. The briefing should include at least a summary of the following areas:

- Program strengths and weaknesses, including all findings and observations;
- Corrective action reporting requirements for all open findings, regardless of source; and,
- Sub-topical, topical and facility ratings.

The team leader should prepare an agenda for the exit briefing. Because of the potential for confrontation during the briefing, it is generally best for the team leader

to provide the briefing and, if necessary, to ask the topical leads to assist with technical details. Agreements and commitments made during the conduct of the survey should be summarized during the exit briefing. This provides an opportunity to identify potential misconceptions before they are presented formally to management outside the surveyed facility. Agreements and commitments should be documented in writing as soon as possible.

10. REPORT PREPARATION

As soon as possible after the survey or self-assessment is completed, a formal report of the results shall be finalized. The individual team members and topic and subtopic leads should ensure that a complete, concise, and accurate final report of the results is compiled in a timely manner. The report preparation shall be overseen by the team leader, who has ultimate responsibility for its completion and accuracy.

Reports and all working papers and other retained material shall be evaluated and reviewed by an Authorized Derivative Classifier before publication of the final report. Before this review, the working drafts shall be protected and marked as working papers classified at a level determined by the team leader to be the highest likely classification of the final report, including paragraph markings as appropriate. Required protection and control shall be provided for classified or sensitive information. Even if the overall report is determined to be Restricted Data (thereby eliminating the requirement for paragraph marking), each finding shall be marked with its classification level and category to ensure that the information will continue to be protected appropriately when the finding is extracted from the report.

Team meetings should be held as necessary to facilitate the finalization of the survey report and evaluate lessons learned from the review. During these meetings the following actions should be undertaken as necessary:

- Review draft report or report section(s);
- Review lessons learned;
- Identify trends that might indicate areas of interest for the next review;
- Identify helpful information sources and resources to consider in the next review;
- Review and summarize agreements and commitments made during the conduct of the review and the exit briefing;
- Determine final report content, especially for areas of contention;
- Document any unique organizational structures/functions or item of potential use to those planning the next review; and,

- Prepare for briefings on the review results to DOE and contractor management, as appropriate.

The survey report should consider all available data in its analysis. Depending upon the survey methods used, this may include data that reflect:

- documented observations of activities at the surveyed facility;
- full and limited scope performance tests;
- documented data collection conducted during the survey period;
- the results of any documented Federal shadowing of contractor self-assessments;
- targeted data collection conducted to satisfy remaining data requirements late in the survey period (particularly as required to verify accuracy of information acquired during rolling assessments, contractor shadow activities, or derived from contractor reports);
- any other documented, objective data that the survey team determines is pertinent.

The resulting report provides measurement results, an analysis of those results, including ratings, and specific identification of areas needing improvement, in the form of findings, observations, and/or suggestions to management.

The appointing authority responsible for the conduct of the survey or self-assessment should require that a review board be established to review the draft report and make recommendations to the team leader to improve the report. Such a board can significantly improve the final product by verifying that there is a clear, logical presentation of results. Questions regarding what assets were present at the facility, what data collection methods were used, what facts were discovered using those methods, what facts were considered and with what relative weight to arrive at findings and ratings, and what factors support the overall facility rating should all be clearly addressed in the report. Use of a review board can ensure that all these questions are adequately addressed and logically presented in the final report.

After the report has been completed, SSIMS data entries have been made, and the report has been distributed, the team leader should document and file lessons learned. These lessons learned should identify what processes were effective, observations of team dynamics, and specific recommendations for the next review. The team leader should include lessons learned as reported by topical leads and their teams. These lessons learned should be provided to the appointing authority for information and evaluation to improve the survey process.

11. CORRECTIVE ACTION PROGRAM

A survey or self-assessment activity only fulfills a portion of its objective if it lacks a robust corrective action program. Therefore, DOE directives require that corrective actions are taken for findings, that finding status is tracked to completion, and that accumulated findings from a given site/facility and from all sites/facilities surveyed or self-assessed by a review activity should be subjected to trending analysis to determine whether they collectively indicate a broader weakness in the S&S program that is not fully addressed by the corrective actions taken in response to the individual findings.

A corrective action program shall include, as a minimum:

- Causal analysis appropriate to the complexity of the issue identified (the rigor of causal analysis should not be based upon the perceived consequence of protection element failure – sometimes very serious issues have readily apparent root causes and sometimes important lessons can be learned from issues that have little immediate protection impact – but on the difficulty in identifying the root causes);

- Identification and implementation of compensatory measures required to maintain required performance levels while corrective actions are in progress;

- Identification and implementation of priorities for completion of corrective actions if all cannot be pursued simultaneously (priorities might be based on availability of resources, costs of associated compensatory measures, and many other factors);

- Identification and implementation of necessary validation testing when corrective actions are complete and before compensatory measures are removed; and,

- A means of tracking and trending causal factors to allow identification of possible systemic management issues that are only discernible when viewing the results of multiple reviews. It should be noted that tracking in SSIMS is required for survey findings.

To maximize the value of surveys and self-assessments, it may also be desirable to go beyond the basic requirements applicable to findings and corrective actions. For example, observations do not specifically require action on the part of the site management, but the careful consideration of observations can lead to improvements in S&S program effectiveness and/or efficiency. Other considerations noted in the survey or self-assessment report or even in supporting working papers may be useful as well, even if the team did not believe they should be highlighted as a finding or an observation at the time of the final report. An examination of these additional factors in conjunction with the findings may contribute to the development of more effective corrective actions or lead to more in-depth improvements which will strengthen and enhance the overall security posture at the site.

APPENDIX A.

SAFEGUARDS AND SECURITY SURVEY AND SELF-ASSESSMENT TOOLKIT

1.0 INTRODUCTION

This Toolkit was created to augment the Safeguards and Security (S&S) Survey and Self-Assessment Technical Standard by providing a variety of samples and tools that may be used to complement the overall survey/self-assessment process. The Toolkit is not meant to be all-inclusive, but rather to provide a starting point that can be expanded and built upon.

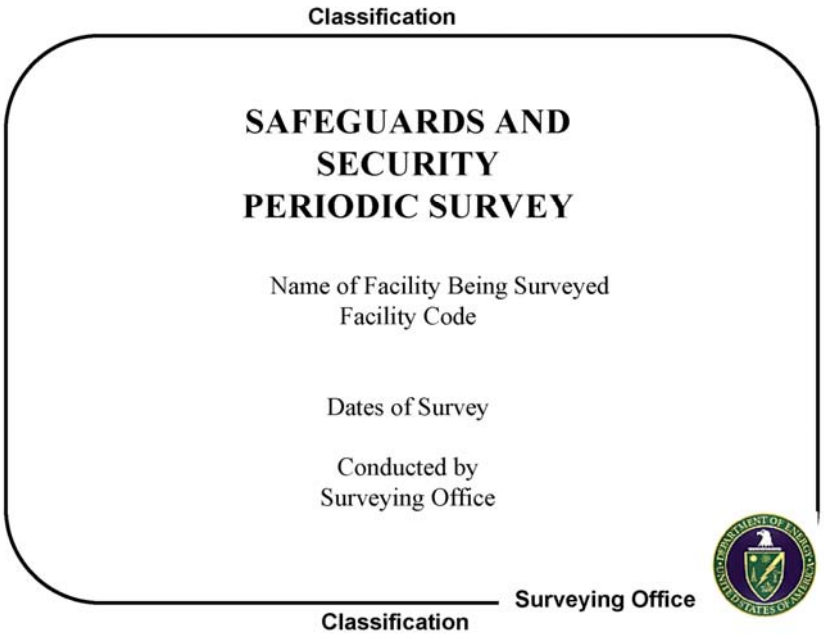
The Toolkit is divided into three sections: Planning, Conduct, and Post-Survey Activities. The Planning section provides tools associated with survey notification, planning, and in-briefings. The Conduct section is broken down into topical areas and their respective subtopical areas. Each topical area contains information, such as areas to be considered in the survey, sample interview questions, etc., that may assist the surveyor in conducting the survey. The Post-Survey Activities section includes sample survey formats, exit briefing slides, transmittal memos, sample corrective action plans, and DOE F 470.8, *Survey/Inspection Report*.

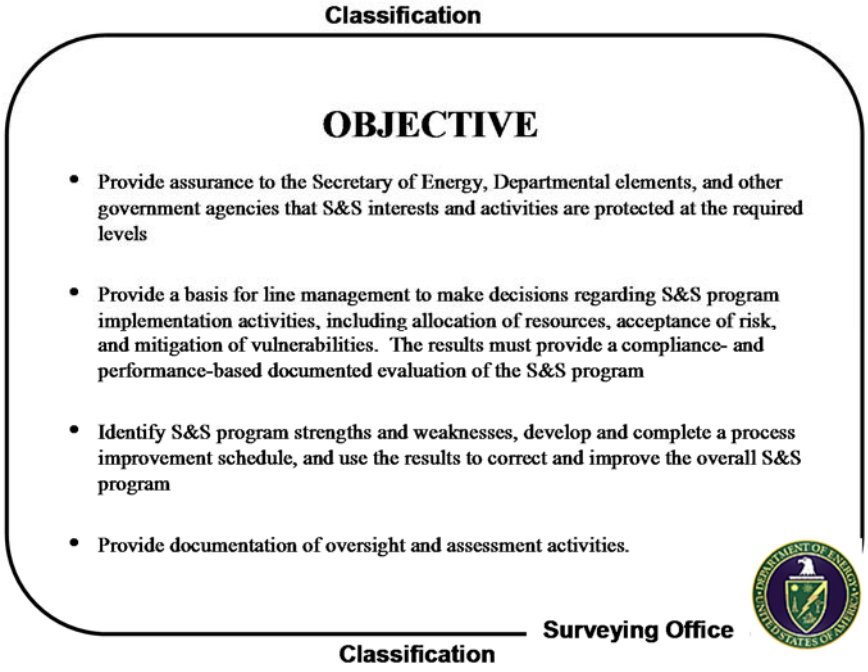
2.0 PLANNING TOOLS

This section addresses the logistics and notifications associated with conducting a survey or self-assessment and provides sample documents for survey notification, planning and in-briefings. The following specific areas are addressed:

2.1 Sample In-Briefing
2.2 Sample Survey Plan Format
2.3 Documents For Possible Review
2.4 Sample Notification Memos
2.5 Sample Accommodation Request

2.1 Sample In-Briefing (Customize for specific survey objectives, activities, etc.)





Classification

SCOPE & METHODOLOGIES

SCOPE - Assess status of all S&S topical areas

- Compliance
- Performance
- Comprehensiveness

METHODOLOGIES

- Status of Open Findings
- Status of Corrective Actions
- Field Reviews, Self-Assessments, Surveillances, etc.
- Performance Tests
- Document Reviews
- Interviews

Surveying Office

Classification

Classification

Topical Area Leads & POCs

	Ph	Pg
Survey Team Lead		
Name, Survey Team Lead		
Name, Contractor Point of Contact		
Program Management & Support		
Name, Survey Topical Lead		
Name, Contractor Point of Contact		
Protective Force		
Name, Survey Topical Lead		
Name, Contractor Point of Contact		
Continue for each topical area.		

Surveying Office

Classification

Classification

Schedule of Activities

Data Gathering
M/D/Y through M/D/Y

Report Writing
M/D/Y through M/D/Y

Data Validations will be completed daily by team members and their respective points of contact.

A Summary Validation meeting will be conducted at the end of data collection activities (give time/date/location and expected participants).

Surveying Office

Classification

Classification

Schedule of Activities (cont.)

Exit briefing:
Date: (M/D/Y)
Time: (Time)
Conference Room: (Number)
Building: (Number)

Attendees will be limited to Topical Leads and their respective point of contact, and upper management.

Surveying Office

Classification

2.2 Sample Survey Plan Format

1. Title of survey

2. Location of facility

3. Purpose of survey

4. Survey dates

5. General facility information /description
   a. Facility data
   b. Work/activities performed
   c. Operating organization (contractor)
   d. S&S interests
   e. Strategic Partnership Projects or other security activities

6. Scope of survey
   a. Period of review, including extended observation or data collection if applicable
   b. Objectives
   c. Topical areas to be included/excluded and justification for each
   d. Topical areas with findings from previous surveys, inspections reports, audits and appraisals (e.g. Government Accountability Office [GAO]/ Inspector General [IG])
   e. Special areas/items of interest/concern

7. Survey planning and preparation
   a. Performance tests (associated safety plans)
   b. Survey guide information
   c. Pre-survey information

8. Survey conduct—approach and methodology
   a. Documents to be reviewed
   b. Performance tests
   c. Individuals to be interviewed
   d. Sampling activities, including extended observation, shadowing or surveillance if applicable

9. Schedule of activities
   a. Survey schedule
   b. In-briefing information
   c. Coordinating instructions
   d. Exit briefing
   e. Schedule for report development

10. Team composition/assignments
    a. Team members
    b. Assignments/responsibilities
    c. Contractor support
    d. Points-of-contact at the facility

11. Authority/governing documents
    a. Directives
    b. References (unclassified/classified)

12. Survey report format

13. Administration, support, and logistics
    a. Work facilities
    b. Transportation
    c. Computer support
    d. Administrative support
    e. Classification support
    f. Training requirements

14. Appendices
    a. Performance tests (including Safety Plans)
    b. Survey guides
    c. Forms

2.3 Documents for Possible Review

The following is a list of documentation that **may be** considered for review during survey conduct. Whether or not to include these documents as part of the data call or to review during the Conduct phase will be determined based on the focus of each topical area, as outlined in the survey plan. The list is not comprehensive; other documents may be available which should also be considered

Program Management Operations

- Organization charts depicting the Safeguards and Security (S&S) management structure and S&S functional structure
- Documents depicting responsibilities and authorities of S&S management, including all delegations of authority and designations of Officially Designated Federal Security Authority (ODFSA) and Officially Designated Security Authority (ODSA)
- Position descriptions for S&S management
- Program Office and local instructions for the implementation of S&S programs
- Supplemental documents and guidance for implementing S&S programs
- Facility/site security plan (SP) and any referenced or supplemental plans and documentation
- Emergency management and security condition (SECON) plans
- Survey reports, inspection reports, Government Accountability Office and Inspector General audit/appraisal reports, self-assessment reports
- Staff raining records
- Contract(s), including Statement of Work
- List of all subcontractors and consultants conducting work for the contractor
- List of U.S. Department of Energy (DOE) directives and security clauses that have been incorporated into applicable contracts
- Approved and pending equivalencies/exemptions to DOE directives and any deviations to national drivers (e.g., Code of Federal Regulations)
- Copy of the facility registration
- Applicable Memoranda of Understanding (MOU)/Agreement (MOA)
- Completed Foreign Ownership, Control or Influence (FOCI) questionnaire (SF 328)
- Key Management Personnel (KMP) list
- Dates of all applicable FOCI determinations and copies of any mitigation agreements
- A copy of the contractor's records of all contracts and subcontracts involving access authorizations
- Vulnerability Assessment (VA) reports
- Risk assessment reports
- Contingency plans
- Survey and self-assessment program procedures
- Issues management plans and procedures
- Corrective action plans and status updates for all open deficiencies
- Finding/deficiency corrective action validation and closing procedures
- Incidents of Security Concern procedure, including initial notification and inquiry reports
- Contract Security Classification Specification (CSCS) forms
- Facility Data and Approval Record (FDAR) forms
- Copy of the approved Performance Assurance Program Plan
- List of essential elements documented in the Performance Assurance program and the testing schedule for each
- Documentation of the integrated contractor assurance system

Protective Force (PF)

- Organization and function charts
- PF general, special and post orders
- PF shift schedules and post assignments
- PF standard equipment issuance (Security Police Officer [SPO] I, II, III, and Special Response Team [SRT])
- PF weapons and ammunition inventories
- Weapons maintenance logs
- MOU with local law enforcement agencies and documentation of exercises conducted with those agencies
- Integration of crisis management personnel into procedures
- PF training records which include:
  - A list of PF personnel who are subject to weapons qualification within 90 days of the start date of the survey
  - A list of PF personnel who are medically certified to participate in the physical fitness program
  - All documentation of PF exercises conducted since the last S&S survey
  - Instructor certification
  - Job analysis
- Job task analyses
- Security Emergency Response Plan (SERP)
- Security Incident Response Plan (SIRP)
- Facility Evacuation Response Plans
- Security Contingency Response Plans
- Target folders
- Schedule for performance testing (results of recent tests)
- Compensatory measures currently in place (including pertinent documentation)
- Procedures (administrative, training, non-response-related operational requirements)
- Access/badge control
- Information containing, at a minimum, policies/procedures for issuing, replacing, and recovering passes/badges
- Inventories (since last S&S survey) of passes/badges made, issued, lost, recovered, returned, and destroyed
- Shipment security plans
- Shipment procedures
- In-transit emergency plan
- Shipment emergency response plan

Physical Protection

- Organization and function charts
- Lock and key records and procedures
- Automated access control system records and procedures (including biometric access input as well as access credential issuances (e.g., keycards, tokens)
- Barrier maintenance procedures/records
- Property control procedures
- Access control procedures
- Local performance testing plans and procedures
- Physical security system description(s) and location(s)
- Intrusion detection system (IDS) maintenance and testing records and procedures
- IDS Analysis and Evaluation Report

- Unscheduled alarm reports
- Central Alarm Station (CAS)/Secondary Alarm Station (SAS) procedures (interface description)
- Emergency response for CAS/SAS recovery
- Emergency power systems (uninterruptible power supply system)
- Compensatory procedures for equipment outages
- Security container documentation and maintenance records
- Automated systems description and procedures
  - Manual
  - Procedures
  - Controls
- Calibration and testing procedures and records (e.g., X-ray, metal detectors, IDS)
- Inspection procedures
- Limited Scope Performance Test (LSPT) results

Information Security

- Organization and function charts
- Training records
- Technical surveillance countermeasure (TSCM) survey reports
- Site inventory of accredited systems, showing property tag number, the accrediting authority, and most recent accreditation date for each
- Formal assignments of TSCM personnel
- TSCM activity support memoranda (if applicable)
- Local TSCM implementation guidance
- TSCMO service schedules, files, and corrective action reports
- TSCM team equipment maintenance and calibration files
- TSCM team training and certification records
- Operations Security (OPSEC) Plan
- OPSEC procedures
- OPSEC program files
- Local threat statement
- Critical Program Information
- Counter-Imagery Program Plan (if applicable)
- Number of derivative classifiers and declassifiers
- Appointment letters (e.g., Inquiry Officer, custodians)
- Training records, reports, and lesson plans
- Classification guidance
- Classified Matter Protection and Control (CMPC) procedures
- Control station procedures
- List of classified holdings, including documents, electronic media, and matter
- Number of Special Access Programs (SAPs)

Personnel Security

- Local procedures for terminations, leave of absences, reinstating clearances, clearance processing, exit briefing process
- Contractor access authorization requests
- Sample initial, comprehensive, refresher, and termination briefing materials
- Previous findings and corrective action plans
- Reciprocal access authorization documentation
- Awareness tools (posters, newsletters)

- Security infraction and violation records
- Requests for visit or access approval (notification and approval of incoming and outgoing classified visits records and records of cleared non-DOE personnel granted access to RD)
- Written delegation of senior Federal official authorized to make determinations on access to Restricted Data by non-DOE personnel in connection with a classified visit
- Visitor control logs
- Local visitor control procedures
- Central Personnel Clearance Index (CPCI) list of individuals overdue for reinvestigation
- Drug testing/handling procedures
- Drug testing records
- Human Reliability Program (HRP) participants
- HRP criteria/plans/procedures
- Random test procedures
- List of individuals on leaves of absence and the associated procedures for tracking
- List of inactive classified contracts
- List of personnel with access authorizations and the associated contract(s)
- List of clearances terminated during the survey period
- List of all access authorizations held by the contractor, including all contractors and subcontractors that have cleared employees conducting work at the facility. This list can come from the DOE CPCI of access authorizations held by the contractor. The CPCI and contractor lists, including the current KMP list, should be compared for discrepancies.

