



NOT MEASUREMENT  
SENSITIVE

DOE-STD-1217-2020  
FEBRUARY 2020

DOE STANDARD

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



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

DISTRIBUTION STATEMENT A. Approved for public release; distribution is unlimited.

THIS PAGE INTENTIONALLY LEFT BLANK

## FOREWORD

This Department of Energy Technical Standard is for use by all Departmental elements. Email any beneficial comments (recommendations, additions, and deletions) and pertinent data that may improve this document to [natasha.sumter@hq.doe.gov](mailto:natasha.sumter@hq.doe.gov) or mail to:

U.S. Department of Energy  
Office of Environment, 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 “must” or “shall” are used to denote actions that must be performed if the objectives of this standard are to be met. If the provisions in this Standard are made requirements through one of the three ways discussed above, then the “shall” statements would become requirements. Goals or intended functionality are indicated by “will,” “may,” or “should.” 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.

THIS PAGE INTENTIONALLY LEFT BLANK

## CONTENTS

FOREWORD.....	iii
ACRONYMS AND ABBREVIATIONS.....	1
1.0 SCOPE.....	5
2.0 PURPOSE .....	5
3.0 APPLICABILITY .....	5
4.0 REFERENCES.....	5
5.0 Internet sources of reference materials.....	6
5.1 <u>DOE Survey Form</u> .....	6
5.2 <u>EFCOG Self-assessment Tool Kit</u> .....	6
6.0 DEFINITIONS .....	7
7.0 DUTIES, RESPONSIBILITIES, AND TRAINING .....	7
7.1 Survey Team Leader .....	7
7.2 Survey Topical Lead .....	9
7.3 Survey Team Members.....	10
7.4 Self-assessment Team Leads and Members .....	11
8.0 SURVEY AND SELF-ASSESSMENT OVERVIEW .....	11
9.0 SURVEY AND SELF-ASSESSMENT PLANNING.....	14
9.1 Cyclic Planning for Surveys and Self-Assessments .....	14
9.2 Planning a Facility Survey or Self-Assessment.....	15
9.2.1 Pre-Planning.....	15
9.2.2 Preliminary Coordination.....	15
9.2.3 Planning Survey and Self-Assessment Activities .....	17
10.0 SURVEY AND SELF-ASSESSMENT CONDUCT .....	17
10.1 In-Briefing.....	17
10.2 Maintaining Communication.....	18
10.3 Data Collection.....	18
10.3.1 Performance Tests .....	20
10.3.2 Data Validation .....	21
10.3.3 Data Analysis .....	21
10.3.4 Ratings.....	23
10.4 Exit Briefing.....	25

11.0	REPORT PREPARATION .....	25
12.0	Issues Management program.....	27
12.1	Corrective Action Program.....	28
12.2	Process Improvement .....	29
12.2.1	Step 1: Understand and Map the Current Process.....	29
12.2.2	Step 2: Complete a Value Added Analysis .....	31
12.2.3	Step 3: Develop an Improved Process.....	33
12.2.4	Step 4: Update Documentation and Develop Metrics .....	34
12.2.5	Step 5: Measure for Success and Return to Step 1.....	34
(1)	TEST OBJECTIVE.....	56
(2)	SCENARIO DESCRIPTION .....	56
(3)	TEST METHODOLOGY AND EVALUATION CRITERIA .....	56
(4)	PASS/FAIL CRITERIA.....	56
(5)	TEST CONTROLS .....	57
(6)	RESOURCE REQUIREMENTS .....	57
(7)	TEST COORDINATION REQUIREMENTS .....	57
(8)	OPERATIONAL IMPACT(S) OF TESTING PROGRAM .....	57
(9)	COMPENSATORY MEASURES .....	58
(10)	COORDINATION AND APPROVAL PROCESS .....	58
(11)	REFERENCES.....	58
1	Introduction .....	237
1.1	Overview of Site.....	237
1.1.1	Mission.....	237
1.1.2	Location/Address .....	237
1.2	Scope .....	237
1.3	Purpose .....	237
2	Roles and Responsibilities.....	237
2.1	Program Office .....	237
2.2	Field/Site Office .....	237
2.3	Contractors .....	237
2.4	ODFSA/ODSA Delegations.....	237
3	Approval of Security Plan .....	237
3.1	Federal Approval of Security Plan .....	237
4	Residual Risk Identification and Acceptance.....	237

---

4.1	Identification of Residual Risk.....	237
4.1.1	Basis for residual risk determination.....	237
4.2	Federal Acceptance of Residual Risk.....	237
5	Assets.....	237
5.1	List of Assets.....	237
5.2	Prioritization of Assets.....	237
6	Security Plan Development and Review.....	237
6.1	Analytical Basis.....	237
6.1.1	Plan based on DOE O 470.3C.....	238
6.1.2	DOE Tactical Doctrine, as applicable.....	238
6.1.3	Security Risk Assessment / Vulnerability Assessment Overview.....	238
6.2	Review and Update.....	238
6.2.1	Review – procedures regarding plan review.....	238
6.2.2	Update – procedures to provide updates and revisions to the plan.....	238
7	Program Planning and Management.....	238
7.1	PPM Overview.....	238
7.1.1	Federal Oversight (Field and Program Office).....	238
7.1.2	Contractors.....	238
7.1.3	Work-for Others.....	238
7.2	Facility Clearance Program.....	238
7.2.1	Procedures applicable to the FCL program.....	238
7.3	Foreign Ownership, Control, or Influence.....	238
7.3.1	Procedures applicable to the FOCI program.....	238
7.4	Classified Visits.....	238
7.4.1	Procedures applicable to classified visits and assignments.....	238
7.5	Unclassified Foreign Visitors and Assignments.....	238
7.5.1	Procedures applicable to unclassified foreign visits and assignments.....	238
7.6	Incident of Security Concern.....	238
7.6.1	Overview of the Incident of Security Concern program.....	238
7.7	Equivalencies and Exemptions.....	238
7.7.1	Overview of the process.....	238
7.7.2	List of Approved Equivalencies and Exemptions incorporated in Security Plan.....	238
7.8	Memorandums of Agreement/Understanding.....	238
7.8.1	Approval process.....	238

7.8.2	Review Process .....	238
7.8.3	List of all MOAs/MOUs .....	238
7.9	SECON .....	238
7.9.1	Overview of the SECON plan and procedures.....	238
7.10	Performance Assurance .....	239
7.10.1	Performance Assurance planning .....	239
7.10.2	Performance testing.....	239
7.10.3	System degradation .....	239
7.10.4	Reviews and updates .....	239
7.11	Safeguards and Security Training .....	239
7.11.1	Overview of the Safeguards and Security Training program.....	239
7.12	Security Awareness Program .....	239
7.12.1	Overview of the Security Awareness program.....	239
7.13	Security-Funded Technologies, if applicable .....	239
7.13.1	Overview of the process to transfer security-funded technologies .....	239
7.14	Demonstrator and Protestor Plan.....	239
7.14.1	Responsibilities .....	239
7.14.2	Memoranda of Agreement or Understanding.....	239
7.14.3	Event notification .....	239
7.14.4	Minimum requirements .....	239
7.15	Workplace Violence Plan .....	239
7.15.1	Responsibilities .....	239
7.15.2	Memoranda of Agreement or Understanding.....	239
7.15.3	Event notification .....	239
7.15.4	Minimum requirements .....	239
8	Physical Security .....	239
8.1	General Site Access.....	239
8.1.1	Employees .....	239
8.1.2	Visitors .....	239
8.1.3	Other Federal Agency Badges.....	239
8.2	Prohibited and Controlled Articles .....	239
8.2.1	Prohibited Articles.....	239
8.2.2	Controlled Articles .....	239
8.3	Entry and Exit Inspections.....	240



8.3.1	Entry Inspections procedures .....	240
8.3.2	Exit inspection procedures .....	240
8.3.3	Property Removal.....	240
8.4	Security Areas (as applicable) .....	240
8.4.1	General Access Areas.....	240
8.4.2	Property Protection Areas .....	240
8.4.3	Limited Areas.....	240
8.4.4	Vaults/Vault-Type Rooms.....	241
8.4.5	Sensitive Compartmented Information Facilities .....	242
8.4.6	Special Access Program Facilities .....	242
8.4.7	Protected Areas .....	242
8.4.8	Material Access Areas.....	243
8.5	Lock and Key Program.....	244
8.5.1	Overview of lock and key program.....	244
8.5.2	Inventory system .....	245
9	Protective Force, if applicable.....	245
9.1	Management .....	245
9.1.1	Overview of Pro Force management.....	245
9.1.2	Non-uniformed staffing.....	245
9.2	Training .....	245
9.2.1	Initial .....	245
9.2.2	Annual .....	245
9.2.3	Firearms.....	245
9.3	Certification.....	245
9.3.1	Medical & Physical .....	245
9.4	Staffing .....	245
9.4.1	Security Officer .....	245
9.4.2	Fixed Post.....	245
9.4.3	Security Police Officer (SPO) Is .....	245
9.4.4	SPO IIs .....	245
9.4.5	SPO IIIs .....	245
9.5	Duties .....	245
9.5.1	Normal duties .....	245
9.5.2	Emergency duties .....	245

---

9.6	Equipment .....	245
9.6.1	Duty Equipment .....	245
9.6.2	Vehicles.....	246
10	Nuclear Material Control and Accountability, if applicable .....	246
10.1	Characterization of the Nuclear Control and Accountability program.....	246
10.1.1	Shall address probability of detection of loss of Category I SNM with 95% probability, if applicable.....	246
10.1.2	Shall define loss detection capability for other Categories of SNM .....	246
11	Personnel Security .....	246
11.1	Procedures for new clearances .....	246
11.2	Clearance transfers, extensions, upgrades, downgrades, and cancellations .....	246
11.3	Reporting requirements .....	246
12	Insider Threat Mitigation Program.....	246
12.1	Procedures applicable to the Insider Threat Mitigation Program.....	246
12.2	Description of Local Insider Threat Working Group (LITWG).....	246
12.3	Human Reliability Program, if applicable .....	246
12.3.1	Overview of HRP program .....	246
12.3.2	Roles and Responsibilities .....	246
12.3.3	HRP Certification.....	246
12.3.4	HRP Removal.....	246
13	Information Security.....	246
13.1	Classified Matter Protection and Control .....	246
13.1.1	Procedures utilized to protect classified matter, to include:.....	246
13.2	Controlled Unclassified Information.....	247
13.2.1	Procedures utilized to protect CUI information .....	247
14	Cyber Security .....	247
14.1	Overview of cyber security program.....	247
14.2	Roles and Responsibilities.....	247
14.2.1	Authorizing Official .....	247
15	Operations Security .....	247
15.1	Overview of the Operations Security program.....	247
15.2	Identification and release of controlled information .....	247
16	Technical Security Program, if applicable .....	247
16.1	Overview of the Technical Security program.....	247

17	Surveys and Assessments .....	247
17.1	Surveys .....	247
17.1.1	Site Office .....	247
17.1.2	Program Office .....	247
17.2	Self-Assessments .....	247
17.3	Findings and Corrective Actions .....	247
17.4	Reviews, Reports and Ratings .....	247

## LIST OF FIGURES

Figure 8:1	Portable Universal Quality System Audit Template .....	13
Figure 12:1	Initial Notification Memo Process Map .....	31
Figure 12:2	Initial Notification Memo Color-Coded Process Map .....	32
Figure 12:3	Notification Memo Improved Process Map .....	33

## LIST OF TABLES

Table E-1	Example of SNM Theft/Diversion Targets .....	250
Table E-2.	Example of Radiological Sabotage Targets .....	251
Table E-3.	Example of Biological/Chemical Sabotage Targets .....	251
Table E-4.	Example of Disruption of Critical Mission Targets .....	252
Table E-5.	Example of Site-Wide Protection Strategies .....	253
Table E-6.	Example of Facility Protection Systems .....	254
Table E-7.	Example of Qualifications and Training .....	255
Table E-8.	Example of MC&A Plans and Procedures .....	256
Table E-9.	Example of Personnel Security/Human Reliability .....	257
Table E-10.	Example of Automated Information Systems Security Programs .....	258
Table E-11.	Example of S&S-Related Maintenance, Testing, and Records Management Programs .....	260
Table E-12.	Example of Site Protection Program Evaluation Program .....	260
Table E-13.	Example of Deviations from DOE Contractor Requirements .....	261
Table E-14.	Example of Pending Deviations from DOE Contractor Requirements .....	261
Table E-15.	Example of Identified Risks Summary .....	263
Table E-16.	SNM Theft/Diversion Targets .....	263
Table E-17.	Example of Credible Radiological Sabotage Targets .....	263
Table E-18.	Example of Credible Biological Sabotage Targets .....	264
Table E-19.	Example of Credible Chemical Sabotage Targets .....	264
Table E-20.	Example of Disruption of Critical Mission Targets Table .....	264

Table E-21. Example of Performance Testing Results of Site-Specific .....	266
Table E-22. Example of Critical Path Scenarios .....	267
Table E-23. Example of Protection Effectiveness (PE) for Theft or Diversion of SNM .....	268
Table E-24. Example of Protection Effectiveness (PE) for Radiological Sabotage .....	268
Table E-25. Example of Protection Effectiveness (PE) for Biological Sabotage.....	269
Table E-26. Example of Protection Effectiveness (PE) for Chemical Sabotage .....	269
Table E-27. Example of Protection Effectiveness (PE) for Disruption of Critical Missions .....	269
Table E-28. Example of Protection Effectiveness (P <sub>E</sub> ) for Theft/Espionage of Classified Information/Matter .....	270
Table E-29. Example of Protection Effectiveness (PE) for Other Losses .....	270
Table E-30. Example of System Effectiveness Summary .....	270

**ACRONYMS AND ABBREVIATIONS**

CAP	Corrective Action Plan
CAS	Central Alarm Station
CDCO	Classified Document Control Office
CDCS	Classified Document Control Station
CI	Critical Information
CMPC	Classified Matter Protection and Control
COMSEC	Communications Security
CPCI	Central Personnel Clearance Index
CSCS	Contract Security Classification Specification
DBT	Design Basis Threat
DEAR	DOE Acquisition Regulation
DNA	Does Not Apply
DOE	Department of Energy
ECD	Estimated Completion Date
EOC	Emergency Operations Center
FACTS	Foreign Access Central Tracking System
FCL	Facility Clearance Level
FDAR	Facility Data and Approval Record
FEMA	Federal Emergency Management Agency
FN	Foreign national
FOCI	Foreign Ownership, Control or Influence
FOF	Force-on-force
FSL	Facility security level

FSC	Facility Security Committee
FSO	Facility Security Officer
GSP	Graded Security Protection
HRP	Human Reliability Program
ID	Inventory difference
IDS	Intrusion detection system
IOSC	Incident of Security Concern
ISC	Interagency Security Committee
JTA	Job Task Analysis
KMP	Key Management Personnel
LLEA	Local law enforcement agencies
LOI	Lines of Inquiry
LSPT	Limited scope performance test
MAA	Material Access Area
MBA	Material Balance Area
MC&A	Material Control and Accountability
MOA	Memoranda of Agreement
MOU	Memoranda of understanding
N/A	Not Applicable
NMMSS	Nuclear Material Management and Safeguards System
NTC	National Training Center
NR	Not Rated
ODFSA	Officially Designated Federal Security Authority
ODSA	Officially Designed Security Authority

OFI	Opportunities for Improvement
OGA	Other government agency
OPSEC	Operations Security
PF	Protective Force
REVCOM	Review and Comment
RIS	Reporting Identification Symbol
RMP	Risk Management Process
S&S	Safeguards and Security
SAP	Special Access Program
SAS	Secondary Alarm Station
SEC	Securities and Exchange Commission
SECON	Security condition
SNM	Special nuclear material
SP	Security plan
SRA	Security Risk Assessment
SRD	Secret Restricted Data
SRT	Special Response Team
SSD	Safeguards and Security Division
SSIMS	Safeguards and Security Information Management System
SSPS	Safeguards and Security Periodic Survey
TID	Tamper-Indicating Device
TSCM	Technical Surveillance Countermeasures
TSCMO	TSCM Officer
TSCMOM	TSCM Operations Managers

UCNI	Unclassified Controlled Nuclear Information
UFVA	Unclassified Foreign Visitors and Assignments
VA	Vulnerability Analysis



## **1.0 SCOPE**

This document provides the Department of Energy (DOE) with a standard methodology for adapting the Department's requirements to conduct and report 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. Appendix A, *Safeguards and Security (S&S) Survey and Self-Assessment Toolkit*, provides guidance and useful templates for planning, conducting, and reporting surveys and self-assessments.

## **2.0 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 and report S&S surveys and self-assessments prescribed in DOE Order (O) 470.4B Minor Change 2.

## **3.0 APPLICABILITY**

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

## **4.0 REFERENCES**

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

DOE Manual 471.3-1, Administrative Change 1, *Identifying and Protecting Official Use Only Information*, January 13, 2011

DOE Order 142.3A Limited Change 2, *Unclassified Foreign Visits and Assignments Program*, January 18, 2017

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

DOE Order 413.3B, Minor Change 5, *Program and Project Management for the Acquisition of Capital Assets*, April 12, 2018

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

DOE Order 470.3C, *Design Basis Threat*, November 23, 2016

DOE Order 470.4B, Minor Change 2, *Safeguards and Security Program*, January 17, 2017

DOE Order 470.6 Minor Change 1, *Technical Security Program*, January 11, 2017

DOE Order 471.1B, *Identification and Protection of Unclassified Controlled Nuclear Information*, March 1, 2010

DOE Order 471.3, Administrative Change 1, *Identifying and Protecting Official Use Only Information*, January 13, 2011

DOE Order 471.5, *Special Access Programs*, March 29, 2011

DOE Order 471.6, Administrative Change 3, *Information Security*, September 12, 2019

DOE Order 472.2, Page Change 1 (Certified), *Personnel Security*, July 16, 2015

DOE Order 473.3A, Minor Change 1, *Protection Program Operations*, January 2, 2018

DOE Order 475.1, *Counterintelligence Program*, December 10, 2004

DOE Order 475.2B, *Identifying Classified Information*, October 3, 2014

DOE Policy 470.1B, *Safeguards and Security Program*, February 10, 2016

*The Risk Management Process for Federal Facilities: An Interagency Security Committee Standard*, 2nd Edition, November 2016

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

Title 32 Code of Federal Regulations Part 2004, *National Industrial Security Program*

Title 32 Code of Federal Regulations, Part 2001, *Classified National Security Information*

## **5.0 INTERNET SOURCES OF REFERENCE MATERIALS**

**5.1 DOE Survey Form:** <https://www.energy.gov/cio/downloads/doe-f-4708>

**5.2 EFCOG Self-assessment Tool Kit:** <https://efcog.org/wp-content/uploads/Wgs/Safeguards%20and%20Security%20Working%20Group/Documents/2014-SSWG%20PPM-Toolkit-S%26S%20Self-Assessment.pdf>

## 6.0 DEFINITIONS

Definitions commonly used in the Safeguards and Security Program can be found in the Office of 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. Deficiency: An inadequacy in the implementation of an applicable requirement or performance standard that is found during an appraisal. Deficiencies may serve as the basis for findings.
- b. 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 shall be further studied before implementation.
- c. 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 shall be further studied before implementation. Opportunities for Improvement (OFI) may also be identified as Suggestions, Recommendations, Findings, Weakness, or other site-specific terminology.
- d. Strength: A term used to identify in a survey or self-assessment that the program or item in review is operating better than required by the Order. Strengths may also be known as noteworthy practices, or other site-specific terminology.
- e. Weakness: A term used to identify in a survey or self-assessment that the program or item in review is operating less than optimum as required by the Order. Weakness may also be known as an opportunity for improvement, or other site-specific terminology.

## 7.0 DUTIES, RESPONSIBILITIES, AND TRAINING

### 7.1 Survey Team Leader

The DOE cognizant security office line management shall appoint a federal employee as the Survey Team Leader for surveys of facilities with an importance rating of “A”, “B,” or “C”. For other facilities, the Survey Team Leader 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 Leader is responsible for the successful completion of the survey. This person shall have a comprehensive understanding of S&S programs, have previous survey experience (preferably as a Survey Topical Lead or Survey Team Leader), and be especially capable of integrating topical area results into a comprehensive assessment of facility security. It is highly desirable that the Survey Team Leader has completed

training courses offered by the National Training Center (NTC) on survey conduct and management.

The Survey Team Leader 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 Leader 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 topical teams, and acting as a team spokesperson during meetings and briefings. In particular, the team leader 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.

Survey Team Leader responsibilities may include the following:

- a. Develops the survey plan.
- b. Prepares and maintains an Annual Master Survey Schedule.
- c. Is trained by DOE NTC (or another training institution/organization), or qualified by their Program Office to lead a survey team.
- d. Appoints Survey Team members for each evaluation. The selections shall achieve a balance of technical knowledge, experience, writing ability, survey experience, survey ability, and availability. Employees who are technical area specialists may augment the staff and could include direct support contractors, other employees, other organization employees, or other site employees.
- e. Ensures the survey team conducts security surveys of facilities under their cognizant authority in a timely manner.
- f. Conducts Survey in-briefings, daily management meetings and closeout briefings.
- g. Ensures survey data is entered in the Safeguards and Security Information Management System (SSIMS); in accordance with SSIMS data entry procedures and DOE line management direction.
- h. Ensures Initial Surveys are conducted for all new facilities with a security interest prior to granting facility approval.
- i. Ensures Periodic Surveys are conducted according to the established risk-based management process,
- j. Ensures Termination Surveys are conducted for all facilities that no longer have a security interest.

- k. Ensures the importance rating for approved facilities is updated as necessary.
- l. Consolidates all staffing resource requirements, to include such items as overtime requirements for federal staff, requests for assistance from other Program Managers or other organizations, typing and editing support, and contractor support. Presents the consolidated schedule, staffing requirements, and scope of the survey to the appropriate leadership.
- m. Ensures that all necessary logistical arrangements are made, including the availability of adequate workstations, classified computers, security containers, and authorized Derivative Classifiers as deemed necessary. Also coordinates with appropriate organizations for the proper access control, site-specific training requirements, and issuance of safety equipment.
- n. Prepares the data call letter with input from the Topical Leads and forwards that letter to the organization(s) to be surveyed or assessed at least 30 days prior to the beginning of the survey.
- o. Conducts daily meetings with the Topical Leads and with the appropriate management of the organization(s) being surveyed to keep them informed of concerns resulting from the day's data-collection activities.
- p. Review and approves Topical Lines of Inquiry (LOIs)
- q. Reviews Topical Area Survey Reports; including survey results from previous surveys.
- r. Provides guidance to Topical Leads and Survey Team members as necessary.
- s. Provides guidance to federal and contractor personnel in the preparation of corrective action plans (CAPs) for findings issued to their organization.
- t. Maintains reports in accordance with DOE requirements
- u. Employ a risk analysis methodology to define the scope and critical topical areas of interest to review during the survey (see Attachment 1).

## 7.2 Survey Topical Leader

A topical lead for each topical area to be surveyed should either be appointed by the same authority appointing the Survey Team Leader or, alternately, be designated by the Survey Team Leader. The topical lead must be an expert in his or her assigned topical area. In some cases, it may be necessary to select a contractor as topical 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 Leader to complete pre-planning, to ensure that each topical area team collects the

data required for preparation of the survey report, and to ensure that written and verbal deliverables assigned to the topical area teams are of high quality and are delivered according to the schedule. Each topical lead conducts, with the assistance of the topical area team, a topical area analysis of results, and recommends topical area 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.

- a. Trained through the DOE NTC or other organization
- b. Responsible for the activities of Survey Team members assigned to their topical area
- c. Responsible for meeting all deliverable deadlines in a timely manner.
- d. Develops Topical Area LOIs for their areas and provides to the Survey Team Leader for approval.
- e. Responsible for ensuring that Survey Team members integrate and coordinate their activities with other topical area teams as appropriate.
- f. Conduct daily meetings with their Survey Team members on data-collection activities and concerns.
- g. Brief the Survey Team Leader on data-collection activities and concerns.
- h. Ensures notes are reviewed for classification and appropriately marked, and then submitted to the Survey Team Leader.
- i. Provide the consolidated Topical Area Report, including the suggested ratings and accurate reference citations, to the Survey Team Leader.
- j. Incorporate changes to the Topical Area Report as required by the Survey Team Leader.
- k. Ensure that all notes, working papers, and other data-collection materials are collected from survey team members for retention.

### **7.3 Survey Team Members**

Selection of survey team members shall be coordinated among the Survey Team Leader, topical leads, and the organizations for which the individuals work. Team members shall be selected for technical competence, professionalism, and experience, 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 shall have previous experience and demonstrated expertise in the topical area or sub-topical area 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 shall perform under the direct supervision of an individual with previous experience and demonstrated expertise in the topical area 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 NTC on survey conduct and management.

- a. Keep Topical Leads or Team Leader informed of data-collection activities and concerns.
- b. Keep notes in sufficient detail for briefing and report development.
- c. Meet deadlines for all deliverables.
- d. Prepare their portion of the final report in the proper format, including recommended ratings and findings.
- e. Provide accurate reference citations for all findings to ensure that the finding is consistent with DOE Orders and other requirements.
- f. Write findings such that corrective actions can be completed.
- g. Process classified information only on accredited computers.
- h. Discuss potential survey results only with other individuals on the Team to confirm if a potential finding shall be a finding in the final survey report. The Survey Team Leader will provide the surveyed organization's management a daily briefing on the status of activities and concerns.