Foreign Visits and Assignments

- List of foreign visitors from sensitive countries during the survey period
- Specific security plans for foreign visitors from sensitive countries
- Escort procedures
- Local procedures for requesting, processing, and approving visits and assignments
- List of foreign visitors or assignees, including hosts, during survey period
- Incident reports involving foreign nationals
- Requests for foreign national visits
- Indices checks
- Documentation authorizing approval for specific categories of visits and assignments
- Sensitive country listings
- Equivalencies/exemptions pertinent to visits and assignments
- Personnel assignment agreements

Nuclear Material Control and Accountability (MC&A)

- MC&A plans and procedures
- Training records, reports, and lesson plans
- Performance tests
- Categorization process documentation
- Incident reporting process and procedures
- Emergency response plans and facility procedures
- Database descriptions
- Material Balance Area (MBA) account structure
- Material transfer records
- Internal control procedures
- Nuclear Material Management and Safeguards System (NMMSS) reports
- Shipper/receiver difference procedures and records
- Material control indicator program

- Inventory difference program
- Materials containment documentation
- Facility procedures
- Material access program
- Authorization access lists
- Search procedures
- Material surveillance procedures
- Portal monitor records and procedures
- Daily administrative check program and procedures
- Tamper indicating device program

2.4 Sample Notification Memos

2.4.1 Notification and Data Call

DATE:

TO:

FROM:

SUBJECT: Notification and Data Call Request - Safeguards and Security (S&S) Survey of XYZ Facility

This memorandum is to formally notify you that a representative of the [Surveying Organization] will conduct a S&S survey of the XYZ facility and its satellite offices during the period [Date–Date], in accordance with the requirements of DOE O XXX, [*Title*], [Appendix, Section, Chapter, etc.]. The topical areas to be evaluated include:

- Program Management Operations
- Protective Force
- Physical Security
- Information Protection
- Personnel Security
- Foreign Visits and Assignments
- Nuclear Materials Control and Accountability.

A list of personnel participating in the survey is reflected in Attachment 1. The Survey Team Leader is John Doe. This survey involves a review and evaluation of the S&S program as implemented by the XYZ facility.

System performance tests will be conducted during this survey in several topical areas. Attachment 2 contains the data call. Please ensure the data call items are available for the survey team's review no later than [Date]. Items can be sent electronically to the Survey Team Leader or in hardcopy form to Room XXX, Building XXX. The in-briefing will be held on [Day, Date], in Room XXX, Building XXX. The exit briefings are scheduled for [Day, Date], in [place] at time(s) to be announced at a later date.

If you or your staff have any questions or require additional information, please contact John Doe on [phone number] or by pager [pager number].

2 Attachments

2.4.2 Safeguards and Security Periodic Survey

DATE:

TO:

FROM:

SUBJECT: Safeguards and Security Periodic Survey (SSPS)

The [Surveying Organization] will conduct an SSPS of the [Organization to be Surveyed] during the period of [Date–Date]. This will be a comprehensive survey and will be conducted in accordance with [Appendix, Section, Chapter, etc.] of DOE O XXX,[*Title*]. The survey will examine the performance of safeguards and security programs to ensure that S&S measures employed by the facility are adequate for the protection of security assets and interests and will encompass all topical areas on DOE F 470.8, *Survey/Inspection Report Form*.

To aid in the planning process, you are requested to provide the documentation listed in the Attachment. These documents are to be provided to [Survey Team Leader] not later than close of business [Day, Date]. In addition, please provide points of contact information for each topical area, including pagers/cellphone and phone numbers. The names of [Surveying Organization]'s Survey Team Leader and Topical Area Leads will be forwarded to your organization under separate cover.

Survey activities will begin with an in-briefing at [Time, Date], in [Place]. Points of contact representing your organization in each topical area should plan to attend.

If you have any questions or require additional information, please contact [Survey Team Leader] on [phone number].

Attachment

[Sample Attachment - Documentation Request]

Attachment 1

All documentation provided should include the past 12 months unless otherwise noted.

Program Management Operations

1. Organization chart(s) or listings with brief description of organizations functions and responsibilities
2. Current site security plan with all referenced or supplemental plans
3. Recent self-assessment report(s)
4. Copy of findings/corrective action plan tracking procedures
5. Current status of all open and closed findings/corrective action plans since the last survey (including Office of Independent Enterprise Assessments, Government Accountability Office and Inspector General)
6. List of and current status of all approved policy equivalencies and exemptions and any approved deviations from national policy (e.g., Code of Federal Regulations)
7. List of all subcontractors performing work (name of company, contract number, names of individuals with access authorizations)
8. Copies of all CSCS and FDAR forms related to the facility clearance

Protective Force

1. Facility security plans
2. Emergency security operation procedures
3. Security emergency response plan
4. Memoranda of Agreement/Understanding (e.g., with local law enforcement)

Physical Protection

1. Security systems test procedures
2. Security systems maintenance procedures
3. Lock and key records and procedures
4. Access control procedures
5. Unscheduled alarm reports for the past three months

Information Security

1. List of locations where classified matter is stored and the name and telephone number of the responsible custodian
2. List of locations where classified matter is used/processed
3. List of total number of classified materials and documents in accountability, including level and category
4. Operations Security (OPSEC) plans
5. All training materials to support the OPSEC program (have available on request)
6. All documents that support OPSEC briefings for contractor personnel (have available on request)
7. All other internal program procedures that support OPSEC
8. List of derivative classifiers

Personnel Security

1. List of all assigned (cleared) employees/subcontractors who have traveled to sensitive countries (official and unofficial)
2. List of all visits and assignments of foreign nationals

3. List of all subcontractors
4. List of uncleared visitors
5. List of outgoing classified visits
6. List of all incoming classified visitors
7. List of Human Reliability Program participants
8. List of terminated clearances (including name, date termination statement signed, date clearance terminated, Central Personnel Clearance Index [CPCI] number)

Foreign Visits and Assignments

1. List of visits
2. List of foreign national (FN) visitors from sensitive countries
3. Specific security plans for FNs visiting from sensitive countries
4. Escort procedures
5. Local procedures for requesting, processing, and approving visits and assignments

Nuclear Material Control and Accountability (MC&A)

1. Categorization process documentation
2. Material Balance Area account structure
3. Inventory difference program plans
4. MC&A plan/procedures (may be part of site security plan or separate document[s])

2.4.3 Initial Safeguards and Security Survey

Date:

To:

From:

Subject: Safeguards and Security (S&S) Survey of XYZ Company

This memorandum confirms informal arrangements between [Surveying Office] and [Organization to be Surveyed] Safeguards and Security Organization personnel that established [Date–Date] as the dates for the [Surveying Office] S&S survey of the [Organization to be Surveyed] facility. The survey is conducted in accordance with Title 48 Code of Federal Regulations Subpart 952.204.73(c) and the requirements of DOE O XXX, [*Title*], [Appendix, Section, Chapter, etc].

An informal and brief preliminary meeting is requested for [Date, Time] with S&S management and selected survey personnel. The survey process will be discussed during this meeting.

Enclosure 1 is a pre-survey questionnaire/data call that identifies the preliminary information required in the topics to be surveyed. Please provide this information to [Surveying Office] by [Date]. This material will be distributed to team members for review and familiarization prior to the survey. Enclosure 2 identifies the accommodations requested for the team's use during the survey.

If there are any questions regarding survey activities, please contact [Survey Team Leader] on [phone number]. Your assistance is appreciated.

Enclosures

[Sample Enclosure - Pre-survey Questionnaire/ Data Call]

Enclosure 1

The survey team needs the following to be delivered to Room XXX no later than [Date] for the XYZ facility and satellite office buildings:

A. PROGRAM MANAGEMENT OPERATIONS

1. A list reflecting security staffing since [*month, year*]. This list should include name of person, date of hire/termination, job title, and security functions (responsibilities)
2. Copies of all memoranda of understanding and management agreements relating to safeguards and security (S&S) programs
3. A copy of all internal operations procedures/practices, with index
4. Copies of the most recent S&S risk assessments, including documentation reflecting risk determination methodology
5. A list of all security training courses that have been approved as part of the training approval plan process
6. A list that reflects the training courses taken by personnel responsible for security functions. Include name, title of course, number of hours, and date of completion
7. Copies of any procedures or other guidance pertaining to the identification and development of S&S training
8. A list of all facilities (copies of Facility Data and Approval Records are acceptable) where the *XXX DOE Office* is identified as the Designated Responsible Office.
9. A list of all classified activities (including the contract), classification level and category of the activity, identification by office and/or Cognizant Security Office, identification by contract number, purchase order number, task statement, or proposal number (including classified Strategic Partnership Projects) (Note: Copies of the Contract Security Classification Specification (CSCS) form may be used in lieu of a listing.)
10. List of all terminated and completed contracts since [*month, year*]. This listing should identify the company/vendor, address/location, Contracting Officer name, organization, office location, and telephone number (Note: Copies of terminated CSCS forms may be used in lieu of a listing.)
11. List of pending Foreign Ownership, Control, or Influence (FOCI) determinations
12. List of FOCI determinations completed since [*month, year*]
13. List of FOCI approved companies, including the FOCI determination date, mitigation types if any, and date of the latest FOCI update
14. A copy of any desktop procedures or other formal XYZ-originated guidance documentation used for the development of the facility/site security plan and other security-related planning documents
15. A list that reflects all S&S plans (e.g., response, emergency, and contingency plans) including title, date, and approval vehicle. Also list any draft plans and plans pending approval
16. Copies of all XYZ-generated guidance or direction (hardcopy or electronic) provided for the conduct of self-assessments and other internal evaluations
17. List of all open findings
18. List of open findings pending validation
19. Copy of Incidents of Security Concern program procedures
20. A list of all security incidents, including computer security incidents, occurring since [*month, year*]. This list should identify the date of the incident, the date of the inquiry report, and the nature of the incident
21. Copies of award fee data (Award Fee Plan, performance criteria)

B. PROTECTIVE FORCE (PF)

1. Copies of all security emergency plans (response, facility evacuation). If this information is not available from this office, please provide the name, organization, office location, and telephone number of the responsible person
2. Copies of all post and general orders, as well as implementing instructions for various program activities (e.g., key control, alarm testing and maintenance, training program development). If this is not applicable to the area being surveyed check here N/A ___. If this is applicable, but the records are not available from this organization, please identify the name, organization, office location, and telephone number of the responsible person
3. Copies of all Memoranda of Understanding (MOUs)/Memoranda of Agreement (MOAs) with local law enforcement agencies (LLEAs) or other organizations/agencies relating to security programs at the XYZ facility and satellite office buildings. If this is not applicable to the area being surveyed, check here N/A ___
4. List of all Protective Force personnel, identified by rank, and supervisors. Also provide a separate listing including PF management name, rank (if applicable), and responsibility (e.g., Lt. John Smith, Supervisor, IMF Instructor, Firearms Instructor)
5. A list of training documentation including, but not limited to, Job Task Analyses, lesson plans, core topics, individual records, physical fitness maintenance. Samples of each should be available for review during the survey
6. Copy of any DOE approval of the PF job analysis
7. Copy of the last (and immediately preceding) annual review of the PF job analysis.
8. Copy of the most recent approved Training Plan
9. If available, an approved Training Approval Program Assessment Report
10. A list of permanent and temporary security posts including post number and hours staffed
11. If existing, a copy of all duty checklists used by the PF during routine and/or emergency operations (e.g., vehicle inspection checklist, incident reports, field interview reports, pre-duty inspection checklists, equipment checklists, Central Alarm Station logs and radio checks, weapons issue, weapons maintenance, weapons cleaning, emergency call-out)
12. Copy of plans documenting the physical configuration of security posts
13. Copy of traffic/parking procedures (safety or security PF interface/enforcement)
14. Copy of general and specific patrol orders that define patrol intervals and routes for classified repositories, vaults, and vault-type rooms
15. Weapons inventory list, including serial number and storage location.
16. Quality Assurance program documentation
17. Communications equipment inventory list, including quantity, make, model, and auxiliary equipment, as well as interface capabilities with LLEA
18. Auxiliary equipment inventory list including quantity, make, model of assigned equipment (e.g., gas masks, protective vests)
19. Copy with pictures (if possible) of patrol and other vehicles used under the contract by the PF. A list including vehicle make, model, vehicle identification number, mileage, condition, unit number, license number, equipment (emergency and standard), owner (company, DOE, or leased from XYZ agency), maintenance agreement, and identification of location of maintenance records (a sample of maintenance records would be helpful)

C. PHYSICAL PROTECTION

1. Copy of key control and property pass procedures
2. Copy of documentation that reflects the total value of capital and sensitive/equipment items (include precious metals as applicable)
3. Listing of all controlled substances and locations, including copies of Drug Enforcement

Agency certificates
4. Listing that identifies all security alarm transmission and monitoring systems, including type, model, manufacturer, and purpose for each (i.e., describe the DOE assets being protected)
5. List of all alarm points identified by system application (e.g., Argus, Litton) and location that provides protection for classified matter and property
6. Copy of the approved alarm test plan and a copy of the DOE approval correspondence
7. Copy of the procedures for making changes to alarm transmission/monitoring systems databases or software
8. Copies of reports since [*month, year*] of unscheduled alarm activations
9. Copy of false alarm rate and nuisance alarm rate since [*month, year*]
10. Copies of maintenance procedures and test results since [*month, year*]
11. Copies of IDS Analysis and Evaluation report since [*month, year*]

D. INFORMATION SECURITY

1. A list of all current XYZ original and derivative classifiers
2. A list of reviewing officials, including name, title, organization, office location, and telephone number
3. A list of all classification guides, including title and date
4. A list of all XYZ shipping/mailroom logs pertaining to the transmission of classified matter since [*month, year]*
5. A list of all areas authorized for processing and storage of classified information/matter, including the classification level authorized and functions performed in each area
6. List of all classified document control stations, including the custodian names, organization, location, and telephone extension.
7. Copy of Classified Matter Protection and Control procedures (marking, destruction)
8. List of all classified material accountability records
9. Copy of DOE-approved Technical Surveillance Countermeasures (TSCM) Plan
10. Copy of the TSCM officers appointment memoranda
11. Copy of the site-wide procedures for the control and use of potential TSCM equipment
12. Copy of the procedures controlling TSCM equipment, the DOE approval for purchasing and controlling TSCM equipment, and an inventory listing, if appropriate
13. Copy of Operations Security (OPSEC) Plan
14. Copy of OPSEC assessment and review reports conducted since [*month, year*]
15. List of contractors (on- and off-site) under the OPSEC program
16. Copy of OPSEC working group meeting minutes for meetings conducted since [*month, year*]

E. PERSONNEL SECURITY

1. A list of all cleared personnel whose access authorization has been terminated since [*month, year*] (Note: This list should include the date of termination, name of person, and organization for which the individual worked.)
2. A list of names of all consultants/vendors issued security clearances that conduct business with XYZ
3. A list of all individuals by name and clearance number terminated for cause
4. A list of individuals by name and clearance number who have had clearances canceled/terminated prior to completion of the background investigation
5. A list by name and clearance number of all foreign nationals who are/were clearance applicants or incumbents. Include in the listing the country of origin and level of clearance
6. A list by name and clearance number of all dual citizens processed for access authorization (clearance) since [*month, year*]

7. A list of individuals on leave-of-absence or extended leave. This list should include name, clearance number, reason for leave, date leave commenced, expected date of return to duty, and/or date of termination
8. Have available each report submitted for derogatory information since [*month, year*]
9. Copy of attendance records for initial, comprehensive, and termination briefings for all contractor employees since [*month, year*]
10. Copies of most current security education briefing/lesson plans for initial, comprehensive, refresher, and termination briefings since [*month, year*]
11. Copy of the compliance verification numbers associated with the most recent refresher briefing
12. Documentation describing the badging system and operating procedures for classified visits. Provide examples of all badge types in use
13. Copy of the procedures for administering incoming and outgoing classified visits
14. Copies of incoming visit requests since [*month, year*]
15. Classified visitor logs since [*month, year*]
16. Copies or log of classified visitor badge requests since [*month, year*]
17. A listing of the number and dates of each positive substance abuse test report
18. A copy of drug test policy
19. A list of all personnel, by name and clearance number, enrolled in the Human Reliability Program (HRP) or other performance assurance program
20. List of all individuals, by name and clearance number, removed from the HRP since [*month, year*]
21. Justifications for HRP positions and date of last review
22. Procedures for Personal Identify Verification process

G. FOREIGN VISITS AND ASSIGNMENTS

1. Lists of all host reports submitted since [*month, year*] including date submitted
2. Local procedures for requesting, processing, and approving visits and assignments
3. List of foreign visitors or assignees, including names of hosts, for survey period
4. Incident reports involving foreign nationals
5. Requests for foreign national visits
6. Indices checks
7. Documentation authorizing approval for specific categories of visits and assignments
8. Sensitive country listings

H. NUCLEAR MATERIALS CONTROL AND ACCOUNTABILITY (MC&A)

1. MC&A Plan
2. Performance test data
3. Categorization documentation
4. Internal control procedures
5. Inventory difference program
6. Shipper/receiver difference procedures and records

2.5 Sample Accommodation Request

The following items will need to be made available to the survey team for the duration of the survey period:

- Two conference rooms or a two-office suite with tables and seating for 15 to 20 people
- Four desktop computers running Microsoft® Windows® [*current operating system*], loaded with Microsoft Word [*current version*] and two Hewlett-Packard LaserJet printers
- Telephones with outside lines and official site phone books or listings
- White board and associated supplies
- U.S. General Services Administration-approved security container (with appropriate markings and required forms)
- Office supplies (staplers, scissors, tape, disks, etc.)
- Copies of XYZ procedures and policy manuals related to survey topics, security plans, Vulnerability Assessments, and applicable DOE directives.

3.0 CONDUCT TOOLS

This section contains tools that have been developed and field-tested by survey and self-assessment teams. They are provided as examples only; other tools may be developed and used as necessary.

3.1 Sample Survey Worksheet
3.2 Instructions for Completing the Sample Survey Worksheet
3.3 Sample Performance Test Safety Plan
3.4 Sample Performance Test Plan

3.1 Sample Survey Worksheet

CLASSIFICATION

WORKSHEET
ORIGINATION DATE:
RESPONSIBLE AGENCY:
FINDING NUMBER:
CONCERN: COMPLIANCE PERFORMANCE BOTH
TOPICAL AREA: SUBTOPICAL AREA:
FINDING DESCRIPTION:
FINDING SYNOPSIS: **IMPACT if not corrected:**
DOE DIRECTIVE:
OTHER (Plan or Procedure Citation):
ORIGINATOR'S NAME/PHONE:
POINT-OF-CONTACT NAME/PHONE:
POINT-OF-CONTACT SIGNATURE:

CLASSIFICATION

3.2 Instructions for Completing the Sample Survey Worksheet

ORIGINATION DATE: Date form completed.