#### **7.4 Self-assessment Team Leads and Members**

Self-assessment team leaders, topical leads, and team members shall 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 area team leaders.

### **8.0 SURVEY AND SELF-ASSESSMENT OVERVIEW**

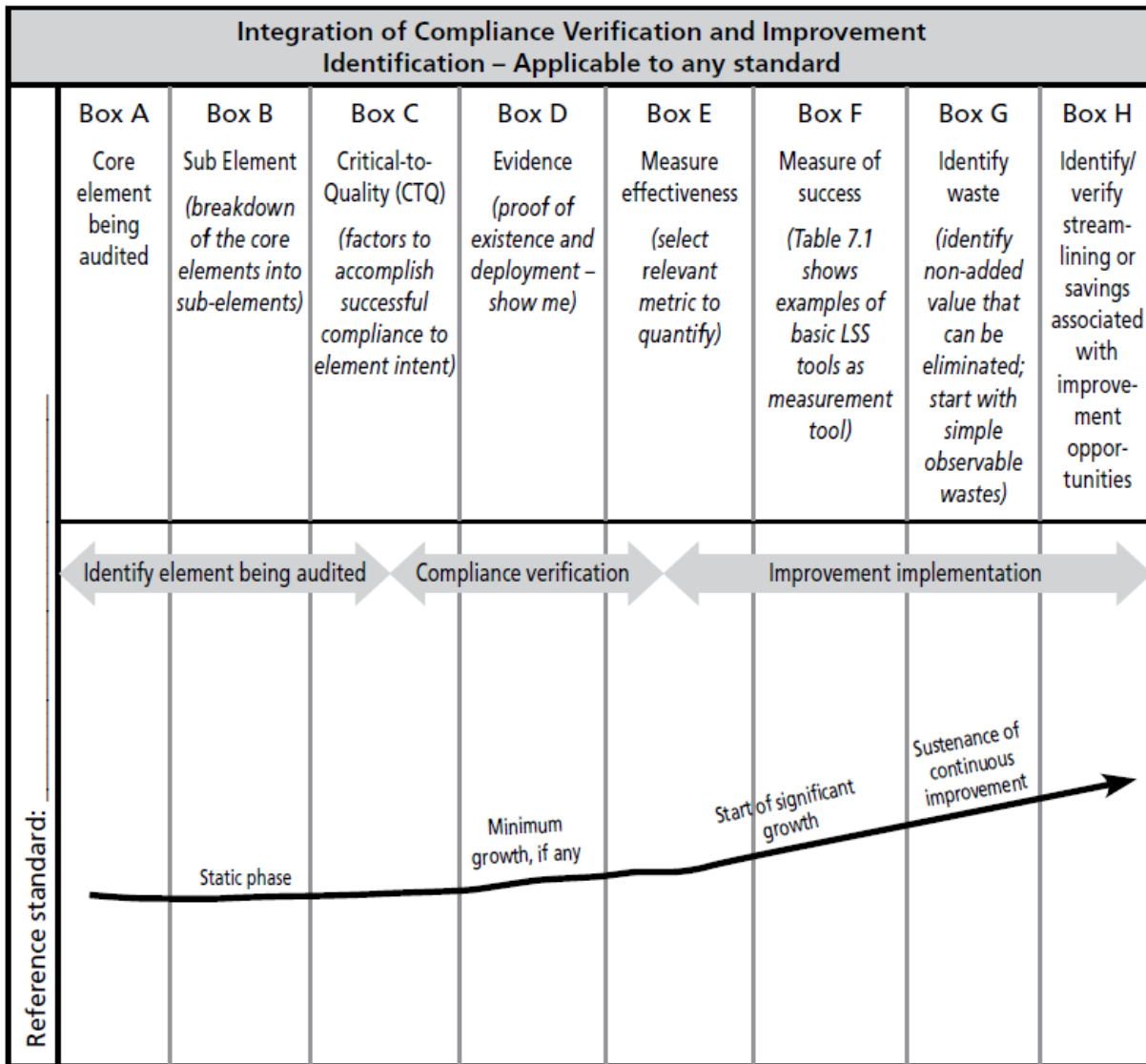
Surveys, self-assessments, and review programs are conducted to ensure that S&S systems and processes at facilities/sites are operating in compliance with Departmental and national-level policies, requirements, standards, and approved deviations for the protection of security assets and interests. Without 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 local S&S mission elements. 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.

Surveys and self-assessments must focus on both performance and compliance. When possible, the survey and self-assessment efforts must ensure compliance with requirements and performance of personnel and systems demonstrating that Departmental and national assets are protected; and that resources are used responsibly, and in the best interest of the nation. For this reason, survey and self-assessment teams shall be familiar with basic survey techniques as well as process improvement techniques, some of which are presented in this document. As there are many available improvement techniques those presented in this document are only some of the recommended options the site may elect to adopt. The Portable Universal Quality System described in *Auditing Beyond Compliance* by Janet Bautista Smith, outlines at a high level how this process of assessing performance could work as shown in Figure 8.1



**Figure 8:1 Portable Universal Quality System Audit Template**

S&S programs have traditionally been considered to be logically divided into topical areas and, within each topical area, sub-elements known as sub-topical areas. 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 topical areas and sub-topical areas are reflected on the DOE Form 470.8, *Survey/Inspection Report Form* (see Attachment 2), and this topical area and sub-topical area structure or a similar format shall 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 SSIMS. Modifications of this form might be

beneficial to capture site-specific information but shall allow for entry of information into SSIMS at least at the topical area level where applicable.

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.

## **9.0 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 S&S directives that apply at each facility, and the past performance of each facility on previous surveys, facility self-assessments, and recent external reviews.

### **9.1 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, a combination of the two, or as otherwise required in the interest of national security. Each activity conducting surveys or self-assessments shall 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 Minor Change 2. 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 topical area and sub-topical area as 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 must 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.

## **9.2 Planning a Facility Survey or Self-Assessment.**

Comprehensive survey and 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 shall 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.

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 include identifying personnel and other support requirements for all phases of the survey.

### **9.2.1 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. Aspects of the impact of these elements can be assessed qualitatively and quantitatively using a risk assessment process similar to that found in Attachment 1. This form of analysis can define what expertise is required for the assessment and on what topical areas the survey shall focus resources. Once this risk assessment is complete, the team leader develops an initial schedule and considers whether a preliminary visit is needed. To assist in the scheduling of the survey from pre-planning to completion of report, a survey checklist, like that presented in Attachment 3 Survey Prep and Report, Checklist, might be useful. Additionally, a survey/self-assessment plan is vital to ensuring a properly planned and executed survey, to capture at a high level the focus of the survey efforts (see Attachment 4, Survey Plan Template). As with many aspects of the survey/self-assessment process, the formality and comprehensiveness of information may vary based on the familiarity of the survey team and the facility or organization assessed.

### **9.2.2 Preliminary Coordination**

Before data collection begins, the following activities shall be conducted:

- Coordinating the proposed schedule with the site/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. (Refer to Attachment 6, *Data Call Information*)
- Conducting a team planning meeting;
- Establishing a schedule and topical area assignments;
- Gathering facility data (e.g., location, S&S interests, queries of SSIMS, EFOCI, and other databases 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, LOIs, 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. The communication formality vary based on the scope and relationship of the surveying team and the facility or organization. Attachment 5, Notification Memo, provides a formal notification memo sample. This sample may not benefit a self-assessment or survey of the local contractor performed by the federal staff.

### **9.2.3 Planning Survey and Self-Assessment Activities**

After completing the pre-planning and preliminary coordination activities, the team lead shall:

- Review data received from data call
- Review LOIs
- Review and assess SP for required information and note approved deviations to DOE policies (See Attachment 12. Note: Appendices B through H accompany Attachment 12 and otherwise have no bearing on this Technical Standard);
- Planning for performance tests, as needed
- Identify who to interview
- Determine what work to observe
- Associate data-collection methods with each line of inquiry chosen

## **10.0 SURVEY AND SELF-ASSESSMENT CONDUCT**

Valid sampling and accurate evaluation shall be the focus of all survey and self- assessment activities during the conduct of the review. This focus shall be apparent during all phases of the review activity so that, as far as possible, the review is a joint exercise between reviewers and reviewed to identify and correct program issues, with the goal of improving the local S&S program. Methodologies typically used to measure compliance include, but are not limited to, document review, testing, observation, and interviews. Effective planning, data collection, validation, and analysis of the information comprises the measurement of performance used to improve the local S&S program and may reduce the potential for differing opinions about the survey or self-assessment results. Additionally, the level of assessment beyond compliance may also be limited based on the authority conducting the assessment and the scope of their assessment.

### **10.1 In-Briefing**

A formal in-briefing has traditionally been the initial onsite 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 shall 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 shall 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;
- Outline schedule of events and communication such as end-of-day meetings, exit briefing date and time, expected completion date of report;
- General introductions of team members; and,
- Schedule of survey or self-assessment activities.

During this meeting or immediately following, the site subject matter experts and points of contact shall collaborate with survey team members to streamline communication and data gathering efforts.

## **10.2 Maintaining Communication**

The team leader and topical leads shall 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. The meetings ensure that the team leader and topical leads understand the status of data collection to meet the selected LOIs; understand information of interest for their respective topical area that was identified by other teams; and maintain an awareness of emerging concerns.

The team also shall 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.

## **10.3 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. This data should be shared

with the 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 shall always remain focused on the effectiveness of the entire S&S program in providing appropriate security for national security assets.

The selected LOIs 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. Attachment 7, Sample LOIs form will assist survey teams in the designation of order requirements that are critical to the effectiveness of the program. High-priority data-collection activities shall 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 shall 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 LOIs. 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 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 shall 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 CAPs 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 CAPs in a particular topical area shall 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, shall, 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.

### **10.3.1 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 shall 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 SNM or classified matter; they can be conducted to assess any portion of the facility security design. In all cases, they must focus on the elements of a topical area or sub-topical area that are critical to the effectiveness of that topical area or sub-topical area. Performance tests may also be in written form if the material is difficult or hazardous to test. 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 shall 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 shall 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. Attachment 8 provides a *Performance Test Safety Plan* template and Attachment 9 provides a *Performance Test Plan* template.

### 10.3.2 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. For this reason, it is preferable that two survey team members are present during data review.

Similarly, it is important for the team to share perceptions with site management on a periodic basis. The Survey or Self-Assessment Team Leader shall inform the Site management 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.

### 10.3.3 Data Analysis

After all data is collected and verified to be current and accurate, it shall 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 shall never be neglected in the final report. Key facts and the team analysis of them shall be documented in the report immediately before an observation or finding is made and additional supporting information, if any, shall 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 developed or 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 34-NOV-01-HQ-0123-SSIS-PM-001.18298, where 34-NOV-01 is the end 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 Minor Change 2, Appendix A, Section 2, paragraph 3), PM is the topical area in which the finding is made, 001 is a sequential number of the finding within the topical area, and 12898 is the facility code responsible for correcting the finding.

The terms finding, observation, opportunity for improvement (OFI), 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 term OFI. OFI 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 an OFI indicates that the review team has identified a potential program improvement which local security management might consider. Findings, observations, opportunities for improvement (OFI), or any other conclusion reached during data analysis shall be based upon validated data collected during the various activities comprising the review.

### 10.3.4 Ratings

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

The team leader, in consultation with topical leads and team members, shall determine the composite facility rating and the topical area and sub-topical area 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 area and sub-topical area ratings and an analysis of the relative importance of each topical area and sub-topical area in the overall protection design of the site/facility. As with each of the topical area and sub-topical area ratings, the logic and considerations leading to the award of the composite facility rating shall 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 and Not Applicable (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 topical area or sub-topical area shall be rated Satisfactory if all aspects of the topical area or sub-topical area 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 area or sub-topical area elements are providing the level of protection assumed in the approved site/facility security plan. In particular, any security element within the topical area or sub-topical area 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 topical area or sub-topical area shall 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 topical area or sub-topical area to

full capability or an approved plan to restore the security elements is being satisfactorily pursued. In some instances, a topical area or sub-topical area 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 topical area or sub-topical area 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 shall 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 topical area 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 topical area shall be rated no higher than Marginal.

Assignment of one or more sub-topical area 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 topical. If less-than-satisfactory sub-topical area ratings exist within a topical area rated Satisfactory, the survey or self-assessment report shall explain why the impact of these sub-topical area ratings do not justify a reduced topical area rating.