RESPONSIBLE AGENCY: Agency responsible for implementing corrective actions.

FINDING NUMBER: Each finding identified in the survey report should have a unique identification number assigned, which should be used throughout the reporting and tracking process. The following number system provides consistency with the Safeguards and Security Information Management System (SSIMS). A number in this format should be system-generated upon entry of the finding into SSIMS.

Example of a finding number:

04OCT15-HQ-12345-SSPS-PF.1-001-5789
| | | | | | |
1 2 3 4 5 6 7

1: the date of the survey/inspection (year/month/day)
2: the office responsible for correcting the finding
3: the facility code of the facility surveyed/inspected
4: the type of survey (e.g., Safeguards and Security Initial Survey, Office of Enterprise Assessments, Inspector Government Accountability Office)
5: the subtopical area code
6: the sequential number of an individual finding within the topical area
7: the facility code of another facility if a finding was issued to it during the survey

The acronyms used to identify the new topical areas for findings are as follows:

PMS	Program Management Support
PF	Protective Force
PSS	Physical Protection
IP	Information Security
PSP	Personnel Security Program
FVA	Foreign Visits and Assignments
NMCAA	Nuclear Materials Control and Accountability

CODE	**TYPES OF SURVEY DOCUMENTS**
EPR	Excluded Parent Review
GAO	Government Accountability Office Reports
IG	Inspector General Reports
NPR	Non-possessing Review
EA	Office of Security Assessment inspections/reviews
SA	Self-Assessments
SPEC	Special Surveys
SSIS	Safeguards and Security Initial Surveys

SSPS	Safeguards and Security Periodic Surveys
SSTS	Termination Surveys
TSCM	TSCM Reports

FINDING DESCRIPTION: The finding description should be used to provide a clear understanding of what was observed or discovered. It is not adequate to reiterate the requirement. The description should clearly identify the pertinent facts, circumstances, and observations surrounding the finding or leading to the finding.

Findings should be clear and focused on the root cause of the observed protection shortfall, rather than merely stating the occurrence of a protection element failure or weakness. A finding should be written in such a manner that it is actionable by the responsible agency, i.e., that action can be taken that will close the finding and the action will correct the observed deficiency. A well-worded finding is one that is readily closeable when the cause or source is corrected and impossible to close without correcting the cause or source.

Necessary and pertinent information should be presented regarding the finding in order to clearly identify what was found, how the information was collected, and any other background information. The discussions should attempt to correlate the data collected and focus on the root cause of the deficiency. The nature of the data (e.g., observations, interviews, tests) should be described, as well as any quantifying data that will put the results in perspective.

For example:

A review was conducted of all current classified contracts at XYZ. This list was compared to a current badge listing, dated 3-1-15, which showed employees, by company, who currently hold a DOE access authorization. This comparison revealed that individuals holding access authorizations are employed by organizations that do not have Foreign Ownership, Control, or Influence (FOCI) determinations on file.

Based on the FOCI report provided by XYZ personnel, dated 3-1-15, and the employee list by contractor, dated 3-1-15; TCY Company currently holds 7 “Q” clearances and Smith Manufacturing currently holds five “Q” clearances. Neither organization has a FOCI determination on file.

FINDING SYNOPSIS: Each finding should be concisely described in a synopsis format. The SSIMS allows a maximum of 2,000 alpha/numeric characters and spaces. Each finding is to have a separate, stand-alone classification level and category. A separate field is provided for the finding classification level and category. The symbols “S” for Secret, “C” for Confidential, “U” for Unclassified, “OUO” for Official Use Only, and “UCNI” for Unclassified Controlled Nuclear Information shall be used for the classification level.

For example:

Not all organizations employing cleared staff members have an approved FOCI determination.

IMPACT STATEMENT: Clearly identify the impact of the deficiency.

DOE DIRECTIVE: Each finding is to have alpha/numeric references to the DOE directive(s), or other documents that identify the requirement(s) not being met in the finding. This reference

should be written as DOE O XXX.XX, followed by the specific identification numbers and/or letters [e.g., DOE O 470.4B, admin chg., 1, Appendix A, Section 2, paragraph 6.(b)].

OTHER: Identify alternative sources stating the requirement (e.g., section of the Code of Federal Regulations, specific local procedures, site security plan).

ORIGINATOR'S NAME/PHONE: Print your name and telephone number.

POINT-OF-CONTACT NAME/PHONE: Print the name and phone of the POC witnessing the activity.

POINT-OF-CONTACT SIGNATURE: Obtain the POC's signature.

3.3 Sample Performance Test Safety Plan

PERFORMANCE TEST SAFETY PLAN

I, _____, acknowledge receipt of the attached safety plan. I understand it is my responsibility to become familiar and comply with the contents of this safety plan.

Acknowledgment of the receipt of this safety plan is a requirement to participate in or observe this exercise. This page must be signed and returned no later than _____.

Name _____

Signature _____

Position _____

Date _____

Detection of Contraband and Prohibited Items
(Type of Performance Test)

Ongoing 365 Days per Year; 24 Hours per Day
(Performance Test Date and Time)

Detection of Contraband and Prohibited Items, John Doe
(Safety Plan Name and Person Preparing)

ALL LIMITED SCOPE PERFORMANCE TESTS (LSPT'S) WILL BE CONDUCTED IN CONFORMANCE WITH THIS SAFETY PLAN AND ONLY AFTER SPECIFIC APPROVAL TO CONDUCT THE LSPT'S HAS BEEN GRANTED BY A RESPONSIBLE U.S. DEPARTMENT OF ENERGY OFFICIAL. PERSONNEL SERVING AS CONTROLLERS WILL BE FULLY QUALIFIED IN ALL ASPECTS OF THE LSPT.

Scenario:

The ongoing LSPTs are conducted to test the ability of Protective Force (PF) personnel to detect and prevent contraband and prohibited items from being introduced into Limited Areas, Exclusion Areas, Protected Areas, and Material Access Areas. LSPTs will be conducted on X-ray machines, metal detectors, and hand and vehicle searches. Security and non-security personnel will try to enter and exit the above-mentioned areas with contraband and prohibited items. Using personnel with whom PF personnel are unfamiliar will ensure credible and realistic test results. The person attempting to introduce the contraband or prohibited item will use only contraband test items that have been approved by the DOE cognizant security office. Once the entry is initiated, the person attempting the entry will only proceed after being cleared to do so by the security officer conducting the search. The persons attempting the entry will wear clothing that would make the concealment of any weapons on their person virtually impossible, and they will keep their hands open and in plain view at all times. The persons attempting to enter or exit any of the aforementioned areas will strictly follow all instructions given by the DOE controller and obey all instructions given by PF personnel. The DOE controller will announce the LSPT

to PF personnel once the contraband or prohibited item has been detected/undetected by the PF. *The sole purpose of the LSPTs is to evaluate the ability of the PF to detect contraband and prohibited items prior to their release into the aforementioned areas. The LSPTs are not designed to test what actions the PF undertakes once they detect or fail to detect the contraband or prohibited item.*
IN THE EVENT OF AN ACTUAL SECURITY ALARM OR SECURITY INCIDENT, THE CONTROLLER WILL IMMEDIATELY ANNOUNCE AND CONCLUDE THE LSPT, TAKE POSSESSION OF THE TEST ITEM/CONTAINER, AND FOLLOW ALL INSTRUCTIONS ISSUED BY PF PERSONNEL.

Requirements:

1. DOE Controller
2. Person to carry contraband or prohibited item into the area
3. Contraband and prohibited item(s)
4. Support items, such as lunch boxes, purses, notebooks, gym bags, vehicles.

PF Response:

_____ Yes _____ No

If a no-notice PF response is desired, check the following measures being taken to ensure safety during the response.

____ Drill announcements will be made on all PF networks immediately after PF response is initiated, and periodically thereafter.

_X_ Controller is located in the PF Central Alarm Station (CAS).

____ The PF is informed that an exercise will take place and that they are to follow the safety and health requirements contained in this plan and in the site procedures. This instruction will be provided by site representatives briefing the PF prior to the shift during which the performance test will take place.

_X_ Controllers are located at the exercise location.

If PF response is not desired, check those measures being taken to preclude response.

____ Prior notification of CAS.

____ Prior notification of PF.

____ Presence of non-playing PF personnel briefed on the scenario at the performance test location.

_X_ Controller located in the CAS. **A second controller will be located in the CAS with a final approved copy of this LSPT Safety Plan and LSPT Safety Briefing. This controller will be able to provide positive identification of the onsite controller and any support personnel participating in the LSPT. The onsite controller will ensure that the CAS controller is physically located in the CAS prior to departure for the area in which the LSPT will be conducted.**

_X_ Controller located in the immediate vicinity (within sight and hearing of the PF and support personnel) of the LSPT.

List other specific safety measures below:

1. All personnel attempting to gain entrance into one of the identified areas will be briefed on the LSPT objectives and how they should conduct themselves during the LSPT.
2. All contraband or prohibited items will be photographed prior to the initiation of the LSPT.
3. All personnel attempting to gain entry or exit with contraband items will be photographed prior to the initiation of the LSPT.
4. All personnel attempting to gain entry or exit with contraband or prohibited items will be instructed to keep their hands in plain view, not to make any sudden moves, and comply with all instructions given by PF personnel.
5. Only epoxy–encased, DOE cognizant security office-approved test weapons will be used in LSPTs requiring weapons.
6. All support personnel attempting to gain entrance or exit with contraband or prohibited items will be briefed and required to read and sign the attached rules of exercise.

Performance Test Boundaries:

_X_ Applicable

The immediate area of the security post where the LSPT is being conducted.

_X_ Not applicable

If applicable, describe the performance tests boundaries and the restrictions on performance test participant movements in detail:

Off-Limit Areas:

____ Applicable

_X_ Not applicable

If applicable, describe the off-limit areas and how they will be designated:

Safety Equipment:

____ Controller Radios

____ PF Radios

____ Orange Vests

____ “Glow Sticks”

____ First Aid Kit

____ Other required safety equipment:

Specific Safety Hazards Not Covered Elsewhere:

____ Applicable

_X_ Not applicable

These LSPTs are being conducted with armed PF personnel. As with all such exercises, the remote possibility exists that weapons may be drawn if the exercise plan is not adhered to, or if PF personnel are not properly trained. However, because of the constraints placed upon the exercise controllers by this plan and the level of preparation of the DOE participants, the level of risk is actually below that experienced during normal day-to-day operations.

Radiation Safety Provisions:

____ Applicable

_X_ Not applicable

If yes, check those applicable to this LSPT:

____ Personnel participating in the LSPT have been briefed concerning radiation safety requirements for the area with which the LSPT will be conducted.

____ Personnel will be continuously escorted while in the radiation areas in which the LSPT will be conducted.

List any other specific radiation safety provisions for this LSPT:

Personnel Assignments (list below):

The names of the DOE controller and the person carrying the contraband or prohibited items will be filled in prior to conducting the LSPT.

Protective Force Appendix Required:

____ Yes

_X_ No

DOE Safety Review:

List any pertinent safety procedures concerning this LSPT that are not addressed in this plan.

Normally, the PF will not be notified in advance of the specifics of the LSPT being conducted. The shift captain will be notified upon termination of the LSPT.

APPROVALS:

_____ Date _____
Director, Safety and Health Organization
DOE Cognizant Security Office

_____ Date _____
Contractor Safety and Health Representative

_____ Date _____
Director, Security Organization
DOE Cognizant Security Office

3.4 Sample Performance Test Plan

PERFORMANCE TEST PLAN

TEST OBJECTIVE

This performance test is designed to

1. Test individual employee response to finding an unattended Secret Restricted Data (SRD) document
2. Verify compliance with the notification process to Classified Document Control Office (CDCO)
3. Verify PF compliance with the procedure for responding to this incident.

SCENARIO DESCRIPTION

A simulated SRD document will be left unattended in an area accessed by "L"-cleared employees. This document will be marked as a formal SRD document. Personnel recovering and responding to the simulated classified document shall have no indication that the contents of the document are actually unclassified.

TEST METHODOLOGY AND EVALUATION CRITERIA

1. A simulated SRD document consisting of approximately five pages of unclassified text and drawings shall be placed on the table next to a copy machine located in Building xxx, Room zzz. The document shall be placed in the designated location at approximately 7:30 am.

2. Upon notification of the unattended "classified" document, the CDCO will verify that the individual finding the document completed the following actions:

   a) Xxxx
   b) Xxxx
   c) Xxxx

The Document Control Center shall also verify that the PF completed the following actions:

   a) Xxx
   b) Xxx
   c) Xxx

Pass/Fail Criteria

In order to successfully complete the performance test, the following must occur:

- Classified Document Control Office is notified within three hours of placement.
- Individual locating the unattended document adheres to all protection and notification requirements.
- PF officer responding to the incident adheres to all protection and notification requirements.

TEST CONTROLS

The following controls will be adhered to during conduct of this performance test.

- Only survey team members involved with the conduct and evaluation of this performance test will be made aware of all information surrounding the conduct of the test.

- There are no additional safety requirements for this performance test. All current facility safety requirements will be adhered to during this performance test.

- This will be a no-notice exercise; therefore, the surveyed organization will not be given any information regarding the conduct of this performance test prior to the test.

- The simulated SRD document used during this exercise will consist of an unclassified document marked at the SRD level with all appropriate markings and covers. There will be no indications to a casual observer that the document is not classified.

RESOURCE REQUIREMENTS

The following resources are needed to conduct this performance test.

- Simulated SRD document

- Identified location to place the document

- Three survey team members to be assigned the following:
  a) Monitor the document
  b) Monitor the PF response
  c) Monitor the CDCO

TEST COORDINATION REQUIREMENTS

No coordination requirements are necessary since this is a no-notice exercise. Survey team members monitoring the various aspects of the performance test will identify themselves to participants only when it becomes necessary.

OPERATIONAL IMPACT(S) OF TESTING PROGRAM

Since this performance test is being conducted during normal duty hours, there will be no need for additional funds for overtime payments, and there is no expectation of a loss of productive time for personnel who will be participating in the exercise.

COMPENSATORY MEASURES

There are no compensatory measures required for the conduct of this exercise.

COORDINATION AND APPROVAL PROCESS

The following steps and documentation will be followed in the conduct of this exercise.

- This test plan will be approved by the survey team leader prior to the conduct of the performance test. Approval of this test plan will be documented by the Survey Team Leader’s signature and date on this test plan.

- A participant log containing name, job title, organization, telephone number, and date will be completed by all participants of this exercise.

- A data collection form containing the date, performance test type, name of evaluator, and chronological description of actions observed will be completed by all survey team members participating in the evaluation of this performance test.

REFERENCES

The following references will be used in the conduct and evaluation of this performance test.

- DOE O XXX.X, *Information Security*
- Information Security Standard Operating Procedure #
- PF Standard Operating Procedure #
- PF Post Order #

SURVEY TEAM LEADER: _____
DATE: _____

(Signature of Approval)

4.0 TOPICAL AREA TOOLS

This section contains items that can be used to assist team members in conducting surveys and self-assessments by providing a series of guidelines, including:
(1) subtopical areas,
(2) areas of consideration
(3) sample documents list,
(4) sample interview candidates,
(5) suggested interview questions.

A. PROGRAM MANAGEMENT OPERATIONS

Subtopical Areas to Program Management Operations

A.1 PROTECTION PROGRAM MANAGEMENT
- Program Management and Administration
- Resources and Budgeting
- Personnel Development and Training

A.2 SAFEGUARDS AND SECURITY (S&S) PLANNING AND PROCEDURES

A.3 MANAGEMENT CONTROL
- Surveys and Self-Assessment Programs
- Performance Assurance Program
- Resolution of Findings
- Incident Reporting and Management

A.4 PROGRAM-WIDE SUPPORT
- Facility Approval and Registration of Activities
- Foreign Ownership, Control, or Influence (FOCI)
- Security Management in Contracting

Areas of Consideration

The topical area team should research answers to the following types of questions during the course of document reviews. Answers to questions such as these may help to focus and streamline survey activities.

Is the organization adequately staffed to accomplish its mission?
- Are there any vacant positions? If so, how long have they been vacant?
- Do personnel perform the duties stated in their job descriptions?
- Are job descriptions current and reviewed periodically?
- Are personnel adequately trained to perform their assigned duties?
- Is there a formal training program in place?
- Are training programs based on the results of job task analysis?
- Has funding been allocated for training?
- Who maintains the organizations training records?
- Has there been an analysis of the job skills needed to fulfill each assigned responsibility? Has this been documented in individual job descriptions?
- Is succession planning considered when training staff?

Has management established an effective and efficient organization structure?
- Is the organization structure documented in writing?
- Are there indications of frequent change in the organizational structure?
- Have responsibilities been explicitly assigned to individuals?
- Are lines of communication, accountability, and authority clear?

Is there a formal, coordinated effort regarding the development, approval, and updates associated with facility/site security plans?
- Do security plans reflect security operations actually occurring at a facility?
- Is there a process in place to ensure S&S plans are reviewed and updated in a timely manner when changes to operating conditions occur?
- Is expertise available to provide a meaningful review of security plans and procedures?
- Are security plans supported by sufficient analysis to establish that protection requirements will be met?

- Is documentation available for vulnerability assessments (VAs) and/or other tests and analysis used to establish the requirements for specific security measures and equipment?
- Are there any equivalencies or exemptions from DOE requirements in place at the facility? Are there any deviations from national requirements?
- What methodologies are used for site VAs?
- Are these methodologies adequate to evaluate the site's vulnerabilities in light of the operational environment?

How is the contractor performing and what criteria are used to evaluate performance?

- Who has input into the award fee process?
- How is the criteria "weighted" and by whom?
- Are there areas requiring improvement? If so, what are they?
- What were the ratings given during past surveys and self-assessments?
- Is there a trend?
- Have all areas been reviewed?

Is there a corrective action tracking system in place? If so, does it cover the entire site/facility?

- Does this tracking system for findings include all periodic surveys, self-assessments, Technical Surveillance Countermeasures (TSCM) services, and DOE review findings?
- Are the milestones for completing the corrective actions reviewed on a recurring basis?
- What types of cause analyses are completed on corrective action plans?
- Is staff trained to conduct root cause analyses? If so, who provides training?

Are there any inquiries currently open?

- Have any staff members conducted inquiries into incidents of S&S concern? Were these individuals appointed in writing?
- Have any inquiries established any possible crimes or fraud, waste, and abuse?
- Have there been any formal inquiry reports developed?
- Was it determined that any damage assessments were required?
- If a damage assessment(s) was conducted, who appointed the damage assessment team(s) and approved the damage assessment report(s)?
- How many incidents of S&S concern have occurred since the last survey?
- Of those incidents, how many were known compromises and how many were potential compromises?

Have all applicable security requirements been incorporated into the contract?

- What is the process for incorporating new directives into the site contract?
- How are new directives incorporated into daily implementation for site-related DOE organizations?
- Has the incorporation of any directives been unduly delayed?
- Are all equivalencies and exemptions correctly characterized?

Are there any Strategic Partnership Projects being performed at the facility?