A topical area or sub-topical area shall be rated Unsatisfactory if limited compliance with the approved security plan and/or performance testing results indicate that the topical area or sub-topical area contributions to the approved security plan fall short of the performance required to protect security assets. Performance shall 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 topical areas and sub-topical areas, 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 area 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.

#### **10.4 Exit Briefing**

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

- Program findings, observations, OFI, and strengths;
- Corrective action reporting requirements for all open findings, regardless of source; and,
- Topical area, sub-topical area, and facility ratings.

The team leader shall 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 shall 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 must be documented in writing as soon as possible.

#### **11.0 REPORT PREPARATION**

As soon as possible after the survey or self-assessment is completed, a formal report of the results shall be finalized, Appendix A provides an extensive sample report format. The individual team members and topical area and sub-topical leads shall 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 shall 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 shall 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 shall 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.

When possible and appropriate, the appointing authority responsible for the conduct of the survey or self-assessment shall 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 shall 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 shall document and file lessons learned. These lessons learned shall identify what processes were effective, observations of team dynamics, and specific recommendations for the next review. The team leader shall include lessons learned as reported by topical leads and their teams. These lessons learned shall be provided to the appointing authority for information and evaluation to improve the survey process.

## **12.0 ISSUES MANAGEMENT PROGRAM**

A survey or self-assessment activity only fulfills a portion of its objective if the reviewed organization lacks a robust issues management process. DOE directives require DOE organizations to have an issues management process that is capable of categorizing findings based on risk and priority, to ensure relevant line management findings are effectively communicated to the contractors, and ensure problems are evaluated and corrected on a timely basis.

The issues management process, at a minimum, shall include the following for issues categorized as high significance findings:

- A thorough analysis of the underlying causal factors;
- Implementation of identified corrective action(s)/CAP that address the cause(s) of the findings to prevent recurrence;
- An effectiveness review conducted by trained and qualified personnel to verify the corrective action/CAP was effectively implemented and prevented recurrences. The review shall include the following:
  - documentation of the analysis process and the results of identified underlying causal factors
  - maintenance tracking, in a readily accessible system, of corrective actions/CAPs; including schedules for the effectiveness reviews;
- Appointment of a mutually agreed upon lead office when findings and/or corrective actions apply to more than one Program Secretarial Office/Departmental Element

## 12.1 Corrective Action Program

Findings are deficiencies that warrant a high level of attention on the part of management. If a finding is left uncorrected, it could adversely affect the DOE mission, the environment, worker safety or health, the public or national security. Findings define the specific nature of the deficiency, whether it is localized or indicative of a systemic problem, and identify which organization is responsible for corrective actions. A corrective action program shall include, at a minimum:

- Causal analysis appropriate to the complexity of the issue identified (the rigor of causal analysis must 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) Attachment 11 *Corrective Action and Causal Analysis* provides helpful examples for forms and a process for defining the root cause analysis;
- 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 must 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.



## 12.2 Process Improvement

When the scope of the survey and resources allow, assessing the effectiveness of the program and identifying resource savings is the desirable outcome of a survey. While compliance audits have a place in the protection of nuclear assets, personnel, and classified matter, performance effectiveness is ensuring the required protection is present while making the best use of resources and expertise. When time permits, the process outlined below shall be completed and submitted as part of the final report. As this effort requires resources and a focus on program management, the assessment team shall never conduct these efforts without support by the managers of the program assessed. Review of this level is time consuming and resource intense; it is not beneficial or expected that survey teams assess every topical area and sub-topical area. Process improvement shall focus on those topical area and sub-topical areas that have the greatest impact to security and the most potential for saved resources.

The steps to process improvement and the tools provided below align to this concept. The five steps of the survey process improvement technique are:

- Step 1. understanding and map the current process;
- Step 2, complete a value added analysis;
- Step 3. develop an improved process;
- Step 4. update documentation and develop metrics; and
- Step 5. measure for success and return to step 1.

### 12.2.1 Step 1: Understand and Map the Current Process

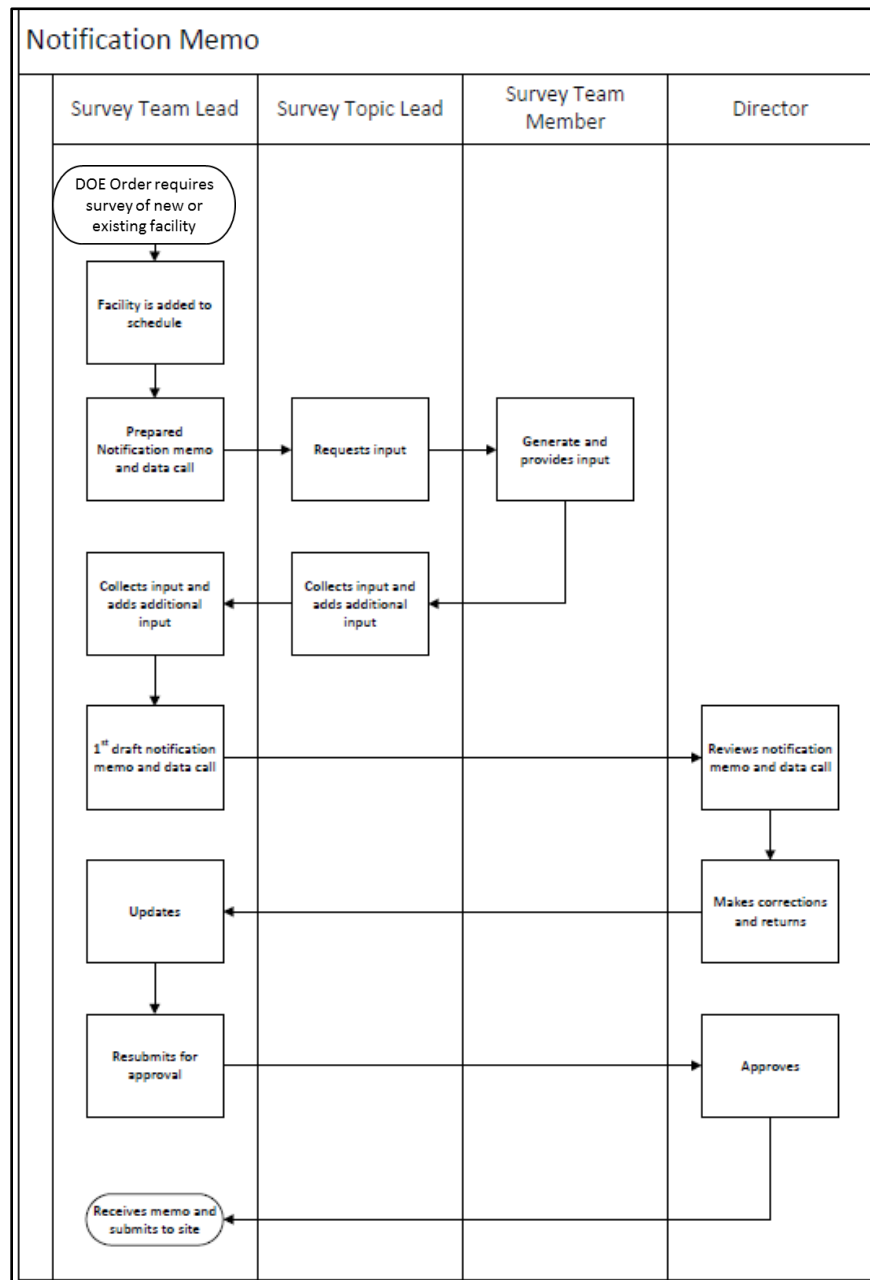
Survey team members work with subject matter experts to outline the process in a systematic method. This can work best in an outline form or in a flow chart such as the example below. There are numerous types of flowcharts and ways to complete the charts. The Cross Functional Flow chart was selected not only to document the flow information but also who was responsible, allowing for identification of information loops which impact the process.

There are a few basic steps and best practices that can help in describing and mapping the process:

- Form a team with members from any area or organization that provides inputs, manages, or contributes to the process. This helps ensure that all aspects of the process are considered and accounted for. Although not necessary, it may also be beneficial to get input from any downstream process owners.

- Identify the steps in the process. It is usually best to start with the beginning and end steps, including the inputs and outputs, and then work to fill in the steps in-between. It is very important to clearly define where the process being mapped begins and ends.
- Identify who owns each step, by job title and/or organization.
- Organize the steps in sequential order from beginning to end. Use this information to draw the baseline process map for the current process using whatever type of map the team has selected.

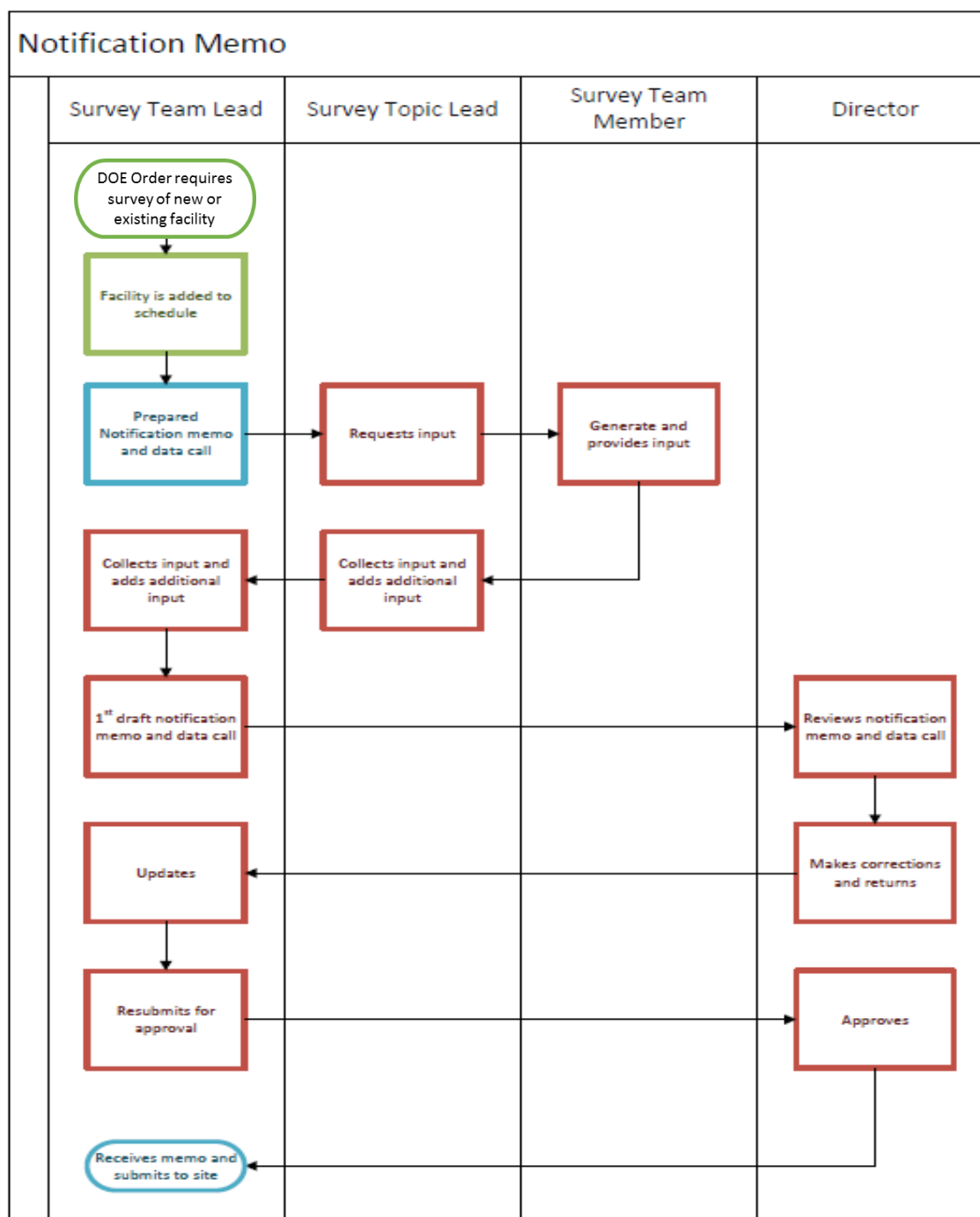
The example in Figure 12.1 maps the process to establish initial communication through a formal memo and data call as part of the initial planning.

**Figure 12:1 Initial Notification Memo Process Map****12.2.2 Step 2: Complete a Value Added Analysis**

Review the documented process identify in each step if it is specifically required by the order, performed to meet order requirements, or other. Analyze all steps identified as ‘other’ for whether they are inconsistencies, bottlenecks or are unnecessary, or whether the steps are necessary due to requirements, internal or external, outside of orders. Necessary/required steps should be analyzed further to determine if there are opportunities for optimization, such as improvements in efficiency or effectiveness through delegation of authority to an employee or deploying new technology.

Continuing with the example, Figure 12.2, below uses the colors green, blue, and red accordingly.

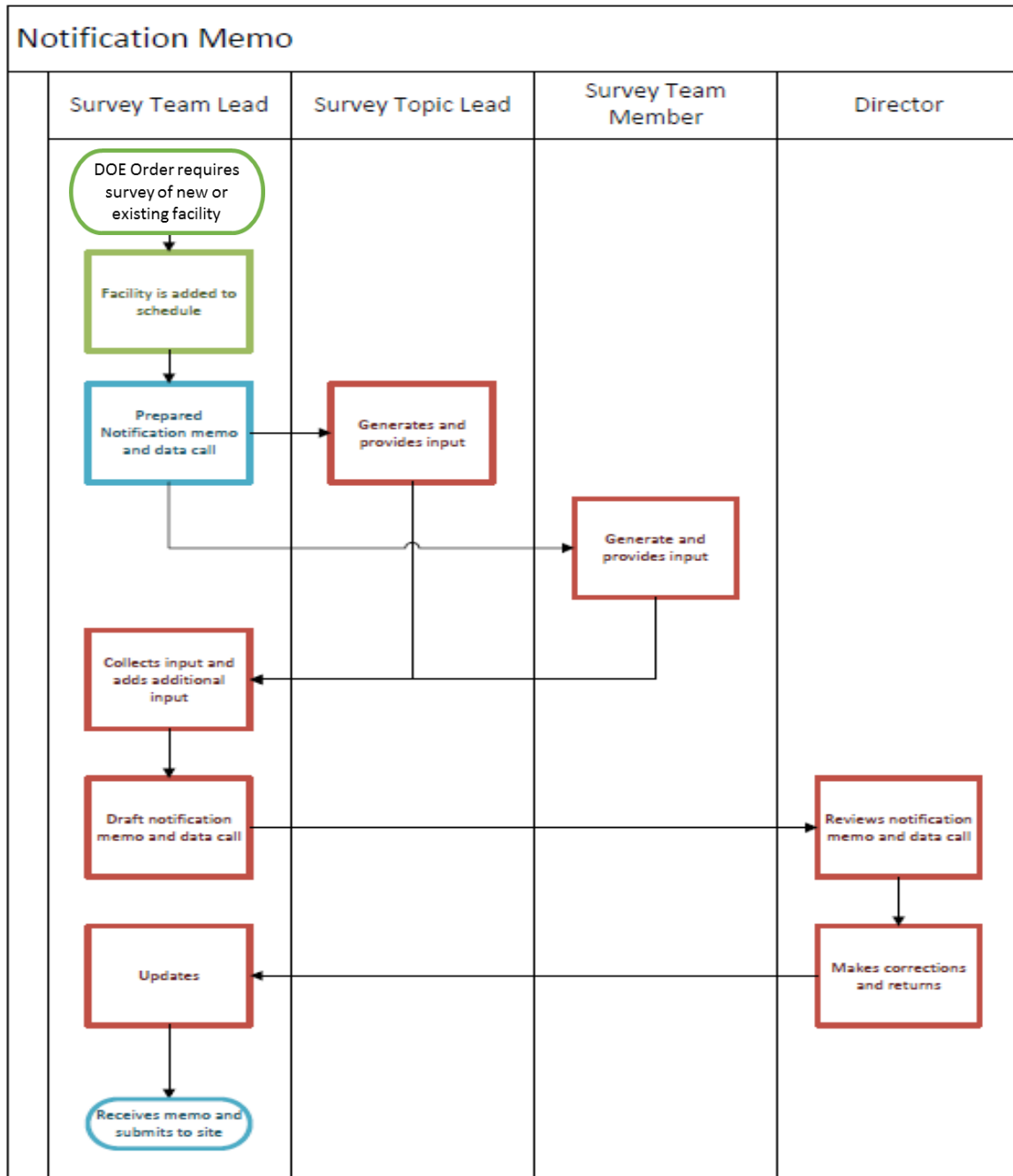
**Figure 12:2 Initial Notification Memo Color-Coded Process Map**



### 12.2.3 Step 3: Develop an Improved Process

All steps required by order or to meet order requirements must be retained in the improved process. Remove all steps determined to be unnecessary. Revise all other steps determined to be necessary/required, incorporating any optimization and/or new owners identified in Step 2. Reconnect all of the required and necessary steps in sequential order from beginning to end, and draw the improved process map, below in Figure 12.3.

**Figure 12:3 Notification Memo Improved Process Map**



**12.2.4 Step 4: Update Documentation and Develop Metrics**

Using the new process, update standard operating procedures and desktop procedures to align with the improved process. Ensure that leadership and employees are aware of the proposed process. Although the survey team and subject matter experts have developed this process there may be resource constraints or impact to other programs with which they are not aware. Additionally, develop qualitative or quantitative metrics to ensure the process is actually successful. Measurements such as time, money, space are all very quantifiable although subjective measures such as employee and customer delight should not be ignored.

**12.2.5 Step 5: Measure for Success and Return to Step 1.**

At this stage, the process has been turned over to the responsible process owners and subject matter experts, who will monitor the process for efficiency and effectiveness. Additional support from the survey team may be necessary if the new process experiences problems, or if further optimization is possible or necessary. If this is the case, the 5-step process improvement technique can be repeated, beginning again at Step 1.

**ATTACHMENT 1: RISK BASED ASSESSMENT SCHEDULING PROCESS**

Topical Area	Sub-Topical Area	Rating Elements (Scale 1 - 5)						Final Score
		1. Program is Document Focused or Work Focused	2. Element is established and not changing	3. New Leadership	4. New Order	5. Findings/Issues Identified previous year	6. Other Ancillary assessment conducted	
						7. Essential Element of S&S Protection 8. Impact to safety, security, or resources if fails	9. EA reported field findings and issues	Score less than 21 ancillary assessment activities will monitor. Score 23 - 30 minimal survey effort will be conducted (ex. Document review, interview process owner). Score greater than 30 complete survey effort will be conducted (includes document review, multiple interviews, observation of work activities and performance testing where applicable)
<b>Program Planning &amp; Management</b>								
	S&S Program Planning							0
	Security Plans							0
	Security Conditions							0
	Performance Assurance							0
	Survey, Review, and Self-Assessment Programs							0
	Facility Clearances and Registration of S&S Activities							0
	Foreign Ownership, Control, or Influence Programs							0
	S&S Awareness							0
	Incidents of Security Concern							0
	Control of Classified Visits							0
	S&S Training Program							0
	Technology Transfer							0
	Tactical Doctrine							0
<b>Protective Force</b>								
	Management							0
	Training							0
	Administration							0
	Security Officers							0
	Security Police Officers (Fixed Post)							0
	Security Police Officers I							0
	Security Police Officers II							0
	Security Police Officers III							0
	Firearms Training							0
	Firearms Operations							0
	Firearms Qualification							0
	Operational Assurance							0
	Special Response Team							0
	Helicopter Operations							0
	Guidelines for Legal Authority/Fresh Pursuit and ROE							0
	Performance Testing							0
	Canine Program							0
	Demonstrator and Protestor Plan							0
	Workplace Violence and Active Shooter Plan							0

<b>Personnel Security</b>		General Requirements						0
		Reciprocity						0
		Personnel Security Quality Training						0
		Personnel Security Files						0
		Adjudicative Considerations Related to Statutory Requirements and Departmental Requirements						0
		Security Clearance Requests/Justification and Access Authorization						0
		Limited Access for Non-US Citizens						0
		Temporary Security Clearance Upgrades And Interim Security Clearances						0
		Reporting Requirements						0
		Human Reliability Program						0
		Workplace Substance Abuse Programs at DOE Sites						0
		Procedures for Determining Eligibility for Access to Classified Matter and SNM						0
<b>Physical Protection:</b>								
		Protection Planning						0
		Security Areas						0
		Posting Notices						0
		Locks And Keys						0
		Maintenance						0
		Barriers						0
		Communications, Electrical Power and Lighting						0
		Secure Storage						0
		Intrusion Detection and Assessment Systems						0
		Entry/Exit Screening						0
		DOE Security Badge Credential and Shield Program						0
		Protection of CAT III/IV SNM						0
		Transportation Security						0
		Protective Force Posts						0
		Safeguards and Security Alarm Management and Control System						0
<b>Information Security</b>								
		General Requirements						0
		Handling And Protection						0
		Foreign Government Information						0
		Release or Disclosure of US Classified Information to Foreign Governments						0
		Disclosure and Release in Emergency Situations						0
		Operations Security						0
		Technical Security Program						0
<b>Unclassified Foreign Visitors and Assignment Program</b>								
		Documentation						0
		Lawful Immigration Status, Citizenship, and Identity						0
		Security Plans						0
		Indices Checks						0
		Access Approval						0
		Grated Approach						0
<b>Nuclear Material Control and Accountability</b>								
		General Requirements						0
		Nuclear Material Management and Safeguards System Reporting						0
		Termination of Safeguards						0



1. Program is Document Focused
  - 1 Program is primarily used to develop a document (example, Vulnerability Analysis (VA))
  - 2 Program is focused on more documentation but has elements of physical work activities (example, SECON)
  - 3 Program is a blend of document and physical work (example, Survey Program)
  - 4 Program is focused more on physical work activities with some elements of documentation review (example, PAP)
  - 5 Program is primarily a physical work program (example, Firearms Qualification)
2. Element is established and not changing
  - 1 The program or element is greater than 10 years old (example, the PPA boundary identified at the fence line for Germantown)
  - 2 The program or element is 5 - 10 years old
  - 3 The program or element is 3 - 5 years old
  - 4 The program element is 1 - 3 years old (example, Performance Assurance Program)
  - 5 The program element is less than 5 years old (example, DBT implementation)
3. New leadership, senior person immediately responsible for the program
  - 1 Leadership establish greater than 5 years
  - 2 Leadership established between 3 and 5 years
  - 3 Leadership established between 1 and 3 years
  - 4 Leadership established for less than 1 years
  - 5 Leadership established for less than 6 months
4. New order (Order can also be procedure or process depending on the impact of the document)
  - 1 Document established greater than 5 years
  - 2 Document established greater between 3 and 5 years
  - 3 Document established between 1 and 3 years
  - 4 Document established for less than 1 year
  - 5 Document established for less than 6 months
5. Findings/issues identified previous year (findings or issues must require CAPS, these are not recommendations or opportunities for improvement)
  - 1 Minor document updates
  - 2 Issues require resource attention but not a complete change of the program
  - 3 Program is functioning but not meeting the intent of the order
  - 4 Program is established on paper but not functioning
  - 5 Lack of an entire program
6. LIR or other ancillary assessment conducted
  - 1 Other assessment activity fully reviews the program
  - 2 Requirements for the program are few, other assessment activities can address the major issues of the program
  - 3 Other assessment activities are effective but a formal survey may provide serious benefit
  - 4 Minor review through program, ancillary assessment activities conducted with no issues noted
  - 5 Program is broad and impacts many organizations, even though other assessment activities were conducted even a formal survey might not address all elements of the program
7. Essential element of S&S Protection
  - 5 Identified as an essential element in the VA/SRA process
8. Impact of safety, security, or resources if fails
  - 1 No impact, minor inconvenience
  - 2 First Aid rendered by employee, loss of OUO information, budget impact to AU-42
  - 3 Medical attention needed, loss of Confidential information, budget impact to AU-40
  - 4 Serious injury, loss of Secret information, budget impact to AU
  - 5 Major injury or death loss of Top Secret information, major budget impact to AU
9. EA reported field findings/issues
  - 1 No issue reported
  - 2 Adverse single occurrence
  - 3 Adverse emerging trend but minor in impact
  - 4 Adverse emerging trend major impact
  - 5 Previously reported adverse continuing trend