A.1 PROTECTION PROGRAM MANAGEMENT

Subtopical Areas to Protection Program Management

Program Management and Administration
Resources and Budgeting
Personnel Development and Training

Sample Document List:

Document review in this area is key to understanding how the S&S organization functions. The following types of documents should be carefully reviewed and validated:

- Organization diagrams depicting the management structure
- Functions, Responsibilities and Authorities Manual, Safeguards and Security Management Plan, delegations of authority, and/or other documents depicting assigned roles, responsibilities, and authorities
- Position descriptions for S&S management positions
- Operating instructions for the implementation of S&S programs
- Supplemental documents and plans implementing S&S programs
- Training records for personnel with S&S responsibilities
- Contract documentation (which directives are applicable to the organization being surveyed)
- Budget documentation
- Training plans and procedures
- Overall training process and training record system (is there one program?)
- Certification records for specialized jobs (material control and accountability [MC&A] measurements, armorers, locksmiths, etc.)
- Documentation of VAs and related tools used in preparation of the facility/site security plan, i.e., ASSESS/ATLAS, JCATS, etc.
- Copies of active equivalencies and exemptions
- Survey and self-assessment reports for the last two years

The existence of other documents, which further delineate the management of the S&S program, may be derived from the review of these initial documents.

Documents should be used as the basis for determining whether management supports the S&S program in a manner that demonstrates both compliance with the requirements and a commitment to performance that assures the adequate protection of national security assets.

Sample Interview Candidates:

Interview candidates may include:

- DOE Operations/Field/Area Office Manager
- DOE Assistant Manager or Director responsible for S&S
- Individual DOE S&S Operational Program Managers
- DOE and contractor management assigned responsibility for developing and implementing this element of the S&S program
- Contracts and Procurement Department management
- Budget and/or Finance Department management
- Human Resources Department management
- Security managers assigned responsibility for developing and implementing the S&S

programs
- Property management
- Emergency management
- Training management
- Contractor Program Managers/Coordinators responsible for S&S training activities (including protective force)

Sample Interview Questions:

Suggested questions to be asked during the interview process may include the following:

- Have resources been prioritized based on impact to mission? Have budgets been allocated in accordance with this prioritization?
- Has management established an effective and efficient organizational structure?
- Is a system in place to ensure integration is occurring at the necessary levels to establish and maintain an effective overall S&S program?
- How have performance measures been communicated?
- Does the program lack visibility or support at any level?
- Is the organization aligned to ensure proper communication and integration? Does this alignment minimize fragmentation of the program?
- Are staffing levels adequate to support the organization structure and to fulfill functional requirements?
- Have responsibilities been explicitly assigned to individuals?
- Are all the positions filled? If not, how long have they been open?
- Are personnel qualified and trained for their positions?
- Are major tasks and skill requirements documented in individual job descriptions?
- Are personnel qualified to perform their oversight responsibilities?
- Is there a formal training program in place? Do all training programs meet established standards?
- Has a formal training process been developed to ensure all personnel who need the training receive the training?
- Are training methodologies and courses standardized and tailored to specific duties and responsibilities?
- Are training programs based on the results of job task analysis?
- Has funding been allocated for training, equipment, and supplies?
- Who maintains the organizations training records?
- Is performance-based testing used?

A.2 SAFEGUARDS AND SECURITY PLANNING AND PROCEDURES

Subtopical Areas to Safeguards and Security (S&S) Planning and Procedures

None

Sample Document List:

The following are representative of the documents that should be reviewed:

- Facility/Site Security Plan and, where several facilities have been consolidated into a site, any subordinate facility plans which have not been consolidated into or replaced by the site security plan
- Approved or pending equivalencies and exemptions with supporting documentation
- Safeguards and Security Information Management System (SSIMS) reports
- Emergency plans
- Contingency plans
- Local procedures
- Material Control and Accountability plans
- S&S training plan
- Survey and inspection reports
- Update projects and current compensatory measures
- Data from evidence files
- Current compensatory measures

The survey team should be thoroughly familiar with the purpose of each document reviewed. The requirement for the document should be compared with the finished product, and an assessment made of the adequacy of the document in complying with the requirement.

Sample Interview Candidates:

Interview candidates may include:

- DOE Operations/Field/Area Office Manager
- DOE Assistant Manager or Director responsible for S&S
- DOE Division Director(s) responsible for S&S-related activities and plans
- Individual DOE S&S Program Managers
- Contractor Senior Management with line responsibility for S&S activities and plans
- Contractor S&S Director
- Contractor Program Managers responsible for S&S SP/Vulnerability Assessment (VA) data
- Personnel responsible for developing the various S&S plans
- Protective Force managers

Sample Interview Questions:

Suggested questions to be asked during the interview process may include the following:

- How does the facility determine the contents of the security plan?
- Is there a local procedure for developing the facility/site security plan?
- What is the protection strategy used at this facility?
- Is the Graded Security Protection Policy (GSP) used for addressing threats? If not, is this approved in writing? What basis is used if the GSP is not applicable?
- What equivalencies/exemptions are in place? When were they approved and by whom? Have they been entered in SSIMS and documented in the facility/site security plan?
- How do equivalencies/exemptions impact protection strategy?
- Are any S&S plans currently being updated? If so, why?

- What process is used for reviewing, approving, and/or updating major S&S plans? Is this process documented?
- Is expertise available to provide a meaningful review of S&S plans and procedures?
- How is integration of major S&S plans ensured?
- Who is responsible for maintaining the analytical data and details of assessment activities supporting the security plan?
- Are VA documents and validation results from performance tests reviewed during the update process or are data obtained from new sources?
- How are changes in policy and/or procedures communicated to those with implementing responsibilities?
- How has management effectively established program direction?
- What is the process used for procedure development/update/approvals?
- How are inspection/survey results used by management to evaluate the effectiveness and viability of S&S plans?

A.3 MANAGEMENT CONTROL

Subtopical Areas to Management Control

Surveys and Self-Assessment Programs
Performance Assurance Program
Resolution of Findings
Incident Reporting and Management

Sample Document List:

Documentation to be reviewed may include the following:

- Survey and self-assessment program plans and schedules
- Incidents of Security Concern (IOSC) plans and implementing procedures
- Survey and self-assessment reports
- Corrective action plans and tracking systems (information derived from)
- Site specific survey/self-assessment guides and procedures
- IOSC inquiry reports and status reports
- IOSC trending and analysis
- IOSC corrective action plan packages
- Inquiry Official appointment letters
- Damage assessments
- Vulnerability Assessment (VA) test data
- List of open/closed finding for past three to five years (review for recurring findings)
- Copy of the approved Performance Assurance Program Plan
- List of essential elements documented in the Performance Assurance Program and the testing schedule for each
- Performance assurance test procedures
- Performance assurance test reports and subsequent correction actions

Sample Interview Candidates:

Interview candidates may include:

- DOE management
- Safeguards and Security (S&S) Division Directors, if appropriate
- DOE Division Director(s)
- Individual DOE S&S Program Managers
- Contractor S&S Director
- Contractor Program Managers
- Personnel responsible for VA testing and security plan development
- Protective Force Managers
- IOSC Inquiry Officials

Sample Interview Questions:

Suggested questions to be asked during the interview process may include the following:

- Are survey and self-assessment programs in place to determine the effectiveness of the S&S program? Are procedures applicable to the programs documented in the facility/site security plan?
- When was the last self-assessment conducted? Did it include all applicable topical and subtopical elements? Was a formal report prepared and submitted?
- Are corrective actions identified in surveys and self-assessments implemented in a timely and effective manner?
- What ratings were given in previous surveys/self-assessments?

- Have recent survey or self-assessment activities resulted in any repeat findings?
- What is the status of open findings? What is the status of the associated corrective action plans?
- What method of cause analysis is used? What training has staff received?
- Are the results of surveys and self-assessments factored into performance measures or award fees?
- For self-assessments, is there a system in place for tracking findings and corrective actions? If so, does it cover the entire site/facility?
- Are survey findings entered in SSIMS?
- Are the milestones for completing the corrective actions reviewed on a recurring basis?
- Have staff members conducted inquiries into incidents of security concern? Were these individuals appointed in writing?
- What kind of trending and analysis is performed on IOSCs? How are the results disseminated to management & staff?
- What kind of IOSC awareness is provided?
- Are incidents involving individuals applying for or holding a security clearance reported to the appropriate personnel security office?
- How are corrective action plans coordinated with management?
- Have any inquiries established any possible crimes or fraud, waste, and abuse?
- Are there inquiries currently open?
- Have there been any formal inquiry reports developed?
- Was it determined that any damage assessments were required?
- If a damage assessment(s) was conducted, who appointed the damage assessment team(s) and approved the damage assessment report(s)?
- Have any incidents of security concern occurred since the last survey? If so, how many? Were the incidents appropriately categorized and reported?
- Were the appropriate notifications made for each incident?
- Does the facility IOSC program plan specify Management Interest (MI) incidents and identify them by category?
- Does the facility maintain a central record of all inquiries into incidents of security concern and damage assessments? If not, in what manner are those records being maintained that facilitates their retrieval and use within the facility (e.g., for tracking and oversight purposes)?
- How long are records maintained?
- What training do staff receive prior to conducting inquiries?
- Is there a formal process for implementing a performance assurance program?
- How often is testing conducted? Are both operability tests and effectiveness tests included?
- Who reviews and approves the Performance Assurance Program Plan? Does the plan identify the essential elements relevant to the site and describe how they were determined?
- Who determines what tests will be conducted and the criteria for evaluation? What is the basis for this determination?
- How are the results of tests documented and analyzed? Are issues requiring corrective action documented and tracked until resolved?
- Are appropriate compensatory measures taken immediately when unsatisfactory test results indicate that national security or health and safety are jeopardized?
- Are performance assurance plans reviewed and updated appropriately?

A.4 PROGRAM-WIDE SUPPORT

Subtopical Areas to Program-Wide Support

Facility Approval and Registration of Activities
Foreign Ownership, Control, or Influence (FOCI)
Security Management in Contracting

Sample Document List:

Documentation to be reviewed may include the following:

- Current contract(s) including statement of work, DOE directives incorporated into the contract (including those pending), and security clauses
- List of all subcontractors and consultants conducting work for the contractor being surveyed (list of all contractors/subcontractors registered)
- Approved facility/site security plan (SP)
- Facility data sheets
- Copy of current award fee criteria and award fee documentation (including performance measurement data) for the last two years
- Most recent FOCI determination, including copies of any applicable FOCI mitigation instruments and National Interest Determinations (NID)
- Approved Contract Security Classification Specification (CSCS) F 470.1
- Signed Facility Data and Approval Record (FDAR) F 470.2
- Equivalencies/exemptions to DOE directives (pending and approved)
- Master facility registration, in the Safeguards and Security Information Management System, and local facility registration listings (if used)
- Previous survey and inspection reports and self-assessments
- List of cleared personnel, including access authorization number and date of latest background investigation, by contract (including all contractors that have cleared employees conducting work at the facility). This list can come from the DOE Central Personnel Clearance Index (CPCI) of access authorizations held by the contractor. The CPCI and contractor lists, including the list of current key management personnel (KMP), should be compared for discrepancies.
- Internal procedures (facility clearance, FOCI)
- Applicable Memoranda of Understanding/Agreement (e.g., MOA documenting responsibilities of DOE and a cognizant other government agency (OGA) for reciprocity of a specific FCL)
- Most recent SF 328, Certificate Pertaining to Foreign Interests
- Most recent list of KMP
- A list of all employees of the company possessing or in the process of obtaining DOE access authorizations who are Representatives of Foreign Interests (RFIs)
- A list identifying any Strategic Partnership Projects (formerly called Work for Others) conducting work at the facility
- A copy of the contractor's records of all contracts and subcontracts involving access authorizations
- A copy of the contractor's procedures for reporting events that have an impact on the status of the facility clearance, and copies of reports filed since the last survey or self-assessment.
- Company visitors log
- Loan or credit agreements (if applicable) to determine if any power has been granted the lender. For each identified loan or credit agreement, obtain the names, country location, and participation amount of each of the lenders involved, as well as the aggregate amount

of the loan or credit agreement.

- Board of Director's meetings minutes to determine if any actions taken by the Board resulted, or will result, in changes that should be reported to DOE
- Copies of all Schedules 13D and 13G submitted to the Securities and Exchange Commission (SEC), if publicly traded
- Annual report and/or financial statement of the company
- Shareholders' agreements to determine if amount of stock is sufficient to elect representation to the Board or an agreement exists whereby the shareholder(s) is permitted representation on the Board, currently or at a future date
- Proxy statements (Notice of Annual Meeting of Stockholders) to determine (1) current beneficial owners of 5% or more of the company's securities; (2) changes to the company's directors; and (3) changes in location of its principal executive offices, state of incorporation, or the company's business, management, proposed mergers
- Annual report and SEC Form 10-K Report to determine (1) changes in revenue/income derived from foreign interests; (2) loan or credit agreements entered into with foreign lenders or in which foreign lenders are participants; and (3) joint ventures/contracts with foreign interests
- Internal Revenue Service Form 5471, Information Return of U.S. Persons with Respect to Certain Foreign Corporations to determine whether all foreign holdings were reported
- Articles of Incorporation and By-Laws or Partnership Agreement to determine if any changes have been made to the company's/partnership's business, management.

NOTE: The following reflects which of the above-mentioned documents apply to the different types of business entities:

- Sole proprietor, divisions of a legal entity, or self-employed consultant – none of the above documents would apply, except negative covenants in loan or credit agreements
- Publicly traded – all of the above documents
- Privately owned – under normal circumstances, none of the documents would be required. However, if the company has issued bonds or debentures, it is required to file a Form 10-K Report with the SEC.

Sample Interview Candidates:

Interview candidates may include the following:

- DOE Safeguards and Security (S&S) Division Director, if appropriate
- DOE and Contractor Contracts and Procurement Managers
- DOE S&S Program Managers
- Contractor S&S Director
- Contractor S&S Program Managers
- Facility Security Officer (FSO)
- Facility Procurement and Contracting Officer – Point-of-contact for records of all contracts and subcontracts
- Corporate Secretary – Point-of-contact for the organization's owners; any changes that may have occurred in the company's business, management, or ownership of subsidiary/parent (i.e., the creation of an intermediate parent); and information on whether the company has acquired ownership in foreign corporations
- Chief Financial Officer or Treasurer – Point-of-contact for information on revenue/income derived from foreign interests, and loan or credit agreements entered into with foreign lenders

Sample Interview Questions:

Suggested questions to be asked during the interview process may include the following:

- Have all applicable DOE directives been incorporated into contracts as appropriate? Are there any pending incorporation?
- Have all applicable security clauses been incorporated into contracts as appropriate? What is the process for ensuring contracting officers are made aware of security considerations?
- How are contracting officers informed of the security requirements to be included in a contract?
- Who has input into the award fee process?
- How are the award criteria 'weighted' and by whom?
- Are facility clearance and FOCI procedures documented in the facility/site security plan?
- Are facility clearances granted prior to allowing DOE S&S interests on the premises of the facility? Have all the DEAR requirements for approval of a facility clearance [48 CFR 952.204-73(c)] been met?
- Have the contractor and subcontractors been given favorable FOCI determinations? Are any of them under FOCI mitigation?
- Does the facility have an approved security plan?
- Is the FSO's access authorization equivalent with the facility clearance?
- Has an FDAR been completed and approved?
- Has a CSCS form been completed for all activities?
- Has a FOCI determination been made on all contractors and subcontractors that require access authorizations?
- Do the contractor and subcontractor provide notifications of any changes that may affect the FOCI determination?
- Do the key management personnel have appropriate access authorizations? If not, have appropriate exclusion actions been taken?
- Have there been any changes in information reportable under any question on the SF 328? If so, were the changes reported as required?
- Has there been a change in a previously reported foreign ownership threshold or factor that was previously favorably adjudicated?
- Have there been any changes in ownership or control, including stock transfers that affect control of the company?
- Did the location of the company's principal executive offices change?
- Have the Articles of Incorporation and By-Laws or Partnership Agreement changed?
- Have anticipated changes and other reportable changes (e.g., changes to KMP information) been identified and reported as required?
- Have Strategic Partnership Projects (Work for Others) been registered in SSIMS?
- Has information concerning classification and protection information been exchanged for all Strategic Partnership Projects between the DOE activity and the requesting agency? Are the exchanges documented?

B. PROTECTIVE FORCE

Subtopical Areas to Protective Force

B.1 MANAGEMENT
B.2 TRAINING
B.3 DUTIES
B.4 FACILITIES AND EQUIPMENT

Areas of Consideration

The topical area team should research answers to the following types of questions during the course of document reviews. Answers to questions such as these may help to focus and streamline survey activities.

How are all aspects of the protection program adequately integrated to ensure effective protection?

- How does the overall protection system operate to accomplish its routine and emergency tasks?
- What protection strategy is used?

Does documentation accurately reflect current conditions and configurations of the facility?

- Does the facility/site security plan accurately describe security operations at the location?
- Does the security plan accurately reflect current site assets and security interests and describe how the protection program is managed?
- Are equivalencies/exemptions in place at the facility? Are they approved and entered in SSIMS? Have they been incorporated into site procedures?

What are the assets of the site/facility?

- Where are they located?
- What is the importance level?
- Are all assets identified in the facility/site security plan?
- Are the assets readily identifiable by the PF?

Is there an approved acceptance and validation testing program in place that encompasses security-related components and subsystems?

- How is it implemented?
- Are compensatory measures implemented immediately when any part of the critical system is out of service?
- How are Security Police Officers notified in case of system failure?

Are protection strategies for the protection of special nuclear material (where applicable) and vital equipment adequately addressed in site planning documents?

- Has a performance assurance program been fully implemented at the facility?
- Are recapture, recovery, and pursuit strategies documented?
- Are programs designed to mitigate the consequences of radiological/toxicological sabotage in place?

B.1 MANAGEMENT

Subtopical Areas to Management

None

Sample Document List:

Documentation to be reviewed may include:

- Facility/Site Security Plan (SP)
- Approved or pending equivalencies and exemptions
- Staffing plans
- Budget documents
- Overtime allocations
- Vulnerability Assessment (VA) data
- Human Reliability Program (HRP) criteria and list of staff assigned to HRP positions
- Response plans
- Recent findings and associated corrective action plans
- General, Post, and Special orders

Sample Interview Candidates:

Interview candidates may include the following:

- Protective Force (PF) Manager
- DOE Safeguards and Security (S&S) Director
- PF Training Coordinator
- Individuals responsible for the VA data
- Special Response Team Lead

Sample Interview Questions:

Suggested questions to be asked during the interview process may include the following:

- How much of the staffing budget is allocated to overtime?
- How does interface/integration with other S&S organizations occur?
- Is the data contained in the security plan/VA an accurate reflection of site operations?
- What could be changed that would improve the overall protection strategy?
- How could technology be used to improve the security posture?
- What is the current PF strength? Armed and unarmed?
- What memoranda of understanding/agreement are currently in place? Are others in process?
- What is the supervision ratio? Is it adequate?
- What is the process for selection of supervisors? What qualifications are necessary?
- What is the process for developing, updated, and maintaining procedures?
- How are changes in procedures communicated?
- How many PF personnel are in the HRP?
- What are the criteria for participation in HRP?