**ATTACHMENT 2: DOE FORM 470.8 SURVEY/INSPECTION REPORT FORM**

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: <input type="radio"/> Initial <input type="radio"/> Periodic <input type="radio"/> Special <input type="radio"/> Termination <input type="radio"/> EA Reviews: <input type="radio"/> NPR <input type="radio"/> EPR <input type="radio"/> Self-Assessment		2. Report #:	
3. Facility Name:		4. a. Facility Code:	
		b. RIS Code:	
5. Survey Date(s):	6. a. Findings: <input type="radio"/> Yes <input type="radio"/> No b. Findings Against Other Facilities:		7. Composite Rating:
8. Previous Survey Date(s): Next Survey Date:	9. Unresolved Findings: <input type="radio"/> Yes <input type="radio"/> No		10. Previous Rating:
11a. Surveying Office:	11b. Cognizant Security Office:		11c. Other Offices with Interests:
<div style="display: flex; justify-content: space-between;"> <div style="width: 48%;"> <p>12. Ratings:</p> <p>a) PROGRAM MANAGEMENT OPERATIONS</p> <p>PROTECTION PROGRAM MANAGEMENT</p> <p>Program Management and Administration _____</p> <p>Resources and Budgeting _____</p> <p>Personnel Development and Training _____</p> <p>S&amp;S PLANNING AND PROCEDURES _____</p> <p>MANAGEMENT CONTROL _____</p> <p>Surveys and Self Assessment Programs _____</p> <p>Performance Assurance Program _____</p> <p>Resolution of Findings _____</p> <p>Incident Reporting and Management _____</p> <p>PROGRAM WIDE SUPPORT _____</p> <p>Facility Approval and Registration of Activities _____</p> <p>Foreign Ownership, Control or Influence _____</p> <p>Security Management in Contracting _____</p> <p style="text-align: right;">OVERALL RATING _____</p> <p>b) PROTECTIVE FORCE</p> <p>MANAGEMENT _____</p> <p>TRAINING _____</p> <p>DUTIES _____</p> <p>FACILITIES AND EQUIPMENT _____</p> <p style="text-align: right;">OVERALL RATING _____</p> <p>c) PHYSICAL PROTECTION</p> <p>ACCESS CONTROLS _____</p> <p>INTRUSION DETECTION &amp; ASSESSMENT SYSTEMS _____</p> <p>BARRIERS AND DELAY MECHANISMS _____</p> <p>TESTING AND MAINTENANCE _____</p> <p>COMMUNICATIONS _____</p> <p style="text-align: right;">OVERALL RATING _____</p> </div> <div style="width: 48%;"> <p>d) INFORMATION SECURITY</p> <p>BASIC REQUIREMENTS _____</p> <p>TECHNICAL SURVEILLANCE COUNTERMEASURES _____</p> <p>OPERATIONS SECURITY _____</p> <p>CLASSIFICATION GUIDANCE _____</p> <p>CLASSIFIED MATTER PROTECTION &amp; CONTROL _____</p> <p>Control of Classified Matter _____</p> <p>Special Access Programs and Intelligence Information _____</p> <p style="text-align: right;">OVERALL RATING _____</p> <p>e) PERSONNEL SECURITY</p> <p>ACCESS AUTHORIZATIONS _____</p> <p>HUMAN RELIABILITY PROGRAMS _____</p> <p>CONTROL OF CLASSIFIED VISITS _____</p> <p>SAFEGUARDS AND SECURITY AWARENESS _____</p> <p style="text-align: right;">OVERALL RATING _____</p> <p>f) MATERIALS CONTROL &amp; ACCOUNTABILITY</p> <p>PROGRAM MANAGEMENT _____</p> <p>MATERIAL ACCOUNTABILITY _____</p> <p>MATERIALS CONTROL _____</p> <p>MEASUREMENT _____</p> <p>PHYSICAL INVENTORY _____</p> <p style="text-align: right;">OVERALL RATING _____</p> <p>g) FOREIGN VISITS AND ASSIGNMENTS</p> <p>SPONSOR PROGRAM MANAGEMENT &amp; ADMIN _____</p> <p>COUNTERINTELLIGENCE REQUIREMENTS _____</p> <p>EXPORT CONTROLS/TECH TRANSFER REQUIREMENTS _____</p> <p>SECURITY REQUIREMENTS _____</p> <p>APPROVALS AND REPORTING _____</p> <p style="text-align: right;">OVERALL RATING _____</p> </div> </div>			
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

**ATTACHMENT 3: .SURVEY PREPPARATION AND REPORT CHECKLIST**Survey Site: \_\_\_\_\_Travel Dates: \_\_\_\_\_Survey Date: \_\_\_\_\_Team Members:

<b>Survey Prep</b>	<b>TM</b>	<b>✓</b>	<b>ECD</b>	<b>COMMENTS</b>
Contact Site POC to establish date of assessment (70 days prior)				
Draft Data Call Memo (65 days prior)				
Forward Final Data Call Memo to Site POC (50 days prior)				
Review previous survey report (30 days prior)				
Review previous areas of Concerns/Findings (30 days prior)				
Review CAPS (30 days prior)				
Using previous information and data call develop Site-Specific LOIs for Topical area Areas (20 days prior)				
Develop survey timeline (15 days prior)				
Request CPCI Listing from PerSec				
Request Incident Reports from Security Officer				
Forward timeline for site approval (10 days prior)				
Coordinate interviews with site POC (10 days prior)				
Coordinate performance testing with site POC (10 days prior)				
Send site final LOIs (5 days prior)				
In-brief presentation (first day)				
Conduct assessment activities				
Out-brief presentation (last day)				

<b>Drafting Report/Review</b>		✓	ECD	COMMENTS
Initial Draft Team Member: (30 days)				
Reviewing Team Member: (10 days)				
Final Reviewing Team Member: (10 days)				
Team Lead: (5 days)				
Initial Draft Team Member reconciles Team Lead comments (5 days)				
Contract POC: (10 days)				
Team reconciles Contract POC comments (10 days)				
Program Manager: (10 days)				
Team reconciles Program Manager comments (10 days)				
Submit report to Admin for correction and submission for approval				
Input issues into Survey database (5 days)				
Input Findings into SSIMS (5 days)				
<b>Report Attachments</b>		✓		COMMENTS
Survey Report Cover Memo (5 days)				
DOE Form 470.8 Report Form				
DOE Form 470.1 CSCS				
DOE Form 470.2 FDAR				
Open Findings (SSIMS)				

**ATTACHMENT 4: SURVEY PLAN TEMPLATE**

1. Title of survey
2. Location of facility
3. Purpose of survey
4. Survey dates
5. General site/facility information /description
  - a. Site/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

**ATTACHMENT 5: NOTIFICATION MEMO**

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). 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 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 6: DATA CALL INFORMATION

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

(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 supported by the initial risk assessment (Attachment 1), as outlined in the survey plan. The list is not comprehensive; other documents may be available which shall also be considered)

a. Program Planning and Management

- 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
- Site/Facility 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 training 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 Analysis (VA) reports
- Security Risk Assessment (SRA) reports
- Contingency plans
- Survey and self-assessment program procedures
- Issues management plans and procedures
- CAPs 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

b. 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)
  - Site/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

c. 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
- d. 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
  - TSCM Officer (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)
- e. 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 CAPs
  - 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, shall be compared for discrepancies.
- f. Insider Threat Program (ITP)
- Local Insider Threat Working Group (LITWG) charter

- ITP Standard Operating Procedures (SOP) or other guidance
- ITP records management procedures
- Name/Position/Title of LITWG Chair
- List of LITWG members
- ITP Training Records for Cleared Employees
- Copies of ITP Training and Awareness Materials

g. Foreign Visitors 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

h. 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

**ATTACHMENT 7: SAMPLE LINE OF INQUIRY FORM****UNCLASSIFIED UNTIL FILLED IN, THEN HANDLE APPROPRIATELY**

## Line of Inquiry for S&amp;S Program Management Topic

SAFEGUARDS AND SECURITY PROGRAM					
Requirement	Notes				
	Yes:	Scale:	No:	Impact:	DNA/NA:
	Yes:	Scale:	No:	Impact:	DNA/NA:
	Yes:	Scale:	No:	Impact:	DNA/NA:

Scale: Level of compliance with the order. (1) = Compliant. (2) = Noteworthy. (3) = Best Practice.

Impact: Level of the effect of noncompliance. (1) = No threat to security interests, ex: documentation issue. (2) = Minor impact to security interests, ex: not all essential elements are performance tested. (3) = Major impact to security interests, ex: classified material is not secure a the end of day.

Page 1 of 1

**UNCLASSIFIED UNTIL FILLED IN, THEN HANDLE APPROPRIATELY**

---

## ATTACHMENT 8: PERFORMANCE TEST SAFETY PLAN EXAMPLE

### 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 shall be signed and returned no later than \_\_\_\_\_.

Name \_\_\_\_\_

Signature \_\_\_\_\_

Position \_\_\_\_\_

Date \_\_\_\_\_

(1) Detection of Contraband and Prohibited Items

(Type of Performance Test)

(2) Ongoing 365 Days per Year; 24 Hours per Day

(Performance Test Date and Time)

(3) Detection of Contraband and Prohibited Items, John Doe

(Safety Plan Name and Person Preparing)

(4) ALL LIMITED SCOPE PERFORMANCE TESTS (LSPTs) WILL BE CONDUCTED IN CONFORMANCE WITH THIS SAFETY PLAN AND ONLY AFTER SPECIFIC APPROVAL TO CONDUCT THE LSPTs 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, Vault-Type Room, 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.

(5) 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

(6) 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 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.

(7) 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.

(8) 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:

(9) Off-Limit Areas:

- ☐ Applicable
- ☒ Not applicable

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

(10) Safety Equipment:

- ☐ Controller Radios
- ☐ PF Radios
- ☐ Orange Vests
- ☐ "Glow Sticks"
- ☐ First Aid Kit
- ☐ Other required safety equipment:

(11) Specific Safety Hazards Not Covered Elsewhere:

- ☐ Applicable
- ☒ 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.

(12) Radiation Safety Provisions:

- ☐ Applicable
- ☒ 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:

(13) 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.

(14) Protective Force Appendix Required:

\_\_\_\_\_ Yes

X No

(15) 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:

Director, Safety and Health Organization  
DOE Cognizant Security Office

Date

Contractor Safety and Health Representative

Date

Director, Security Organization  
DOE Cognizant Security Office

Date

**ATTACHMENT 9: PERFORMANCE TEST PLAN****(1) TEST OBJECTIVE**

This performance test is designed to test individual employee response to finding an unattended Secret Restricted Data (SRD) document, verify compliance with the notification process to Classified Document Control Office (CDCO), and verify PF compliance with the procedure for responding to this incident.

**(2) 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.

**(3) TEST METHODOLOGY AND EVALUATION CRITERIA**

a. 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.

b. 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) Xxxx
- b) Xxxx
- c) Xxxx

**(4) PASS/FAIL CRITERIA**

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

- CDCO 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.



**(5) 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.

**(6) 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:
  1. Monitor the document
  2. Monitor the PF response
  3. Monitor the CDCO

**(7) 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.

**(8) 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.

**(9) COMPENSATORY MEASURES**

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

**(10) 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.

**(11) 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)

**ATTACHMENT 10: SAMPLE SURVEY REPORT TEMPLATE****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, shall be included in the report.
- B. Report Content.
1. Initial and Periodic Survey Reports and Self-Assessment Reports. Reports shall contain the following items.
    - (a) An executive summary containing:
      - i. The scope, methodology, period of coverage, duration, date of the exit briefing to management;
      - ii. 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);
      - iii. 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;
      - iv. The overall composite facility rating with supporting rationale; and
      - v. A reference to a list of findings identified during the survey or self- assessment.
    - (b) An introduction containing:
      - i. The scope, methodology, period of coverage, duration, date of the exit briefing to management; and
      - ii. 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 area and sub-topical areas that includes:
      - i. A description of the site's implementation of the topical area/sub-topical area element;

- ii. The scope of the evaluation;
        - iii. A description of activities conducted;
        - iv. The evaluation results and associated issues (including other Department elements or other government agency (OGA) review or inspection results related to the topical areas/sub-topical areas that were included in the survey);
        - v. 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
        - vi. An analysis that provides a justification and rationale of the factors responsible for the rating.
- (d) Attachments, including, for example:
  - i. A copy of the current DOE F 470.2, Facility Data and Approval Record (FDAR);
  - ii. A listing of all active DOE F 470.1, Contract Security Classification Specification (CSCS), or DD F 254, Contract Security Classification Specification;
  - iii. A listing of all new findings resulting from the survey/self-assessment;
  - iv. A listing of all previous findings that are open, to include the current status of corrective actions;
  - v. A listing of team members including names, employer, and their assigned area(s) of evaluation; and
  - vi. A listing of all source documentation used to support the survey/self- assessment conduct and results.

Narrative: The narrative section of the report shall 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 shall 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 shall reflect the compliance and performance segments of the survey. Reports shall 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 must be identified. Open findings from the previous survey shall 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 shall be included in the body of the narrative.
- Findings, observations, opportunities for improvement, and suggestions, along with supporting data for each, shall 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 shall correlate to the survey results and establish the basis for the ratings. The survey report shall reflect validated and defensible ratings. The narrative description shall be consistent with and support the composite and topical area ratings (including “Does Not Apply”).
- The report shall identify findings corrected on the spot. These findings and corrective actions shall be clearly described in the narrative.
- The status of corrective actions for open findings and findings from the previous survey shall be included in the narrative.
- A concluding analysis of each topical area shall be included in the narrative.
- Reasons for a less-than-satisfactory rating shall be explained in detail.

**ATTACHMENT 11: CORRECTIVE ACTION AND CAUSAL ANALYSIS**

<b>PART I</b>	
<b>CORRECTIVE ACTION ELEMENTS</b>	
<b>Action Plan Cover Sheet</b>	
<b>Finding Number:</b>	<b>Facility Code:</b>
<b>Responsible Program Office:</b>	
<b>Topical Area:</b>	<b>Sub-topical Area:</b>
<b>Reference(s) (i.e., Orders, Requirements, etc.):</b>	
<b>Description of Deficiency:</b>	
Information above provided by Surveying organization	
<b>PART II</b>	
<b>Root Cause Analysis Process Used:</b>	
<b>Cause Code(s):</b>	
<b>Corrective Action Description:</b>	

<b>Estimated Completion Date:</b>		
<b>Revised Completion Date:</b>		
<b>Reason for Revised Completion Date:</b>		
<b>Completion Date:</b>		
<b>Responsible Manager:</b>		
Print Name	Signature	Date

### Instructions for Completing Corrective Action Plan Cover Sheet

The Surveying Organization will fill in Part I of the Corrective Action Plan Cover Sheet. The organization assigned the finding will be responsible for completing Part II of the form.

PART II		
<p><b>Root Cause Analysis Process Used:</b> <i>Identify the technique used to identify the Cause Code. There are a number of acceptable tools to include but not limited to, the five whys, fishbone, tree, failure modes effects analysis. The preferred tool is the fishbone chart as well as using the causal analysis tree to help in identifying the root cause outlined below. Please attach the completed tool(s) showing how the root cause was identified.</i></p>		
<p><b>Cause Code(s):</b> <i>Cause code identified by Root Cause Analysis, code, description, and examples are available in DOE-STD-1197-2011 Occurrence Reporting Causal Analysis. More than one code is acceptable but not common, except if one of the codes is human error, which is generally supported by a second code.</i></p>		
<p><b>Corrective Action Description:</b> <i>High-level description of corrective action to include compensatory measures required. Milestones (numbered) are to be included in the Corrective Action Description section of the cover sheet, or at a minimum, reference that there are "X" number of milestones to be met in completing the corrective action.</i></p>		
<p><b>Estimated Completion Date:</b> <i>First expected completion date assuming all resources are available and the corrective action activities are not disrupted.</i></p>		
<p><b>Revised Completion Date:</b> <i>Update completion date, initial form submission will not have information in this block, however additional submissions may include adjustments required by a delay in corrective action efforts.</i></p>		
<p><b>Reason for Revised Completion Date:</b> <i>A brief narrative on why the date must be revised, not for the purposes of approval by the surveying organization but for informational purposes.</i></p>		
<p><b>Completion Date:</b> <i>Date the corrective action was completed, necessary so surveying organization can review the effectiveness of the efforts implemented.</i></p>		
<p><b>Responsible Manager:</b> <i>Information by responsible manager for completing the corrective action.</i></p>		
Print Name	Signature	Date



<b>CORRECTIVE ACTION PLAN MILESTONES SHEET</b>	
<b>Finding Number:</b>	<b>Date:</b>
<b><u>Milestone:</u></b> <b><u>No.:</u></b>	
<b><u>Milestone Description:</u></b>	
<b><u>Deliverables/Completion Criteria:</u></b>	
<b>Milestone Due Date:</b>	<b>Date Milestone Completed:</b>
<b>Milestone Manager (print and sign):</b>	
<b><u>Milestone:</u></b> <b><u>No.:</u></b>	
<b><u>Milestone Description:</u></b>	
<b><u>Deliverables/Completion Criteria:</u></b>	
<b>Milestone Due Date:</b>	<b>Date Milestone Completed:</b>
<b>Milestone Manager (print and sign):</b>	

### Instructions for Completing Corrective Action Plan Milestones Sheet

SECTION	INSTRUCTIONS
Finding Number	Enter the finding number.
Milestone Number	Enter milestone number (consecutive starting with 1).
Milestone Description	<ul style="list-style-type: none"> <li>• Write milestones with clear deliverables that solve the problem. Ensure that milestones address and correct the deficiency.</li> <li>• Limit individual milestone instructions to brief, concise statements describing logical segments of the specified milestone. Include milestones for recurrence control.</li> <li>• Write realistic and achievable milestones that can be verified.</li> <li>• Do not overextend milestones beyond your control. Ensure that resources are available.</li> <li>• Identify the milestone manager responsible for completion of each milestone and the respective program element.</li> <li>• Identify only one milestone if only a single action is required to correct the deficiency.</li> <li>• If completion of milestones is required by persons outside of the responsible manager's authority, the responsible manager coordinates the milestone with the supporting program element.</li> </ul>
Deliverables/ Completion Criteria	Include completion criteria that are discrete, finite, and verifiable.
Milestone Due Date	Enter the due date for each milestone.
Date Milestone Completed	Enter the actual date each milestone was completed.
Milestone Manager	Milestone managers sign for concurrence of each assigned milestone.

## Root Cause Scenario

**Background:** Carl has been a DOE employee for about 3 years, working in an office administrative position. Although he has a Q clearance, he very rarely handled classified documents in his position.

Another employee in his organization, the Classified Document Control Station (CDCS) custodian, was retiring soon and had given two weeks' notice. The position needed to be filled immediately due to the high volume of access the CDCS goes through each day. Shortly after his retirement, an annual inventory of all classified documents was scheduled to take place.

The Director tasked Carl's supervisor to fill this position as soon as possible. Since Carl has a clearance and is familiar with the organization, he was offered the new position as the CDCS Custodian. Carl was somewhat familiar on how to handle classified matter, but had not gone through CMPC training for CDCS training since there were no classes held at the time. Given his 3 years with DOE, the supervisor believed this would not be an issue and filling the position was more important due the upcoming inventory. The Director was not aware of the lack of training Carl had.

**Incident:** Carl has now been in this new position for about 3 weeks, and has been assisting with the inventory of the classified documents stored in the security containers in the CDCS. Carl was leaving early on Wednesday for a long weekend and would be out until the Monday of the following week. On his way out he told another employee, who was working on the inventory, that the SF 700 Part 2s were being stored in his desk drawer, in case they needed to access a security container.

**Problem:** SF 700 Part 2 was stored in an employee's desk drawer instead of a security container.

How the Root Cause Analysis was determined for this finding:

A Safeguards and Security Periodic Survey was conducted and a finding was assigned with a CAP response due within 30 days after survey date (example provided). The team involved in determining the root cause of the finding, consisted of the elements HSO, AHSO, and management not directly involved with the finding. The team reviewed and discussed the scenario above.

Interviews with the employees involved helped obtain additional information of the events leading up to the issuance of a finding. The team collected all the information and used the **Root Cause Tool 1** (see example) to determine the possible topical area where the root cause may fall under (i.e. A4 Management), which can be determined through group discussion. The **Casual Analysis Table** was used to assist with breaking down the root cause by topic. There were sections that did not apply to this situation, so the team placed a Not Applicable (N/A) in those sections. The team continued to work their way through all the levels of the table (A1-A7, and down through the "B's" and "C's" of each of those sections). Once the team has exhausted all possibilities, Root Cause Tool 1 was then complete. In filling in Tool 1, the group noticed that there is the potential to have

more than one root cause for each section (see ‘A4’ in example). If this happens then capture all suspected causes that apply.

After completing Root Cause Tool 1, the team analyzed the information to select the top or most critical issues. Once those were established, we transferred the selections over to the **Root Cause Tool 2** table under ‘Suspected Cause.’ The team then rated the Suspected Causes for ‘Areas of Impact’ in a scale of 1-5 (5 = Highest impact; 1 = Lowest impact). Once completed, we totaled up the ratings assigned to determine the overall score that had the greatest impact, giving us our root cause.

If there are two or more areas of impact that have the same scoring number then the Subject Matter Expert and the team shall discuss which area of impact outweighs the other. For example, if it is a matter of mission vs. resources, the team may decide to use the Mission Area of Impact number versus the resource number for this CAP. If the same finding occurs in the following year, then the organization may decide to use the resource areas of impact as the root cause for the finding. For this reason, all records that were used to determine root cause shall be retained to document the analysis that was conducted for each root cause.

Figure ATTM 11.1 Blank Root Cause Analysis Tool 1 Template

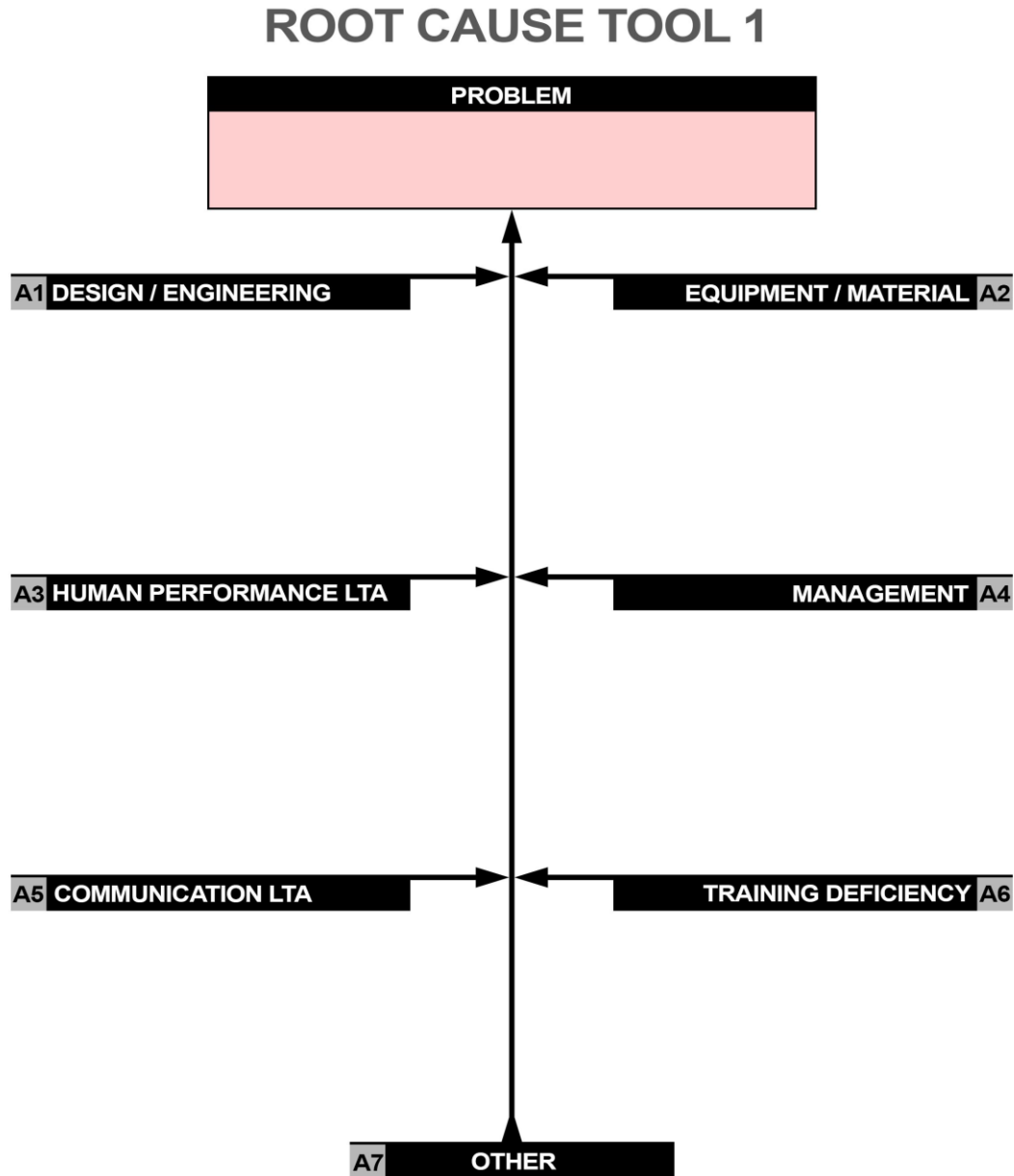
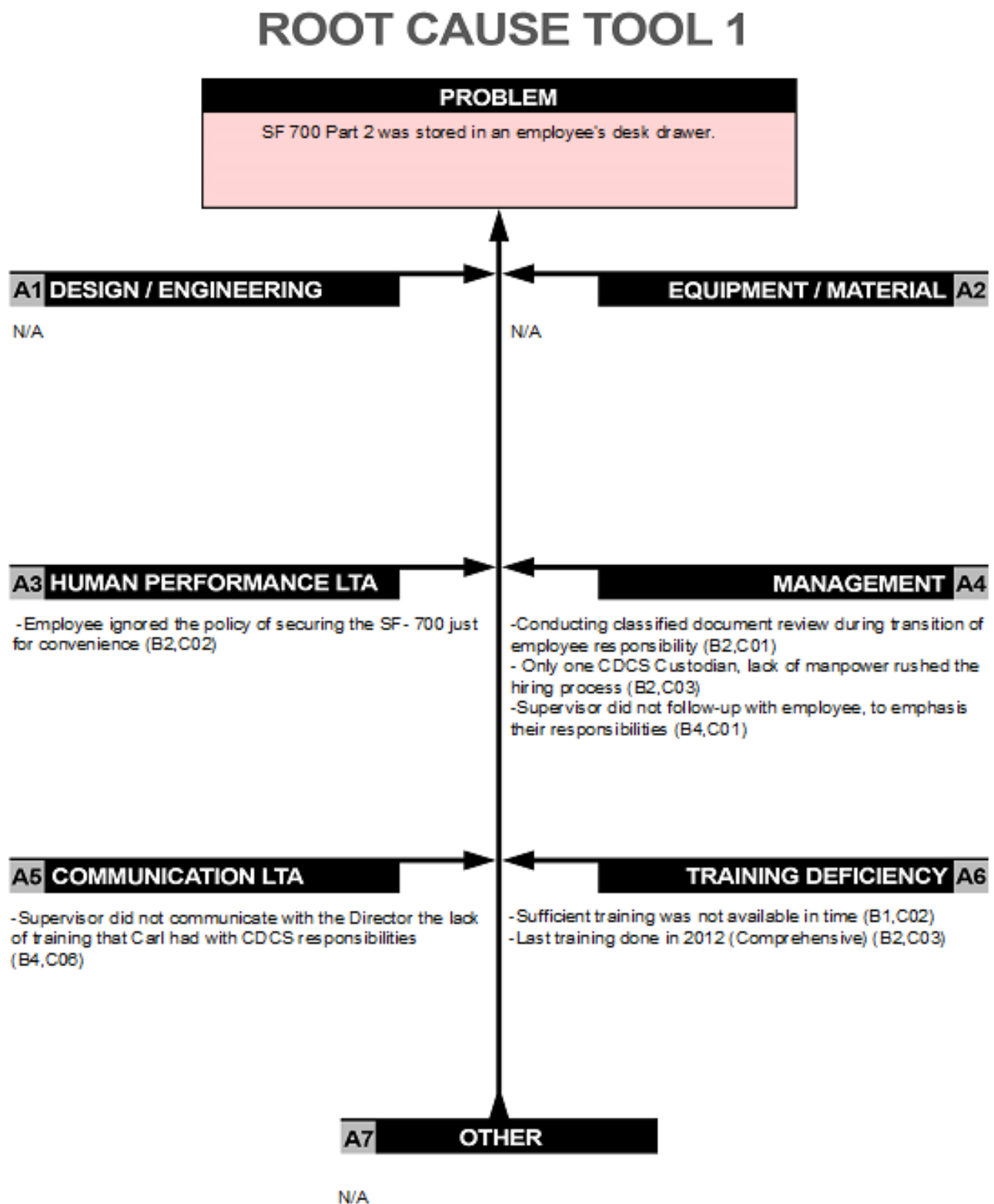