B.2 TRAINING

Subtopical Areas to Training

None

Sample Document List:

Documentation to be reviewed may include:

- Annual Protective Force (PF) Training Plan
- Staffing plans
- Job Task Analyses (JTAs)
- Overtime allocations
- Training records (including a list of PF personnel who are subject to weapons qualification within 90 days of the start date of the survey and a list of PF personnel who are medically certified to participate in the physical fitness program
- Training materials (rosters, curriculum, tests)
- Site-specific risk analysis for lesson plans
- List of PF instructors and their certifications
- List of Special Response Team instructors and their certifications
- List of firearm instructors and their certifications
- List of standard equipment issuance
- General, Post and Special orders
- Description of training records system in use
- Recent findings and associated corrective action plans (including documented root cause) relevant to this topic

Sample Interview Candidates:

Interview candidates may include:

- PF Manager
- DOE Safeguards and Security Director
- PF Training Coordinator
- Individuals responsible for Vulnerability Assessment data
- Instructors

Sample Interview Questions:

Suggested questions to be asked during the interview process may include the following:

- How many personnel have failed to pass fitness qualifications during the survey period?
- How many personnel have failed their firearms qualifications during the survey period?
- What type of remedial training is required for failing?
- How many instructors have been certified through the National Training Center?
- What types of training facilities are used?
- Have JTAs been completed for all identified positions? Have all essential components been included?
- What are the strengths and weaknesses of the training program?
- Are JTAs site-specific?

B.3 DUTIES

Subtopical Areas to Duties

None

Sample Document List:

Documentation to be reviewed may include the following:

- Facility/Site Security Plan (SP)
- Approved Job Task Analyses
- Staffing plans
- Overtime allocations
- List of standard equipment issued
- Protective Force schedules and post assignments
- Memoranda of understanding/agreement affecting duties/response
- General, Post, and Special orders
- Shipment security plans and procedures
- Emergency response plans
- List of critical targets
- Special Response Team (SRT) rosters
- Security Incident Response Plan
- Recent findings and associated corrective action plans relevant to this topic
- Security lock and key control procedures

Sample Interview Candidates:

Interview candidates may include the following:

- PF Manager
- DOE Safeguards and Security (S&S) Director
- PF Training Coordinator
- Individuals responsible for Vulnerability Assessment data
- PF Operations Manager
- SRT personnel
- Security Officers, Security Police Officers
- Facility's designated responders (as described in the Emergency Response Plan)
- Emergency Operations Center (EOC) personnel responsible for response and recovery
- Warehouse personnel (shipment preparations)

Sample Interview Questions:

Suggested questions to be asked during the interview process may include the following:

- How are compensatory measures determined? Relayed to PF?
- What are the critical targets associated with this facility? How are they recognized?
- How are communication channels determined to be effective (both internal to the PF organization and external to its counterparts)?
- What role does the EOC play during shipments?
- When was the last Force-on-Force exercise conducted?
- How are changes in operations (e.g., material movements, compensatory measures, increase threat levels) communicated?
- How are changes to policies and procedures transmitted? Who is responsible for ensuring Post Orders are approved and current?
- How are security locks and keys controlled within the PF?
- What are the critical targets at this facility? What training is provided relative to the

identification of critical targets? Who has received this training and what are the criteria?

B.4 FACILITIES AND EQUIPMENT

Subtopical Areas to Facilities and Equipment

None

Sample Document List:

Documentation to be reviewed may include the following:

- Facility/Site Security Plan (SP)
- Equivalencies and exemptions
- Staffing plans
- Budget documents
- Overtime allocations
- List of standard equipment issued and instructions for use
- Protective Force (PF) schedules and post assignments
- Memoranda of understanding/agreement affecting duties/response
- General, Post and, Special orders
- PF weapons and ammunition inventories
- Equipment maintenance logs (including weapons)
- Recent findings and associated corrective action plans relevant to this topic
- Security Incident Response Plan

Sample Interview Candidates:

Interview candidates may include the following:

- PF Manager
- DOE Safeguards and Security Director
- PF Training Coordinator
- Individuals responsible for Vulnerability Assessment data
- PF Operations Manager
- Special Response Team (SRT) personnel
- Armorers

Sample Interview Questions:

Suggested questions to be asked during the interview process may include the following:

- What are the critical targets associated with this facility? How are they recognized? Where are they located?
- Are communication channels effective (both internal to the PF organization and external to its counterparts)?
- Is the PF equipped to meet its mission?
- Are training facilities adequate?
- Are modifications in equipment or facilities anticipated? If so, when and why?
- Has there been a change in mission that would affect the appropriateness of equipment used in the protection strategy at this facility?
- Are the vehicles used at this facility suitable and reliable to meet the mission?
- Have any issues associated with maintenance or functioning of equipment been identified? If so, has corrective action been taken?

C. PHYSICAL SECURITY

Subtopical Areas to Physical Security

C.1 ACCESS CONTROLS
C.2 INTRUSION DETECTION AND ASSESSMENT SYSTEMS
C.3 BARRIERS AND DELAY MECHANISMS
C.4 TESTING AND MAINTENANCE
C.5 COMMUNICATIONS

Areas of Consideration

The topical area team should research answers to the following types of questions during the course of document reviews. Answers to questions such as these may help to focus and streamline survey activities.

How are aspects of the protection program integrated to ensure effective protection?

- How does the overall protection system operate to accomplish its routine and emergency tasks?
- What protection strategy is used?

Does documentation accurately reflect current conditions and configurations of the facility?

- Does the facility/site security plan (SP) accurately describe operations at this facility?
- Does the facility/site security plan accurately reflect current site assets and security interests?
- Does the SP accurately describe current site physical protection elements and systems?
- Are equivalencies/exemptions in place at the facility? Are they supported by appropriate VA or risk assessment? Have they been appropriately approved, entered in SSIMS, and incorporated into the affected security plans?
- Does the site have an approved, current Response Plan for security emergencies?
- Does the site have an approved, current Compensatory Measures document?

What are the assets of the site/facility?

- Where are assets located?
- What is the impact of theft and/or diversion?
- Are all assets identified in the facility/site security plan?

Is an approved verification and validation testing program in place that encompasses security-related components and subsystems?

- How is it implemented?
- Are there documented procedures?
- Are compensatory measures implemented immediately when any part of the critical system is out of service?
- How are repairs initiated when a system element fails?
- Is the response to alarms and/or system failures documented?

Are protection strategies for the physical protection of special nuclear material, classified matter, and vital equipment adequately addressed in site planning documents?

- How are the Graded Security Protection (GSP) Policy, local threat guidance, and Vulnerability Assessment used in protection and control planning?
- Are recapture, recovery, and pursuit strategies documented?
- How are programs designed to mitigate the consequences of radiological/toxicological sabotage?

- Are there agreements with local agencies in place for assistance and/or notification ?

C.1 ACCESS CONTROLS

Subtopical Areas to Access Controls

None

Sample Document List:

Documentation to be reviewed may include:

- Lock and key records and procedures including storage, lock and key issuing, and custodian responsibilities
- Automated access control system records and procedures (including biometric access input as well as access credentials, issuance of keycards, tokens, etc.), System Administrator responsibilities, and performance testing and maintenance
- Property control and removal procedures, records, and issuance criteria
- Contraband searches during entry or exit
- Access control procedures, access lists/logs, and personnel training
- Visitor logs
- Performance testing plans and procedures, records of past performance tests
- Documents identifying security areas and S&S interests
- Termination/transfer procedures and notifications
- Building plans and protection area diagrams
- Comparison of Human Reliability Program (HRP) data with access control data
- Badge control procedures and automated system descriptions
- Date of last badge inventory and results (including issued, lost, recovered, destroyed)

Sample Interview Candidates:

Interview candidates may include the following:

- Security staff and management assigned responsibility for developing and implementing the Physical Security program
- Receptionist/employee controlling access to facility
- Access Control personnel
- Personnel assigned to monitor portals
- Personnel performing inspections of vehicles and hand-carried items
- Personnel responsible for key control and automated access control systems
- Locksmiths
- Property Management personnel
- Maintenance personnel

Sample Interview Questions:

Suggested questions to be asked during the interview process may include the following:

- What types of access control systems are used at the facility (e.g., receptionists, badge readers)?
- How are various functions notified of terminations and transfers?
- What policies are in place to ensure timely termination of access through retrieval of keys and access credentials upon termination or transfer?
- Have building lock-up procedures been established?
- How are records secured, maintained, and retrieved?
- Who performance-tests the systems, and how are the records kept?
- What happens in the event of an unsuccessful test or system failure?
- Are there well defined search system policies and calibration specifications for personnel and vehicle searches?

- Is there a documented process for ensuring access is terminated as appropriate (e.g., HRP status changes, clearances terminated, employees terminated)?
- How is the site badging system equipment secured after hours?
- Have auxiliary power sources been provided to all critical systems? What are the testing and maintenance procedures for ensuring auxiliary power is available?
- What type of temporary badge system is used at the facility?
- What types of records are maintained relative to badging?
- Are unused badges protected to prevent unauthorized use, theft, or loss?
- Do the site procedures address badge recovery after an employee's termination?
- Are lost badges being handled according to appropriate procedures?

C.2 INTRUSION DETECTION AND ASSESSMENT SYSTEMS

Subtopical Areas to Intrusion Detection and Assessment Systems

None

Sample Document List:

Documentation to be reviewed may include the following:

- Facility/site security plan
- Physical security system description(s) and location(s)
- Maintenance and testing records and procedures
- Alarm reports, including false and nuisance alarms
- Calibration and testing procedures and records
- Central Alarm Stations (CAS)/Secondary Alarm Station (SAS) procedures
- Emergency response for CAS/SAS recovery
- Emergency power systems (uninterruptible power supply system) certification and maintenance logs
- Compensatory procedures for equipment outages
- Limited scope performance test results
- IDS Analysis and Evaluation Report

During the course of document reviews, the survey team should try to validate that (1) physical security systems logs are maintained, (2) system tests are being performance-tested and documented as required, (3) system maintenance is being performed and documented as required, and (4) procedures are comprehensive.

Sample Interview Candidates:

Interview candidates may include the following:

- Safeguards and Security staff responsible for security systems
- Security Police Officers and Security Officers
- Engineers (involved with security systems)
- Alarms maintenance/installation and testing personnel
- CAS/SAS management
- CAS/SAS operators
- Protective Force Managers
- Emergency management planners
- User personnel responsible for walk-testing or other performance testing of alarm systems
- Maintenance personnel

Sample Interview Questions:

Suggested questions to be asked during the interview process may include the following:

- Are approved equivalencies/exemptions in place or pending? Have approved equivalencies/exemptions been entered in SSIMS and documented in the facility/site security plan? Have they been incorporated in site procedures?
- Are any line-item construction projects associated with physical security systems? If so, when were they last reviewed and who conducted the review?
- Is there a documented Testing and Maintenance Plan?
- How well is the physical security system program functioning?
- Is equipment calibrated according to documented specifications?
- Are response times consistent with those documented in security plans and Vulnerability Assessment?
- What areas of the system could be improved, and what steps have been taken toward the

improvements?

- Does the site have policies and procedures for the installation, alignment and calibration of intrusion detectors?
- Are there appropriate anti-tampering devices on primary and backup power sources for intrusion detection equipment?
- Are there a minimum of false or nuisance alarms that can be verified by documentation?
- Do the site systems have power backups, tamper protection devices, etc.?
- What strengths did the IDS analysis and evaluation identify? What weaknesses were identified? What was the cause and what corrective actions have been implemented?

C.3 BARRIERS AND DELAY MECHANISMS

Subtopical Areas to Barriers and Delay Mechanisms

None

Sample Document List:

Documentation to be reviewed may include the following:

- Facility/Site security plan and Vulnerability Assessment (VA) data
- Performance assurance test plans, procedures, and results
- Post Orders
- Critical target lists and locations
- Physical security system description(s) and location(s)
- Maintenance and testing records and procedures
- Alarm reports
- Calibration and testing procedures and records
- Central Alarm Station (CAS)/Secondary Alarm Station (SAS) procedures
- Emergency power systems (uninterruptible power supply system)
- Compensatory procedures for equipment outages
- Lock and key control procedures and inventory results

Sample Interview Candidates:

Interview candidates may include the following:

- Safeguards and Security staff responsible for security systems
- Security Police Officers and Security Officers
- Engineers (involved with security systems)
- Alarms maintenance/installation and testing personnel
- CAS/SAS Management/Operators
- VA staff
- Emergency management planners
- Lock and Key Administrator

Sample Interview Questions:

Suggested questions to be asked during the interview process may include the following:

- Are approved equivalencies/exemptions in place or pending?
- Are any line-item construction projects associated with physical barriers? If so, when were they last reviewed and who conducted the review?
- Is there a documented Testing and Maintenance Plan for barrier systems?
- How well are automated barrier systems functioning?
- Is equipment calibrated according to documented specifications?
- Are response times consistent with those documented in security plans and VAs?
- What areas of the system could be improved, and what steps have been taken toward the improvements?
- What technologies could be deployed at this facility to enhance the overall protection?
- How often are key inventories conducted? How are discrepancies resolved and what are the reporting requirements?
- Are the barriers at the site commensurate with the risk?
- Are the barriers designed to provide for adequate delay time to allow for appropriate response?
- Are the barriers at SNM areas, vaults, and MAA perimeters sufficient to ensure SNM cannot be removed?
- Do the security containers meet all required DOE and other standards?

C.4 TESTING AND MAINTENANCE

Subtopical Areas to Testing and Maintenance

None

Sample Document List:

Documentation to be reviewed may include the following:

- Performance assurance test plans, procedures and results
- Post Orders
- Physical security system description(s) and location(s)
- Maintenance and testing records and procedures
- False Alarm Rate (FAR)/Nuisance Alarm Rate (NAR)
- Calibration procedures and records
- Central Alarm Station (CAS)/Secondary Alarm Station (SAS) procedures
- Emergency power systems (uninterruptible power supply system)
- Compensatory procedures for equipment outages
- Inspection procedures

Sample Interview Candidates:

Interview candidates may include the following:

- Safeguards and Security staff responsible for security systems
- Security Police Officers and Security Officers
- Engineers (involved with security systems)
- Alarms maintenance/installation and testing personnel
- CAS/SAS Management
- CAS/SAS Operators
- Other personnel responsible for monitoring/clearing alarm indications
- Protective Force Managers
- Emergency management planners

Sample Interview Questions:

Suggested questions to be asked during the interview process may include the following:

- What is the process for implementing compensatory measures if a system fails?
- Is any trend analysis of maintenance requests being conducted for security equipment/systems?
- How is information coordinated between the organization responsible for testing and maintenance and the user organization?
- Is any testing and maintenance of security systems completed by vendors? If so, what mechanisms are in place to ensure appropriate access authorizations are held if required?
- Who performs the periodic testing (technicians, custodians, or security personnel)?
- How are the records maintained and/or retrieved?
- Is the testing proceduralized, and how are personnel trained to the procedures?
- Are maintenance personnel qualified by the equipment vendor to perform repairs?
- What is required to put the system back in service after maintenance and/or repair?
- Does the site have a training and qualification requirement for security technicians?

C.5 COMMUNICATIONS

Subtopical Areas to Testing Communications

None

Sample Document List:

Documentation to be reviewed may include the following:

- Performance tests of communication equipment
- Protective Force (PF) Post Orders
- PF General Orders
- Facility/site security plan and any Vulnerability Assessments
- Description of communication equipment, its location and test documentation
- Types of communication equipment issued to PF
- Shipment procedures

Sample Interview Candidates:

Interview candidates may include the following:

- PF Members
- Safeguards and security staff responsible for communication systems
- Alarms maintenance/installation and testing personnel
- Central Alarm Station (CAS)/Central Alarm Station (SAS) personnel
- Special Response Team members
- Emergency management planners

Sample Interview Questions:

Suggested questions to be asked during the interview process may include the following:

- How many channels are used on the PF radio system, and is this adequate?
- Do the PF channels have priority?
- Can non-PF radios eavesdrop on PF channels?
- How are PF radios issued/controlled?
- When was the last time your communication systems were upgraded and why?
- Are PF radios equipped with an encryption capability?
- Are there radio duress alarms, and how often are they tested?
- Are alternate means of communication available, and what are they?
- Is there an anti-jamming capability, and/or jamming detection?
- Can a single radio be identified and disabled by the CAS/SAS operator?
- How are the repeater towers protected?
- What compensatory actions are taken when radio communication is unavailable?

D. INFORMATION PROTECTION

Subtopical Areas to Information Protection

D.1 BASIC REQUIREMENTS
D.2 TECHNICAL SURVEILLANCE COUNTERMEASURES (TSCM)
D.3 OPERATIONS SECURITY (OPSEC)
D.4 CLASSIFICATION GUIDANCE
D.5 CLASSIFIED MATTER PROTECTION AND CONTROL (CMPC)
Control of Classified Matter
Special Access Programs and Intelligence Information

Areas of Consideration

The topical area team should research answers to the following types of questions during the course of document reviews. Answers to questions such as these may help to focus and streamline survey activities.

Is there a formal, coordinated effort regarding the implementation and management of the CMPC program?

- Have procedures been developed and approved for all aspects of the CMPC program, (i.e., generation, transmission, reproduction, dissemination, destruction)?
- Have control stations been established and are employees properly trained for their duties?
- Do the facility/site Security Plan and other planning documents adequately address CMPC?
- Has adequate training been provided to custodians and key personnel?

How is classification guidance disseminated?

- Does the facility have Derivative Classifiers (DCs) appointed in writing?
- Have DCs received required training?
- Is current classification guidance on hand for each of the facility's classified projects?

Does the facility have Special Access Programs (SAPs)?

- Have the SAPs been properly registered in accordance with the applicable DOE policy?
- Do all persons having access to SAPs have proper clearance and briefings?
- Are there specific security plans and operating procedures associated with SAPs?

How are DOE-HQ guidance and directives distributed?

- Are affected documents updated in a timely manner as guidance/direction is received?

What ratings were given for CMPC topics during past surveys and self-assessments?

- Is there a trend?
- Have all elements been reviewed?
- What is the status of open findings and corrective actions?

D.1 BASIC REQUIREMENTS

Subtopical Areas to Basic Requirements

None

Sample Document List:

The following documents should be requested and reviewed during the survey:

- Training records for personnel with information security responsibilities
- Information security procedures
- Classification guidance
- Local site-specific implementation procedures
- Facility/site security plan
- Controlled Unclassified Information procedures

Sample Interview Candidates:

Interviews candidates may include the following:

- Classification Officer
- Classified Matter Protection and Control (CMPC) Custodians and Control Station Operators
- CMPC Program Manager
- S&S Director
- Users of classified matter and Controlled Unclassified Information
- Cyber Security management and staff
- Operation Security Program Manager
- Technical Surveillance Countermeasures Operations Manager

Sample Interview Questions:

Suggested questions to be asked during the interview process may include the following:

- How is information security guidance disseminated to the facility personnel?
- What kind of training is provided to generators, users, control station operators?
- Is approved classification guidance disseminated and available to users for each of the facilities' classified projects?
- How is guidance (policy/procedure/requirements/changes) disseminated to the field/users?
- How are information system requirements funneled into security education and awareness?
- How is information security integrated to overarching S&S planning documents and other topical area plans?
- Do facility/site Security Plan and related documents adequately address the information security program?
- How is Controlled Unclassified Information stored, marked, generated, and reviewed at this facility?
- Are initial and annual classification awareness briefings conducted as required?

D.2 TECHNICAL SURVEILLANCE COUNTERMEASURES

Subtopical Areas to Technical Surveillance Countermeasures (TSCM)

None

Sample Document List:

The following documents should be reviewed:

- Formal assignments of TSCM Operations Managers (TSCMOMs) and TSCM Officers (TSCMOs)
- TSCM activity support memoranda (if applicable)
- Local TSCM operations plan
- TSCM service case files including inspections, surveys, advice and assistance, and preconstruction services
- Current annual TSCM schedule
- List of facilities that meet the minimum technical and physical security requirements
- TSCMO service files and corrective action reports
- TSCM team training and annual eligibility for TSCM Technician certification or re-certification records
- Local TSCM awareness education program
- Local security procedures, safety concerns, facility layout, site operation, and badge procedures
- Equivalencies/exemptions to DOE directives the facility may have pending and/or approved

Sample Interview Candidates:

The following individuals may be interviewed as appropriate:

- DOE TSCMOM
- Local Sensitive Compartmented Information Facility Special Security Officer (if applicable)
- Contractor TSCMO(s)
- Managers and technicians working with the TSCM program

Sample Interview Questions:

Suggested questions to be asked during the interview process may include the following:

- Are local TSCM capabilities available and sufficient to detect, deter, and/or nullify technical penetrations and hazardous conditions? If not, is a signed memorandum of understanding (MOU) to provide for appropriate TSCM support with another DOE site approved and coordinated through TSCM management?
- What kind of training has been provided to the TSCM team members?
- What reporting procedures of a TSCM penetration or hazard are in place? Are these procedures included in the site TSCM awareness briefing?
- Is there a TSCM awareness program?
- Is there a list of all facilities that meet TSCM service criteria?
- What procedures are followed to request TSCM services or report TSCM concerns?
- Are TSCM assets effectively utilized to conduct TSCM services in areas that discuss, process, and/or produce classified information?
- Is an annual schedule of TSCM activities in writing and approved? Is the schedule completed before the beginning of each new fiscal year?
- Are complete and up-to-date TSCM reference documents and memoranda, including DOE TSCM Manual and classified TSCM Annex, available?

- Is there an annual re-certification eligibility of TSCM personnel sent to TSCM program management?
- Are an appropriate number of contractor TSCMOs assigned to provide for effective management and coordination of local TSCM services?
- Have TSCMOs attended any training concerning TSCM services and activities?
- Does TSCM Technician training include safety, administrative, and specialized technical course (e.g., telephony, Operations Security, counterintelligence, information systems)?

D.3 OPERATIONS SECURITY

Subtopical Areas to Operations Security (OPSEC)

None

Sample Document List:

Specific OPSEC program documentation to be reviewed may include:

- Local OPSEC Plan
- Local OPSEC Awareness program files
- OPSEC reviews (of sensitive activities and facilities)
- Local Threat Statement
- Local Critical Information (CI) list
- Indicators list or other documentation reflecting current assets, threats, operations, and other relevant factors
- Counter-Imagery Program Plan (if applicable)
- Results of Internet Website assessments

Sample Interview Candidates:

Interview candidates may include the following:

- OPSEC point-of-contact
- Counterintelligence Program Manager
- OPSEC Working Group Chairperson
- Director/Manager of Safeguards and Security (S&S)
- Program/Project Manager of selected sensitive activities

Sample Interview Questions:

Suggested questions to be asked during the interview process may include the following:

- What OPSEC training has been provided to the OPSEC point-of-contact?
- Is an OPSEC program implemented to cover each program office, site, and facility to ensure the protection of classified and controlled unclassified information?
- Has a point-of-contact been established with overall OPSEC responsibilities for each site, facility, and program office?
- Does the OPSEC point-of-contact participate in the development of local implementation training and/or briefings tailored to the duties of the individual employees?
- Are OPSEC assessments being conducted at facilities having Category I special nuclear material (or credible rollup of Category II to a Category I quantity), Top Secret, or Special Access Program information within their boundaries?
- How are OPSEC concerns being disseminated to the staff of the facility?
- Have CPI and Indicator lists been developed? Are they current?
- Are assessments of websites conducted? How are they done? Has a process been established to conduct these assessments?
- Is there a review process for looking at website information prior to posting/making public? Who conducts the review and have criteria been established?

D.4 CLASSIFICATION GUIDANCE

Subtopical Areas to Classification Guidance

None

Sample Document List:

The following documents should be requested and reviewed during the survey:

- Number of Derivative Classifiers (DCs) and Derivative Declassifiers (DDs)
- Appointment letters
- Training records and materials
- Procedures
- Classification guidance
- Reviews/Inspections/Appraisals by other organizations

Sample Interview Candidates:

Meetings should be scheduled and interviews conducted with the following personnel:

- Classification Officer
- DCs and DDs
- Users of classified matter
- Classified Matter Protection and Control points of contact and custodians
- Unclassified Controlled Nuclear Information (UCNI) Reviewing Officials

Sample Interview Questions:

Suggested questions to be asked during the interview process may include the following:

- Have DCs been formally appointed and trained?
- How is classification guidance issued to other DCs?
- How is DC training provided and at what frequency?
- How do site personnel know where to go to get information reviewed for classification?
- Are reviews being conducted in a timely manner?

D.5 CLASSIFIED MATTER PROTECTION AND CONTROL

Subtopical Areas to Classified Matter Protection and Control (CMPC)

Control of Classified Matter
Special Access Programs and Intelligence Information

Sample Document List:

Documentation to be reviewed may include the following:

- CMPC procedures
- Control station procedures
- Training/briefing records and materials
- List of repositories (by custodian/organization, location, accountable/unaccountable)
- Facility/site Security Plan and any subordinate plans applicable to CMPC
- Recent self-assessments, survey reports, security appraisals and inspections
- Incidents of Security Concern (IOSC) involving CMPC
- List of equipment used to reproduce and destroy classified matter with locations and associated approvals
- Accountable matter inventory list(s)
- Special Access Program (SAP) security plans
- Results of accountable annual inventories
- Corrective action plan packages for recent findings

Sample Interview Candidates:

Interviews may be conducted with the following individuals:

- CMPC point-of-contact
- Control Station Operators
- Custodians or authorized users
- Reproduction staff
- Classified communications center staff
- Safeguards and Security (S&S) Director
- IOSC Program Manager
- SAP Manager/Sensitive Compartmented Information Facility Manager
- Cyber security management and staff

Sample Interview Questions:

Suggested questions to be asked during the interview process may include the following:

- How are site-specific implementation instructions disseminated to facility staff?
- What kind of training is provided to Control Station Operators, custodians, and authorized users of classified information? How often?
- Does the facility have any special or unique equipment to generate classified documents? What kind of training and procedures are available for this equipment?
- What procedures are used to enforce limiting access, need-to-know, and handling classified documents outside storage locations?
- What is the process for receipts not returned within the suspense period? How are follow-up actions documented?
- How are fax transmissions documented for verbal receipts?
- What are the hand carry procedures? How are staff identified and approved for hand carry? What kind of contingency plans are in place?
- How is information from other government agencies handled?
- What are the emergency procedures pertaining to CMPC?

- What procedures are available for intra-site messengers or post office couriers to ensure they constantly attend and control classified matter?
- What check-out procedures are used for staff who have transferred, terminated employment, or are otherwise unavailable for employment to ensure that they have surrendered all classified material in their possession?
- What is the notification process for suspensions/revocations of access authorizations?
- When was the last inventory conducted of accountable matter? What were the results?
- Is classified email a common practice at this facility?
- Are e-mails containing classified information marked in accordance with national requirements?
- How are classified document facilities managed (is there overnight storage, how is classified waste handled)?
- How is security managed for SAPs at this facility?
- How is need-to-know for SAPs determined?
- How are intelligence-related efforts coordinated with the Office of Intelligence?
- Has an individual been designated as being responsible for procurements involving field intelligence elements and/or Sensitive Compartmented Information?

E. PERSONNEL SECURITY

Subtopical Areas

E.1 ACCESS AUTHORIZATIONS

E.2 HUMAN RELIABILITY PROGRAM (HRP)
E.3 CONTROL OF CLASSIFIED VISITS
E.4 SAFEGUARDS AND SECURITY AWARENESS

Areas of Consideration

The topical area team should research answers to the following types of questions during the course of document reviews. Answers to questions such as these may help to focus and streamline survey activities.

Is there a formal, coordinated effort regarding the implementation and management of the Personnel Security program?

- Have procedures been developed and approved for all aspects of the program?
- Are processes completed in a timely and efficient manner?
- Do the facility/site security plan and other planning documents include Personnel Security elements such as HRP?
- Has adequate training been provided to key personnel?
- Has the HRP been formally documented? Have roles and authorities been defined?

Are the appropriate people cleared for the mission of the facility?

- Is proper justification required for all access authorizations? Is the approval appropriate?
- How often are re-justifications required?
- Are regular reviews conducted of access authorizations for subcontractors/consultants?

Are employees knowledgeable of their safeguards and security (S&S) responsibilities?

- Are meaningful briefings/training provided to staff in accordance with national requirements and DOE directives?
- Are attendance records kept?
- Are evaluations or other records used to ensure the information provided as part of S&S awareness is meaningful, adequate, and understood by staff?
- Does the security awareness program undertake use other supplementary awareness activities? If so, what are they? How are they distributed and what populations do they reach? Are they effective?
- Have individuals (both DOE Federal employees and contractor employees) been designated in writing as authorized representatives for purposes of accepting the SF 312, *Classified Information Non-Disclosure Agreement*?

Is there an effective classified visits program in place?

- Do the site security plan and local procedures address all types of classified visits (DOE employees, other cleared U.S. citizens, non-U.S. citizens?
- Who is the designated Federal official responsible for approving and documenting cleared U.S. citizens for access to RD/SNM during classified visits? Are clearances of visitors appropriately verified? What records of these visits are kept?
- Are continuing classified visits approved for no more than one year at a time?
- Are the identities of visitors, their level and type of clearance, and need to know established?
- For visit by foreign nationals, do procedures ensure that the following are established and

verified: identity of the visitor, assurance that the classified information to be shared is covered by an existing treaty or agreement, security assurances from the appropriate foreign embassy, and approval by the appropriate DOE Federal official for the sharing of the specific information to be disclosed?

- Are knowledgeable hosts assigned for classified visits by non-U.S. citizens? What training do the hosts receive? Do the hosts ensure that the foreign national does not receive access to classified information before approval is received from the appropriate DOE Federal Official? How do the hosts ensure that the foreign national is precluded from access to classified information outside the scope of the governing treaty or international agreement?

E.1 ACCESS AUTHORIZATIONS

Subtopical Areas to Access Authorizations

None

Sample Document List

Documentation to be reviewed may include the following:

- Access authorization/clearance requests to determine if justifications are adequate and include appropriate contract references
- Personnel security files:
  - Has proof of U.S. citizenship been validated using acceptable evidence?
  - Have the appropriate preprocessing checks been completed?
  - When access authorizations/clearances are granted based on reciprocity, are the required procedures for verifying the existing clearance followed and appropriately documented?
  - Have the appropriate forms been completed and submitted?
  - Do procedures ensure that individuals are not permitted to access classified information/matter or special nuclear material (SNM) until the DOE has granted, reinstated, shared, or transferred an active clearance/access authorization?
  - Are the files current and do they include all records required by the applicable DOE directive?
- Local procedures
- Contractor access authorization requests (justifications)
- Nondisclosure Agreement (SF 312) forms
- Training records, to include adjudicator training at sites where adjudicators are located
- Central Personnel Clearance Index records
- List of clearances terminated during the review period
- Case analysis sheets
- List of reinvestigations that are due or past due
- List of individuals on administrative leave
- List of individuals on leave of absence during the period
- List of classified contracts and the access authorizations associated with them

Sample Interview Candidates:

Interview candidates may include the following:

- Personnel Security Specialists, Personnel Security Assistants and other operations personnel
- Supervisors and cleared employees
- Badging personnel
- Personnel with clearances
- Human Reliability Program Adjudicator

Sample Interview Questions:

Suggested questions to be asked during the interview process may include the following:

- Is the need for an access authorization/clearance determined prior to processing? What constitutes valid need?
- What constitutes the type of access authorization/clearance to be processed and how is this determined (i.e., are the category and level of classified information/matter or category of SNM for each level requested defined)?
- What are the criteria for processing interim access authorizations?

- What procedures are in place to ensure foreign nationals who have been granted access authorizations are not granted access to classified matter such as Top Secret or NATO- or Intelligence-related information or to SNM?
- What procedures are in place to ensure that clearances/access authorizations are terminated for individuals who terminate employment or transfer to a position not requiring an access authorization?

E.2 HUMAN RELIABILITY PROGRAM

Subtopical Areas to Human Reliability Program (HRP)

None

Sample Document Lists:

Documentation to be reviewed may include the following:

- Implementation schedule
- Training records/materials
- Drug testing/handling procedures
- Drug testing records
- Random test procedures
- Site implementation plans and procedures
- Review procedures against requirements established in 10 CFR Part 712
  - Are HRP positions designated in accordance with the appropriate criteria (and are criteria defined)?
  - Do procedures include annual submission of required forms?
  - Do procedures include appropriate reviews (i.e., supervisory review, medical assessment, management evaluation, and DOE personnel security)?
  - Do procedures address reporting requirements?
  - Do procedures address temporary reassignments and/or removals based on issues identified through the HRP process? Appeals process?
- Review the initial and annual refresher HRP instruction and education program
  - Do lesson plans include appropriate information for all types of positions (i.e., supervisors and managers, employees, HRP medical personnel, and for those with nuclear explosive responsibilities)?
- Review files to ascertain if appropriate records are maintained and properly protected

Sample Interview Candidates:

Interview candidates may include the following:

- Facility Managers, Supervisors, and cleared personnel
- Participants in the HRP
- Supervisors
- HRP Coordinator
- Medical personnel

Sample Interview Questions:

Suggested questions to be asked during the interview process may include the following:

- Has the program been reviewed and approved by DOE?
- Is there a drug testing program for HRP positions? Have procedures been developed and implemented which provide for random drug testing of staff in HRP-designated positions?
- What is the rate of random drug testing?
- Does the site have an HRP Implementation Plan?
- Do individuals in or applying for an HRP position undergo a security review and clearance determination prior to being assigned an HRP position?
- What training is provided for individuals in and/or administering the HRP program?
- Do all employees have a “Q” access authorization prior to assuming the duties of an HRP position?
- Has a formal process been established for HRP?

E.3 CONTROL OF CLASSIFIED VISITS

Subtopical Areas to Control of Classified Visits

None

Sample Document List:

Documentation to be reviewed may include the following:

- Written delegation of authority for senior Federal official to make determinations allowing individuals cleared by another agency to have RD access in connection with classified visits
- Procedures applicable to the classified visits program as documented in the facility/site security plan
- Classified visit reports, control logs, and other classified visit files, including tracking of access granted in connection with a classified visit to individuals cleared by another agency
- Documentation establishing responsibility for operational approval of classified visits
- Documentation of programmatic approval received for access to specified facilities, data, or technology
- Designation of individuals to serve as hosts for classified visits by non-U.S. citizens

Sample Interview Candidates:

The following people should be considered for interviews:

- Employees responsible for processing and controlling classified visits
- Individuals responsible for processing, controlling, and approving visits of uncleared U.S. citizens
- Staff who routinely host visitors or tours
- Senior Federal official delegated authority to make determinations of RD access for individuals cleared by another agency

Sample Interview Questions:

Suggested questions to be asked during the interview process may include the following:

- What is the local policy regarding escort-to-visitor ratios?
- Are visitor logs used at Protected Areas? Material Access Areas? Exclusion Areas?
- Have procedures been developed and implemented for classified visits by DOE employees, contractors, and subcontractors? For employees and contractors of other Government agencies, including DoD, NRC, and NASA employees? For non-U.S. citizens?
- Are specific procedures developed for individuals from other government agencies who wish to access classified information for which they do not hold the appropriate clearance?
- Who approves requests for classified visits?
- When are briefings provided to individuals cleared for access to RD solely in connection with the classified visit? What acknowledgement do these individuals sign?
- What are the responsibilities of an escort?
- From what office are classified visit requests sent and received?
- How is information concerning temporary clearances granted to individuals cleared by another agency transmitted to visit escorts?
- How are the identities of visitors, their level and type of clearance, and need-to-know established?
- Do local site procedures require that formal visit requests be submitted for visiting DOE

personnel?

- How are the identities of foreign visitors, assurances that the information proposed for sharing is covered by treaty or international agreement, security assurances from the foreign embassy, and verification of official DOE Federal approval for sharing of the classified information established?
- How is information concerning classified information that may be shared with a foreign visitor passed to the assigned host?
- How are foreign visitors precluded from access to classified information outside the scope of the international agreement or treaty governing the visit? How is information relevant to the limitations of the visit passed on to the host?

E.4 SAFEGUARDS AND SECURITY AWARENESS

Subtopical Areas to Safeguards and Security Awareness

None

Sample Document List:

Documentation to be reviewed may include the following:

- Lesson plans for the initial briefing, comprehensive briefing, refresher briefing, and termination briefing
  - Do the briefings address site-specific needs, S&S interests, and potential threats to the facility/organization? Is the information up to date (last review/update)?
  - Do contents include items outlined in the applicable DOE directive for each briefing?
  - Are briefings given prior to assuming duties or accessing applicable information, as applicable?
- Instructional aids (includes student handouts)
- Written designations of Federal and contractor employees authorized to accept SF 312s on behalf of the Government
- Briefing attendance/completion records
- Evaluation records
- Supplemental awareness tools (posters, newsletters, etc.)
- Sampling of Classified Information Nondisclosure Agreements (SFs-312) to verify they are appropriately executed before access to classified information or matter is granted
- Applicable procedures
  - Do procedures include appropriate notification for failure or refusal to complete an SF-312?
  - Do procedures include all required briefings?
- Briefing records. Records must be maintained to provide an audit trail verifying an individual's receipt of the briefings.
  - Are completed SF-312s maintained on all individuals completing the comprehensive briefing?
  - Is DOE F 5631.29 used to document completion of the termination briefing?
  - Are lesson plans and records of supplementary activities maintained?
  - Are SF 312s retained in accordance with the applicable DOE and General Records Schedules?
  - Do contractors retain SF 312s only for the period of employment and send forms of employees who terminate to DOE? Does the DOE cognizant security office ensure that this is done?
  - Are SF 312s stored in accordance with requirements of the Code of Federal Regulations and the applicable DOE Administrative Records Schedule?
  - Are originals or legally enforceable facsimiles of the SF 312 maintained in a file system from which they can be readily retrieved?

Sample Interview Candidates:

Interview candidates may include the following:

- S&S Manager (DOE and Contractor)
- DOE and Contractor Security Awareness Coordinators
- Security Awareness Briefing Attendees
- Operations Security Manager
- Site Managers and Supervisors
- Facility/site employees (to gauge effectiveness of security awareness activities)

- Individuals authorized to witness and accept the SF 312

Sample Interview Questions:

Suggested questions to be asked during the interview process may include the following:

- Do awareness briefings/training contain site-specific information and recent threat information?
- Has the facility/site security awareness coordinator attended the NTC security awareness training?
- Do S&S awareness information and/or briefings address site-specific procedures as well as specific topics such as recent espionage cases, foreign intelligence recruitment techniques, incidents and considerations, and S&S threats and vulnerabilities?
- What types of training records are kept relative to security awareness?
- How are the contents of the Annual Refresher Briefing determined?
- How are briefings scheduled?
- Are initial briefings given before employees are given unescorted access to other than public areas of the facility/site?
- Are comprehensive briefings completed and the SF 312 executed before individuals receive access to classified information and/or SNM?
- Are refresher briefings done on an annual basis? What actions are taken by the facility/site when a cleared individual fails to complete the annual refresher briefing?
- Are termination briefings conducted whenever an individual no longer requires access to classified information for any reason (including administrative termination of a security clearance, termination of employment, unavailability for work due to circumstances such as being barred from the site or imprisoned, etc.)?
- What efforts are undertaken to obtain the individual's signature on the Security Termination Statement Form (DOE F 5631.29) if the individual is not available to sign the form?
- Is notification made to the processing personnel security office within the required time frame when an individual's clearance is terminated?

F. FOREIGN VISITS AND ASSIGNMENTS

Subtopical Areas

F.1 SPONSOR PROGRAM MANAGEMENT AND ADMINISTRATION
F.2 COUNTERINTELLIGENCE (CI) REQUIREMENTS
F.3 EXPORT CONTROLS/TECH TRANSFER REQUIREMENTS
F.4 SECURITY REQUIREMENTS
F.5 APPROVALS AND REPORTING

Areas of Consideration

The topical area team should research answers to the following types of questions during the course of document reviews. Answers to questions such as these may help to focus and streamline survey activities.

Is access to facilities adequately controlled?

- Is foreign national local area network access being granted based on a documented assessment of risk?
- Are hosts aware of their responsibilities?
- Who has approval authority for all unclassified foreign visits and assignments at the site/facility? Is this designation in writing?
- Who approves the security plans for unclassified foreign visits and assignments to security areas?
- What is the process for ensuring adequate coordination among security, CI, export control, and foreign intelligence should a foreign national require access to a security area or sensitive subject, or if the individual is visiting from a sensitive country?
- Have employees been notified of the requirement to report foreign nationals who may attend officially sponsored offsite functions? If not, how does the approval authority know to concur or exempt the activity?

Are security measures in place?

- Does the facility have a standard or generic security plan in place?
- Do security plans address the sensitivity factors, including area type to be visited, determination of whether information containing sensitive subjects will be shared, and affiliation with sensitive countries or countries identified as state sponsors of terrorism?
- Does the security plan identify general restrictions on access?
- Is there a specific security plan for each visit/assignment involving a sensitive country national, security area, and/or subject?

F.1 SPONSOR PROGRAM MANAGEMENT AND ADMINISTRATION

Subtopical Areas to Sponsor Program Management and Administration

None

Sample Document List:

The following documentation should be considered for review:

- Documentation authorizing approval for specific categories of visits and assignments
- Indices checks
- Training records (escort and hosts)
- Security incidents/infractions involving visits and assignments
- Escort/host procedures
- Visit-specific security plans
- Unclassified computer security review
- Operations Security (OPSEC) reviews/assessments
- Counterintelligence (CI) program reviews/assessments
- Notification of approval documentation
- Equivalencies/exemptions pertinent to visits and assignments
- Foreign National Visits and Assignments closeout information
- Justification-for-visit request approvals and denials
- Foreign Access Central Tracking System (FACTS) submittals
- Facility/site security plans

Sample Interview Candidates:

The following individuals are candidates for interviews:

- Safeguards and Security Manager (DOE and Contractor)
- OPSEC/CI Program Manager (DOE and Contractor)
- Unclassified Computer Security Manager
- Program Managers and Supervisors
- Local FACTS Coordinator
- OPSEC Coordinator and/or OPSEC Working Group members
- Hosts/escorts
- Visit control

Sample Interview Questions:

Suggested questions to be asked during the interview process may include the following:

- Which organization maintains the responsibility for indices checks?
- Who has approval authority for all unclassified visits and assignments at the site?
- Who approves the security plans for unclassified foreign visits and assignments to security areas?
- What is the process for ensuring adequate coordination among security, CI, export control, and foreign intelligence should a foreign national require access to a security area or sensitive subject, or if the individual is visiting the site from a sensitive country?
- Are approved procedures in place for unclassified visits and assignments by foreign nationals?

F.2 COUNTERINTELLIGENCE REQUIREMENTS

Subtopical Areas to Counterintelligence (CI) Requirements

None

Sample Document List:

The following documentation should be considered for review:

- Documentation authorizing approval for specific categories of visits and assignments
- Indices checks
- Sensitive countries listing
- Documentation identifying sensitive topics
- Visit-specific security plans
- CI briefings
- CI Host briefings/debriefings
- Justification-for-visit request approvals and denials
- Foreign Access Central Tracking System submittals

Sample Interview Candidates:

The following people should be considered for possible interviews:

- Safeguard and Security Manager (DOE and Contractor)
- CI Program Manager (DOE and Contractor)
- Operations Security (OPSEC) Coordinator, OPSEC Working Group members, and/or other individuals assigned responsibilities for the OPSEC program
- Hosts/escorts
- Visit control

Sample Interview Questions:

Suggested questions to be asked during the interview process may include the following:

- Which organization maintains the responsibility for indices checks?
- Who has approval authority for all unclassified visits and assignments at the site?
- Who approves the security plans for unclassified Foreign National Visits and Assignments (FNVA) to security areas?
- Is there a process covering the conduct and approval of CI consultations in lieu of indices not returning when return of indices is required?
- Do records indicate indices checks were requested and/or completed as required?
- What is the process for ensuring adequate coordination among security, CI, export control, and foreign intelligence should a foreign national require access to a security area or sensitive subject, or if the individual is visiting the site from a sensitive country?
- How does CI provide review and input to approval authority on FNVA requests?

F.3 EXPORT CONTROLS/TECHNOLOGY TRANSFER REQUIREMENTS

Subtopical Areas to Export Controls/Technology Transfer Requirements

None

Sample Document List:

The following documentation should be considered for review:

- Sensitive countries listing
- Documentation identifying sensitive topics
- Visit-specific security plans
- Notification of approval documentation
- Equivalencies/exemptions pertinent to visits and assignments
- Justification-for-visit request approvals and denials

Sample Interview Candidates:

The following people should be considered for interviews:

- Safeguards and Security Manager (DOE and Contractor)
- Export Control/Technology Transfer Manager or Subject Matter Expert
- Program Managers and Supervisors
- Hosts/escorts
- Visit control

Sample Interview Questions:

Suggested questions to be asked during the interview process may include the following:

- Is export control and tech transfer involved in the Foreign National Visits and Assignments (FNVA) approval process? How and at what level?
- Who approves the security plans for unclassified FNVA to security areas?
- What is the process for ensuring adequate coordination among security, counterintelligence, export control, and foreign intelligence should a foreign national require access to a security area or sensitive subject, or if the individual is visiting the site from a sensitive country?

F.4 SECURITY REQUIREMENTS

Subtopical Areas to Security Requirements

None

Sample Document List:

The following documentation should be considered for review:

- Sensitive countries listing
- Documentation identifying sensitive topics
- Visit-specific security plans
- Notification of approval documentation
- Justification-for-visit request approvals and denials

Sample Interview Candidates:

The following people should be considered for interviews:

- Safeguards and Security Manager (DOE and Contractor)
- Program Managers and Supervisors
- Hosts/escorts
- Visit control

Sample Interview Questions:

Suggested questions to be asked during the interview process may include the following:

- Does the facility have a standard or generic security plan in place? Does the plan address visits by non-U.S. citizens?
- Does the security plan adequately ensure security interests and sensitive information/technologies are not placed at risk?
- Does the security plan identify general restrictions on access?
- Is there a specific security plan for each visit/assignment involving a sensitive country national, security area, and/or subject?

F.5 APPROVALS AND REPORTING

Subtopical Areas to Approvals and Reporting

None

Sample Document List:

The following documentation should be considered for review:

- Documentation authorizing approval for specific categories of visits and assignments
- Indices checks
- Escort/host procedures
- Sensitive countries listing
- Documentation identifying sensitive topics
- Visit-specific security plans
- Notification of approval documentation
- Deviations pertinent to visits and assignments
- Justification-for-visit request approvals and denials
- List of DOE Foreign Access Central Tracking System (FACTS) entries for site/facility for specified scope of self-assessment

Sample Interview Candidates:

The following people should be interviewed regarding the unclassified Foreign National Visits and Assignments (FNVA) program:

- Safeguards and Security Manager (DOE and Contractor)
- Program Managers and Supervisors
- Hosts/escorts

Sample Interview Questions:

Suggested questions to be asked during the interview process may include the following:

- Which organization maintains the responsibility for indices checks?
- Who has approval authority for all unclassified visits and assignments at the site?
- Who approves the security plans for unclassified FNVA to security areas?
- What is the process for ensuring adequate coordination among security, counterintelligence, export control, and foreign intelligence should a foreign national require access to a security area or sensitive subject, or if the individual is visiting the site from a sensitive country?
- What is the process to ensure that the approval authority considers information from the review process and Subject Matter Expert reviews?
- How are approval determinations being documented in DOE FACTS when required?
- Who is the approval authority? Has that approval authority been further re-assigned? Has it been re-assigned in writing and what was the distribution?
- Are there plans and procedures for re-assignment of approval authority and has that re-assignment been reviewed and approved by the head of the cognizant DOE field element and the approval authority?
- Who is the designated point-of-contact for Unclassified FNVA program management? Has that point-of-contact information been provided to the DOE cognizant security office?

G. MATERIALS CONTROL AND ACCOUNTABILITY (MC&A)

Subtopical Areas

G.1 PROGRAM MANAGEMENT
G.2 MATERIAL ACCOUNTABILITY
G.3 MATERIALS CONTROL
G.4 MEASUREMENT
G.5 PHYSICAL INVENTORY

Areas of Consideration

The topical area team should research answers to the following list of questions during the course of document reviews. Answers to questions such as these may help to focus and streamline survey activities.

Has the facility documented and implemented the MC&A program to ensure an adequate infrastructure is in place?

- How does the performance testing program evaluate its materials loss-detection capability and support and verify vulnerability assessments?
- How does the accounting system provide a complete audit trail for all nuclear materials from receipt or production through transfer or disposition?
- Has a physical inventory program been developed and implemented to determine the quantity of nuclear materials on hand both by item and in total?
- Has a measurement control program been implemented to establish nuclear inventory values and to ensure the quality of the nuclear materials database?
- Is there a program in place to assess the material control indicators and ensure detection of losses and unauthorized removals of safeguarded items or materials, both on an individual and cumulative basis?
- Has a program been formally documented for controlling personnel access to nuclear materials; nuclear materials accountability, inventory, and measurement data; and other items or systems where misuse could compromise the safeguards program?

Is there a formal, coordinated effort regarding the development, approval, and updates associated with the MC&A plan?

- Is there a process in place to ensure MC&A plans and procedures are reviewed and updated in a timely manner?
- Is a nuclear material surveillance program formally documented within the plan and is it capable of detecting unauthorized activities or anomalous conditions?
- Does the nuclear materials containment program ensure that nuclear materials are used, stored, or processed only in authorized locations? Is it formally documented in the MC&A plan?
- Are facility requirements and performance metrics adequately documented in the plan?
- Does the MC&A plan have the proper approval?
- Is the plan comprehensive?

Has management established an effective and efficient organization structure?

- Is the MC&A function sufficiently independent from production operations to ensure that there are no conflicts of interest that might be detrimental to the protection of nuclear materials?
- Are there indications of frequent change in the organizational structure?

- Where are roles, responsibilities, and authorities defined and documented?
- Are lines of communication, accountability, and authority clear?
- Is the organization at a level to achieve effective program implementation?
- Is there a documented program that ensures personnel performing MC&A functions are trained and qualified?

Has the facility properly categorized its nuclear material?

- Is there a documented categorization process?
- How have Material Balance Areas (MBAs) been designated?
- Were all materials considered when category levels were established?
- Are adequate controls in place to ensure categorization limits are not exceeded?

Do the Site Security Plan/Vulnerability Assessment documents adequately address MC&A elements?

- Do MC&A personnel participate actively in the site security plan development?
- Was the full threat spectrum used and were multiple scenarios evaluated and documented?
- Were single, abrupt, and protracted theft and diversion scenarios documented?
- Is the documentation consistent with the MC&A plan, procedural directives, and security-related documentation, and does it accurately correlate with conditions at the facility?
- Is the performance testing program active and effective?
- Is occurrence investigation and reporting defined and incorporated into the overall facility program?

G.1 PROGRAM MANAGEMENT

Subtopical Areas to Program Administration

None

Sample Document List:

Documentation to be reviewed may include the following:

- Approved Material Control and Accountability (MC&A) plans and procedures
- Facility/Site Security Plan and Vulnerability Assessments (VAs)
- Equivalencies/exemptions for MC&A with supporting documentation
- Organization charts
- Training records, lesson plans
- MBA operating plans
- Surveys, internal assessments and corrective action plans
- MC&A performance testing program plan and documentation
- Categorization process documentation
- Incident reporting process and procedures
- Emergency response plans

Sample Interview Candidates:

Interview candidates may include the following:

- MC&A Program Manager and management chain
- Facility Nuclear Material Representative
- Material Balance Area Custodians/alternate custodians
- Emergency management personnel
- Operations personnel
- Personnel responsible for developing security plan/VA documents
- Personnel responsible for MC&A internal reviews and assessments

Sample Interview Questions:

Suggested questions to be asked during the interview process may include the following:

- Has a nuclear MC&A program that meets the requirements of applicable DOE directives for all special, source, and other nuclear materials on inventory been implemented?
- Is the MC&A management official organizationally independent from responsibilities of other programs?
- Is the MC&A program documented in a properly approved MC&A plan and procedure?
- Is the MC&A program implemented on the basis of the graded safeguards concept?
- Has a program to periodically review and assess the integrity and quality of the MC&A program and practices been implemented? Is this program on schedule?
- Has a documented program to ensure that personnel performing MC&A functions are trained and qualified been implemented? Does the site use the NTC training program? Has it received approval from the Training Approval Program?
- Has a loss-detection evaluation been performed and documented for each Category I facility including facilities for which a credible scenario for rollup of Category II to a Category I quantity of special nuclear materials been identified?
- Have performance requirements for MC&A system elements been documented and a performance testing program implemented? Is the program active? Is it effective?
- Have MC&A loss-detection elements been included in documented procedures for reporting Incidents of Security Concern?
- Are procedures developed and documented for characterizing materials on inventory to

determine categories and attractiveness under the graded safeguards concept?

G.2 MATERIAL ACCOUNTABILITY

Subtopical Areas to Material Accountability

None

Sample Document List:

Documentation to be reviewed may include the following:

- Material Control and Accountability (MC&A) plans and procedures related to materials accounting
- Equivalencies/exemptions
- Facility procedures
- Database descriptions
- Material Balance Area (MBA) account structure
- Material transfer records
- Inventory records
- Organization charts
- Internal control procedures
- Nuclear Material Management and Safeguards System (NMMSS) reports
- Training records, reports, lesson plans
- Shipper/receiver agreements
- Shipper/receiver difference procedures and records
- Inventory difference program
- Internal assessments and corrective action plans

Sample Interview Candidates:

Candidates for interviews include the following:

- MC&A Program Manager
- MBA Custodians/alternate custodians
- Training personnel
- Measurements personnel
- Individuals responsible for NMMSS
- Measurements and Measurements Control personnel
- Personnel responsible for MC&A internal reviews and assessments

Sample Interview Questions:

Suggested questions to be asked during the interview process may include the following:

- Does the accounting structure assist in the determination of the category and attractiveness level of each MBA?
- Who determines the MBA and account structure? Who can change it? How is it changed?
- What role does the accounting system play in determining categories of MBAs?
- What role does the accounting system play during inventory?
- What records does the system require to be input? Are data transcribed? How are laboratory data input? How are the accuracy and timeliness of entries ensured and verified?
- What output formats are used and who receives copies of the reports?
- Are the required reports being issued in a timely manner?
- Who prepares MBA transfers? How are authorizations verified? Are authorizations in the form of signatures or computer passwords?
- What calculations do accounting personnel perform? Are they trained and qualified to perform these calculations?
- How are transfer checks accomplished? Are they documented?

- Is confirmation of measured values on internal transfers required? If so, how is this accomplished?
- How often are measurement instruments calibrated?
- Have the nondestructive assay measurement methods been approved and certified?
- How is the inventory reconciliation documented and supported?
- Is a wall-to-wall inventory conducted or is some other means used?
- Is there an approved statistical sampling plan? If so, who approves this plan?
- Is a shipper/receiver agreement in place for all offsite receipts and shipments?
- How are measurement methods certified?
- How are measurements personnel trained and certified?
- How are transfer forms controlled?
- Are material items deemed non-amenable to measurement documented in the MC&A plan?
- Is there a documented, approved, measurement-control program?
- Are statistical limits appropriate, approved, and used to monitor and correct measurement system performance?
- Are standards appropriate for the material types being assayed? Are they traceable to the national measurement base?
- Is there an approved scales/balance program? Are there stipulated requirements for check-weights to be used prior to obtaining an accountability weight? Are these documented?
- Are confirmation/verification measurements conducted for shipments and receipts?
- For liquids processing, are prescribed solution mixing times required prior to taking a sample for accountability measurement?

G.3 MATERIALS CONTROL

Subtopical Areas to Material Control

None

Sample Document List:

Documentation to be reviewed may include the following:

- Materials containment documentation
- Material Control and Accountability (MC&A) plans and procedures
- Facility procedures
- Equivalencies and exemptions
- Facility/Site Security Plan and Vulnerability Assessments (VAs)
- Material Access program plan
- Authorization access lists
- Combination change records
- Material Balance Area (MBA) Custodian lists and training records
- Material surveillance procedures
- Portal monitor records and procedures
- Daily administrative check program and procedures
- Tamper Indicating Device (TID) program procedures and records of receipt, disbursement, application, removal, inventory, and destruction
- Internal assessments and corrective action plans

Sample Interview Candidates:

Candidates for interviews may include the following:

- MC&A Program Manager
- MBA Custodians/alternate custodians
- Training personnel
- Portal Monitoring staff
- Personnel responsible for MC&A internal reviews and assessments

Sample Interview Questions:

Suggested interview questions may include the following:

- How are keys and combinations to Special Nuclear Materials (SNM) areas controlled?
- Does the facility have a documented program to provide controls of nuclear material operations relative to Material Access Areas (MAAs)?
- Are there approved procedures governing MBA-to-MBA and MAA-to-MAA material transfers?
- What training is provided to MBA custodians? Frequency?
- What transfer controls are in place?
- Are material surveillance programs in place for Category I and II material?
- Are Process Accountability Flow Diagrams used? Are they up to date? Have personnel been trained to use them?
- How are tamper-indicating devices (TID) controlled and maintained?
- How is waste monitoring done? Is it comprehensive?
- Are documented controls covering nuclear material being used or stored in processing areas?
- How is access to SNM use and storage locations approved?
- How is the two-person rule implemented at the facility?
- Are material custodians prohibited from hands-on SNM functions?

- Are searches conducted of all persons exiting an MAA?
- Is a daily administrative check program implemented at the facility?
- How is the TID program documented and approved?
- Does the TID program include sample testing of new TIDs to ensure compliance with requirements?
- Who is responsible for testing and calibrating portal monitors? Are problems corrected in a timely manner?

G.4 MEASUREMENT

Subtopical Areas to Measurement

None

Sample Document List:

Documentation to be reviewed may include the following:

- Measurement control procedures
- Material Control and Accountability (MC&A) plans and procedures
- Facility/site Security Plan and vulnerability assessments
- Equivalencies and exemptions
- List of materials not amenable to measurement
- Measurement control methodology in use at the site/facility
- Documentation of standards
- Control charts
- Method selection/qualification program procedures
- Training plans
- Records showing differences over time with trending and bias analysis

Sample Interview Candidates:

Candidates for interviews may include the following:

- MC&A Program Manager
- Measurement personnel
- Measurement control personnel
- Training personnel
- Accounting staff
- Personnel responsible for selecting and qualifying measurement systems
- Personnel responsible for MC&A internal reviews and assessments

Sample Interview Questions:

Suggested interview questions may include the following:

- What types and forms of nuclear materials are in the inventory?
- What nuclear materials are included in the accounting records?
- What materials are included on the list of nuclear materials that are not amenable to measurement? Are they clearly and accurately defined?
- How are the accuracy and precision of each measurement method estimated?
- How do the measurement control procedures ensure that only calibrated measurement systems for which control has been demonstrated are used for accountability?
- Do the calibration standards have traceability?
- What method is used to monitor measurement control? Does this method show that the measurement method used meets accuracy and precision goals under actual conditions at the facility? Are measurement uncertainties defined?
- How are data trends evaluated? How are biases quantified?
- How are individuals trained to perform measurements? Is there a training plan?
- How do individuals demonstrate proficiency in measurement techniques? Are they required to demonstrate proficiency before they perform accountability measurements?
- Does the training cover basic equipment operation? Method capability and potential interferences? Calibration and recalibration requirements? Documentation requirements for measurement results?
- Are personnel trained in actions to be taken when out-of-control situations are detected?

How effective is the training?

G.5 PHYSICAL INVENTORY

Subtopical Areas to Physical Inventory

None

Sample Document List:

Documentation to be reviewed may include the following:

- Measurement control procedures
- Material Control and Accountability (MC&A) plans and procedures
- Facility/site Security Plan and vulnerability assessments
- Equivalencies and exemptions
- Inventory schedule
- Supporting documentation for alternative inventory frequencies
- NMMSS records
- Statistical sampling plans
- Inventory difference (ID) histories and trend analyses
- Inventory listings
- Records for in-process materials
- List of materials not amenable to measurement

Sample Interview Candidates:

Candidates for interviews may include the following:

- MC&A Program Manager
- Nuclear Materials Representative
- Statistician
- Operations Manager
- Accounting staff

Sample Interview Questions:

Suggested interview questions may include the following:

- What types and forms of nuclear materials are in the inventory?
- Are the Material Balance Area boundaries clearly and properly defined?
- What locations in the processing areas may cause process holdups? Are holdups included in the inventory?
- What is the basis for the quantities of holdup? Is holdup measured, or does it have a technical basis?
- What cutoff procedures are used at the time of physical inventories? In cases where cutoff procedures are not used, what controls are in place to ensure that all material movements are included in the inventory?
- What controls are in place to ensure that materials selected for inventory in the process area are not processed further until the inventory activities for these materials are complete? If the material cannot be tallied at the time of inventory, what monitoring measures are used to follow it until it reaches a measurable form?
- Are there any side streams (e.g., solid or liquid waste) resulting from the processing activities? If so, how are these accounted for?
- Under what circumstances does the facility perform special inventories? Have any special inventories been done? Have corrective actions been indicated, and if so, have they been implemented?
- What has the facility defined as inventory defects? What is the response to address

defects?

5.0 POST-SURVEY TOOLS

This section contains items to aid in documenting and presenting the results of survey or self-assessment activities.

5.1 Sample Initial/Periodic Survey Report Format
5.2 Sample Termination Survey Report
5.3 Sample Slides for Exit Briefing
5.4 Sample Report Transmittal Memorandum
5.5 DOE Survey/Inspection Report Form

5.1 Sample Initial/Periodic Survey Report Format

a. Report Format. The report may be formatted with a cover page, table of contents, ratings, executive summary, introduction, description of facility and interests, narrative (including topical area description of the program), conclusions, synopsis of findings, and appendices. The DOE 470.8, *Survey/Inspection Report Form*, if used, should be included in the report.

b. Report Content.

(1) Initial and Periodic Survey Reports and Self-Assessment Reports. Reports should contain the following items.

(a) An executive summary containing:

1 The scope, methodology, period of coverage, duration, date of the exit briefing to management;

2 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, and overall scores assigned to the most recent contract appraisal);

3 A brief synopsis of major strengths and weaknesses that impact the effectiveness of the facility's overall S&S program, including identification of any topical areas rated less than satisfactory;

4 The overall composite facility rating with supporting rationale; and

5 A reference to a list of findings identified during the survey or self-assessment.

(b) An introduction containing:

1 The scope, methodology, period of coverage, duration, date of the exit briefing to management; and

2 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, and overall scores assigned to the most recent contract appraisal).

(c) Narrative for all rated topical and subtopical areas that includes:

1 A description of the site's implementation of the topical/subtopical element;

2 The scope of the evaluation;

3 A description of activities conducted;

4 The evaluation results and associated issues (including other Department elements or OGA review or inspection results related to this topic/subtopic that were included in the survey);

5 The identification of all findings, including new and previously identified open findings, regardless of source (e.g., EA, IG, GAO), and their current corrective action status; and

6 An analysis that provides a justification and rationale of the factors responsible for the rating.

(d) Attachments, including, for example:

1 A copy of the current DOE F 470.2, *Facility Data and Approval Record* (FDAR);

2 A listing of all active DOE F 470.1, *Contract Security Classification Specification* (CSCS), or DD F 254, *Contract Security Classification Specification*;

3 A listing of all new findings resulting from the survey/self-assessment;

4 A listing of all previous findings that are open, to include the current status of corrective actions;

5 A listing of team members including names, employer, and their assigned area(s) of evaluation; and

6 A listing of all source documentation used to support the survey/self-assessment conduct and results.

Narrative: The narrative section of the report should clearly describe the surveyed facility – its safeguards and security (S&S) interests and activities, its protective measures, and the status of the S&S program at the time the survey or self-assessment activity was completed. The report should also explain how the protection measures were evaluated. Use of statistical data will help describe the facility's S&S interests and the survey effort. Such data might include numbers of employees with each level of access authorization, the number of classified documents in each level and category, and the number of documents sampled for compliance/performance.

The report should reflect the compliance and performance segments of the survey. Reports should explain what the S&S program is supposed to do, what was surveyed, how the survey data was compiled (e.g., extended data collection or within a few days), and what was found. Suggested content includes:

- The status (e.g., approved, pending, under revision) of any required planning documents (e.g., Facility/Site Security Plan, Material Control and Accountability [MC&A] plans, local implementation procedures, etc.).

- All new findings should be identified. Open findings from the previous survey should be identified in the narrative portion of the survey report. Open findings maintain their original finding number. A new finding, including one that is a repeat of a closed finding, receives a new SSIMS-compatible finding number. When a finding is a repeat of a closed finding, reference to the closed finding should be included in the body of the narrative.

- Findings, observations, opportunities for improvement, and suggestions, along with supporting data for each, should be clearly described. The term "finding" refers to a factual statement of issues and deficiencies representing a failure to meet a documented legal, regulatory, performance, compliance, or other applicable requirement found during the survey or self-assessment.

- Descriptions of the facility's strengths and weaknesses should correlate to the survey results and establish the bases for the ratings. The survey report should reflect validated and defensible ratings. The narrative description should be consistent with and support the composite and topical area ratings (including "Does Not Apply").

- The report should identify findings corrected on the spot. These findings and corrective actions should be clearly described in the narrative.

- The status of corrective actions for open findings and findings from the previous survey should be included in the narrative.
- A concluding analysis of each topical area should be included in the narrative.
- Reasons for a less-than-satisfactory rating should be explained in detail.

5.2 Sample Termination Survey Report

SCOPE

This report documents the results of the Safeguards and Security (S&S) termination survey of the XXX Site facilities Safeguards and Security Division (SSD) which was conducted by personnel from XXX Site Office. This report contains the results of the termination survey conducted [inclusive dates].

This survey was an on-site effort designed to review and ensure the proper and effective disposition and transfer of Department of Energy (DOE) classified matter, facility approvals, access authorizations, and site operating procedures from the XXX SSD to XXX Site Office. Located in Building 123, SSD was operated under FDAR Number 123-HQ-01-001 with an Importance Rating of A. Possession of Secret Restricted Data (S/RD) weapon data was authorized at the facility. Additionally, the SSD was the single Reporting Identification Symbol (RIS) for receipt and shipment of all Category I and II special nuclear material (SNM) stored and processed at the facility. The end users were assigned individual material balance area numbers under the SSD RIS. The SSD did not store SNM directly; it was stored at the end user locations, which included XXXX and GDT National Laboratory. As of the time of this survey, SNM was being shipped directly to and stored at, the assigned user under their own RIS account. SSD continues to provide oversight and management of the Nuclear Materials Control and Accountability program at the XXX under the auspices of XXX Site Office.

FACILITY OPERATIONS

The SSD was tasked by DOE to manage the security operations at the XXX facility. This activity has been modified and this responsibility will be absorbed into the XXX Site Office management activities.

VERIFICATION ACTIVITIES

RESOLUTION OF FINDINGS

At the beginning of this termination survey all survey findings associated with SSD had been closed.

CLASSIFIED MATTER

All classified matter, including accountable matter, has either been destroyed or transferred to XXX Site Office.

A walk through and visual verification of classified security containers was conducted as part of this termination survey. There were no issues relating to this survey.

SSD has executed a Certificate of Non-possession for activities at Building XXX and a final DOE F 470.1, *Contract Security Classification Specification*; copies are included as **Appendix 1**.

Communications Security (COMSEC)
The COMSEC equipment assigned to SSD has been transferred to XXX Site Office and this account is being closed. Appropriate documentation is on file with the XXX Site Office Facility Security Officer.

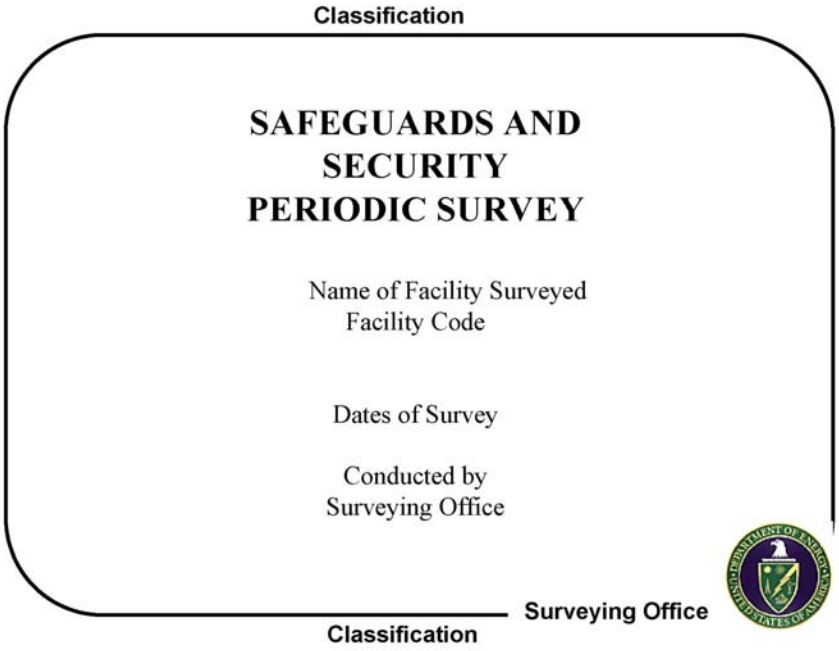
NUCLEAR MATERIAL CONTROL AND ACCOUNTABILITY
SSD did not possess nuclear and/or other hazardous material presenting a potential radiological or toxicological sabotage threat as explained above.

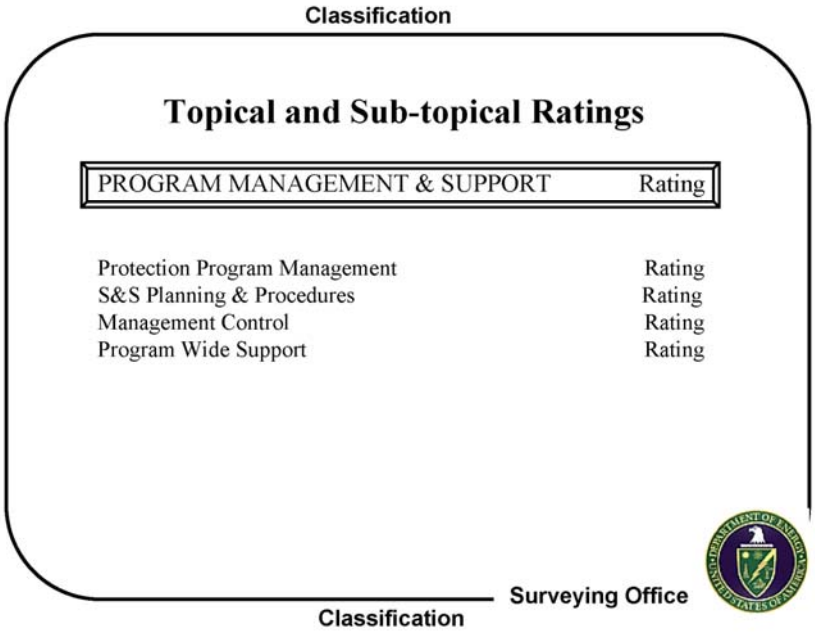
PERSONNEL SECURITY
The staff associated with the SSD conduct similar functions under XXX Site Office thus their access authorizations will remain active and transferred to the Site Office. There were no contractors supporting the SSD.

FACILITY CLEARANCE
At the completion of this termination survey, the Facility Data and Approval Record will be terminated. There are no contract(s) or subcontracts associated with this facility, thus no further actions are required.

CONCLUSION
This termination survey successfully confirmed (1) the termination or transfer of all classified matter and/or nuclear and other hazardous material presenting a potential radiological or toxicological sabotage threat; (2) all personnel access authorizations are needed and will be transitioned to XXX Site Office; (3) all S&S activities continue under the XXX Site Office; and (4) the facility clearance has been terminated.

5.3 Sample Slides for Exit Briefing. Slides would be included for each topical and subtopical area.





Classification

Protection Program Management

Program Management & Administration:	Rating
Resource & Budgeting:	Rating
Personnel Development & Training:	Rating

A satisfactory rating is given if all applicable compliance and performance measures are met and implementation is suitable for the mission operating environment.

If less than a satisfactory rating is given, list key issues that influenced the rating.

Continue for each sub-topical area.

Surveying Office

Classification

Classification

Composite Rating

A composite rating is based upon

- the rating for each topical area;
- the impact of all open deficiencies, regardless of source; and
- the existing conditions at the end of the survey period, not future planned corrective actions.

Less than satisfactory ratings must be based on validated weaknesses in the S&S system or deficiencies in performance. All ratings must be supported and documented to include the rating justification and rationale.

Surveying Office

Classification

5.4 Sample Report Transmittal Memorandum

DATE:

REPLY TO
ATTN OF:

SUBJECT: Safeguards and Security Periodic Survey Report (Organization Being Surveyed)

TO: All Departmental Elements with a Registered Activity
All Appropriate Headquarter Elements

The attached report outlines results of the recent Safeguards and Security Survey of the [Organization Surveyed] conducted by the [Organization, Office]. This periodic survey conducted [M/D/Y] encompassed [all security topical areas as defined on DOE F 470.8, Survey/Inspection Report Form, the following topical and subtopical areas, or other description as appropriate.]

The composite rating assigned to [organization being surveyed] is [rating]. The assignment of this rating [indicates that the facility S&S program is operating as expected; dictates that corrective action plans be developed, or other description as appropriate.]

If you have questions regarding this report, please contact [Name, Organization] on [telephone number].

Include classification information as appropriate.

5.5 DOE Survey/Inspection Report Form (Current form available at http://energy.gov/cio/office-chief-information-officer/services/forms)

DOE F 470.8
(09/2014)
Replaces DOE F470.8 (09-2012)
All Other Editions are Obsolete

U.S. Department of Energy
SURVEY/INSPECTION REPORT FORM

1. Type: Survey: ◉ Initial ○ Periodic ○ Special ○ Termination ○ EA Reviews: ○ NPR ○ EPR ○ Self-Assessment		2. Report #:
3. Facility Name:		4. a. Facility Code: b. RIS Code:
5. Survey Date(s):	6. a. Findings: ○ Yes ○ No b. Findings Against Other Facilities:	7. Composite Rating:
8. Previous Survey Date(s): Next Survey Date:	9. Unresolved Findings: ○ Yes ○ No	10. Previous Rating:
11a. Surveying Office:	11b. Cognizant Security Office:	11c. Other Offices with Interests:

12. Ratings:

a) PROGRAM MANAGEMENT OPERATIONS
- PROTECTION PROGRAM MANAGEMENT ____
  - Program Management and Administration ____
  - Resources and Budgeting ____
  - Personnel Development and Training ____
- S&S PLANNING AND PROCEDURES ____
- MANAGEMENT CONTROL ____
  - Surveys and Self Assessment Programs ____
  - Performance Assurance Program ____
  - Resolution of Findings ____
  - Incident Reporting and Management ____
- PROGRAM WIDE SUPPORT ____
  - Facility Approval and Registration of Activities ____
  - Foreign Ownership, Control or Influence ____
  - Security Management in Contracting ____

OVERALL RATING ____

b) PROTECTIVE FORCE ____
- MANAGEMENT ____
- TRAINING ____
- DUTIES ____
- FACILITIES AND EQUIPMENT ____

OVERALL RATING ____

c) PHYSICAL PROTECTION
- ACCESS CONTROLS ____
- INTRUSION DETECTION & ASSESSMENT SYSTEMS ____
- BARRIERS AND DELAY MECHANISMS ____
- TESTING AND MAINTENANCE ____
- COMMUNICATIONS ____

OVERALL RATING ____

d) INFORMATION SECURITY
- BASIC REQUIREMENTS ____
- TECHNICAL SURVEILLANCE COUNTERMEASURES ____
- OPERATIONS SECURITY ____
- CLASSIFICATION GUIDANCE ____
- CLASSIFIED MATTER PROTECTION & CONTROL ____
  - Control of Classified Matter ____
  - Special Access Programs and Intelligence Information ____

OVERALL RATING ____

e) PERSONNEL SECURITY
- ACCESS AUTHORIZATIONS ____
- HUMAN RELIABILITY PROGRAMS ____
- CONTROL OF CLASSIFIED VISITS ____
- SAFEGUARDS AND SECURITY AWARENESS ____

OVERALL RATING ____

f) MATERIALS CONTROL & ACCOUNTABILITY
- PROGRAM MANAGEMENT ____
- MATERIAL ACCOUNTABILITY ____
- MATERIALS CONTROL ____
- MEASUREMENT ____
- PHYSICAL INVENTORY ____

OVERALL RATING ____

g) FOREIGN VISITS AND ASSIGNMENTS
- SPONSOR PROGRAM MANAGEMENT & ADMIN ____
- COUNTERINTELLIGENCE REQUIREMENTS ____
- EXPORT CONTROLS/TECH TRANSFER REQUIEMENTS ____
- SECURITY REQUIREMENTS ____
- APPROVALS AND REPORTING ____

OVERALL RATING ____

13. Report Prepared by: Date:	14. Report Approved by: Date:
15. Distribution:	
16. General Comments:	

Ratings: S = Satisfactory M = Marginal U = Unsatisfactory DNA = Does Not Apply

CONCLUDING MATERIAL

Review Activity
EM
Policy (AU-51)
AU
MA
NE
NNSA
SC

Preparing Activity
Office of Security Policy (AU-51)

Field and Operations Offices
CH
ID
NNSA Service Center
ORO
RL
SRO

Project Number
P2013-06

Site Offices
ANL
INL
LASO
LLSO
NSO
OR
PSO
RLSO
SRSO
SSO
YSO

External Agency