Figure ATTM 11. 2 Example of a Completed Root Cause Tool 1



**Figure ATTM 11. 3 Blank Root Cause Tool 2 Template**

Suspected Cause					
	Mission	Resource	Quality	Safety/Envir.	Total

Steps:

1. Input ‘Suspected Cause’ from *Root Cause Tool 1*
2. Rate the impact (1-5 (5 = Highest impact; 1 = Lowest impact)) of each cause for each ‘Area of Impact’ (use ‘N/A’ if not applicable)
3. Total the ratings for an overall score to determine cause with greatest impact

### **Definitions**

***Mission*** – the overall program or organization mission agenda

***Resources*** – budget and personnel are typically referenced as resources; however, other items may also apply (e.g. hardware/equipment)

***Quality*** – to the level of work

***Safety/Environment*** – Affecting ability to work in ideal conditions, or impact to public safety

Figure 11.4 Example of a Completed Root Cause Tool 2

Suspected Cause					
	Mission	Resource	Quality	Safety/ Envir.	Total
Sufficient training was not available. (B1,C02)	5	N/A	N/A	N/A	5
Supervisor did not communicate with the Director the lack of training the employee had with CDCS responsibilities. (B4,C06)	5	2	4	N/A	11
Lack of manpower rushed the hiring process; hiring underqualified employee. (B2,C03)	4	3	5	N/A	12
Employee ignored the policy of securing the SF- 700 just for convenience (employee Negligence). (B2,C02)	5	N/A	4	1	10

Steps:

1. Input 'Suspected Cause' from *Root Cause Tool 1*
2. Rate the impact (1-5 (5 = Highest impact; 1 = Lowest impact)) of each cause for each 'Area of Impact' (use 'N/A' if not applicable)
3. Total the ratings for an overall score to determine cause with greatest impact

#### Definitions



***Mission*** – the overall program or organization mission agenda

***Resources*** – budget and personnel are typically referenced as resources; however, other items may also apply (e.g. hardware/equipment)

***Quality*** – to the level of work

***Safety/Environment*** – Affecting ability to work in ideal conditions or impact to public safety

## **Appendix A SAFEGUARDS AND SECURITY SURVEY AND SELF-ASSESSMENT TOOLKIT**

### **A.1 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 sub-topical 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 CAPs, and DOE F 470.8, Survey/Inspection Report.

### **A.2 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:

1. Sample In-Briefing
2. Sample Survey Plan Format
3. Documents For Possible Review
4. Sample Notification Memos
5. Sample Accommodation Request

**A.2.1.1 Sample In-Briefing (Customize for specific survey objectives, activities, etc.)****Classification****SAFEGUARDS AND  
SECURITY  
PERIODIC SURVEY**Name of Facility Being Surveyed  
Facility Code

Dates of Survey

Conducted by  
Surveying Office

Surveying Office

**Classification****Classification****OBJECTIVE**

- Provide assurance to the Secretary of Energy, Departmental elements, and other government agencies that S&S interests and activities are protected at the required levels
- Provide a basis for line management to make decisions regarding S&S program implementation activities, including allocation of resources, acceptance of risk, and mitigation of vulnerabilities. The results must provide a compliance- and performance-based documented evaluation of the S&S program
- Identify S&S program strengths and weaknesses, develop and complete a process improvement schedule, and use the results to correct and improve the overall S&S program
- Provide documentation of oversight and assessment activities.

Surveying Office

**Classification**

## 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**PhPgSurvey 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

**A.2.1.2 Sample Survey Plan Format**

1. Title of survey
2. Location of facility
3. Purpose of survey
4. Survey dates
5. General facility information /description
6. Facility data
7. Work/activities performed
8. Operating organization (contractor)
9. S&S interests
10. Strategic Partnership Projects or other security activities
11. Scope of survey
12. Period of review, including extended observation or data collection if applicable
13. Objectives

14. Topical areas to be included/excluded and justification for each
15. Topical areas with findings from previous surveys, inspections reports, audits and appraisals (e.g. Government Accountability Office (GAO)/ Inspector General (IG))
16. Special areas/items of interest/concern
17. Survey planning and preparation
18. Performance tests (associated safety plans)
19. Survey guide information
20. Pre-survey information
21. Survey conduct—approach and methodology
22. Documents to be reviewed
23. Performance tests
24. Individuals to be interviewed
25. Sampling activities, including extended observation, shadowing or surveillance if applicable
26. Schedule of activities
27. Survey schedule
28. In-briefing information
29. Coordinating instructions
30. Exit briefing
31. Schedule for report development
32. Team composition/assignments
33. Team members
34. Assignments/responsibilities
35. Contractor support
36. Points of contact at the facility
37. Authority/governing documents

38. Directives
39. References (unclassified/classified)
40. Survey report format
41. Administration, support, and logistics
42. Work facilities
43. Transportation
44. Computer support
45. Administrative support
46. Classification support
47. Training requirements
48. Appendices
49. Performance tests (including Safety Plans)
50. Survey guides
51. Forms

#### **A.2.1.3 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 shall also be considered.

1. Program Planning and Management
2. Organization charts depicting the Safeguards and Security (S&S) management structure and S&S functional structure
3. 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)
4. Position descriptions for S&S management
5. Program Office and local instructions for the implementation of S&S programs



6. Supplemental documents and guidance for implementing S&S programs
7. Facility/site security plan (SP) and any referenced or supplemental plans and documentation
8. Emergency management and security condition (SECON) plans
9. Survey reports, inspection reports, Government Accountability Office and Inspector General audit/appraisal reports, self-assessment reports
10. Staff raining records
11. Contract(s), including Statement of Work
12. List of all subcontractors and consultants conducting work for the contractor
13. List of U.S. Department of Energy (DOE) directives and security clauses that have been incorporated into applicable contracts
14. Approved and pending equivalencies/exemptions to DOE directives and any deviations to national drivers (e.g., Code of Federal Regulations)
15. Copy of the facility registration
16. Applicable memoranda of understanding (MOU)/Agreement (MOA)
17. Completed Foreign Ownership, Control or Influence (FOCI) questionnaire (SF 328)
18. Key Management Personnel (KMP) list
19. Dates of all applicable FOCI determinations and copies of any mitigation agreements
20. A copy of the contractor's records of all contracts and subcontracts involving access authorizations
21. Vulnerability Analysis (VA) reports
22. Security Risk Assessment (SRA) reports
23. Contingency plans
24. Survey and self-assessment program procedures
25. Issues management plans and procedures
26. CAPs and status updates for all open deficiencies
27. Finding/deficiency corrective action validation and closing procedures
28. Incidents of Security Concern procedure, including initial notification and inquiry reports

29. Contract Security Classification Specification (CSCS) forms
30. Facility Data and Approval Record (FDAR) forms
31. Copy of the approved Performance Assurance Program Plan
32. List of essential elements documented in the Performance Assurance program and the testing schedule for each
33. Documentation of the integrated contractor assurance system
34. Protective Force (PF)
35. Organization and function charts
36. PF general, special and post orders
37. PF shift schedules and post assignments
38. PF standard equipment issuance (Security Police Officer (SPO) I, II, III, and Special Response Team (SRT))
39. PF weapons and ammunition inventories
40. Weapons maintenance logs
41. MOU with local law enforcement agencies and documentation of exercises conducted with those agencies
42. Integration of crisis management personnel into procedures
43. PF training records which include:
  44. A list of PF personnel who are subject to weapons qualification within 90 days of the start date of the survey
  45. A list of PF personnel who are medically certified to participate in the physical fitness program
  46. All documentation of PF exercises conducted since the last S&S survey
  47. Instructor certification
  48. Job analysis
  49. Job task analyses
50. Security Emergency Response Plan (SERP)

51. Security Incident Response Plan (SIRP)
52. Facility Evacuation Response Plans
53. Security Contingency Response Plans
54. Target folders
55. Schedule for performance testing (results of recent tests)
56. Compensatory measures currently in place (including pertinent documentation)
57. Procedures (administrative, training, non-response-related operational requirements)
58. Access/badge control
59. Information containing, at a minimum, policies/procedures for issuing, replacing, and recovering passes/badges
60. Inventories (since last S&S survey) of passes/badges made, issued, lost, recovered, returned, and destroyed
61. Shipment security plans
62. Shipment procedures
63. In-transit emergency plan
64. Shipment emergency response plan
65. Physical Protection
66. Organization and function charts
67. Lock and key records and procedures
68. Automated access control system records and procedures (including biometric access input) as well as access credential issuances (e.g., keycards, tokens)
69. Barrier maintenance procedures/records
70. Property control procedures
71. Access control procedures
72. Local performance testing plans and procedures
73. Physical security system description(s) and location(s)

74. IDS maintenance and testing records and procedures
75. IDS Analysis and Evaluation Report
76. Unscheduled alarm reports
77. Central Alarm Station (CAS)/Secondary Alarm Station (SAS) procedures (interface description)
78. Emergency response for CAS/SAS recovery
79. Emergency power systems (uninterruptible power supply system)
80. Compensatory procedures for equipment outages
81. Security container documentation and maintenance records
82. Automated systems description and procedures
83. Manual
84. Procedures
85. Controls
86. Calibration and testing procedures and records (e.g., X-ray, metal detectors, IDS)
87. Inspection procedures
88. Limited Scope Performance Test (LSPT) results
89. Information Security
90. Organization and function charts
91. Training records
92. Technical surveillance countermeasure (TSCM) survey reports
93. Site inventory of accredited systems, showing property tag number, the accrediting authority, and most recent accreditation date for each
94. Formal assignments of TSCM personnel
95. TSCM activity support memoranda (if applicable)
96. Local TSCM implementation guidance
97. TSCMO service schedules, files, and corrective action reports

98. TSCM team equipment maintenance and calibration files
99. TSCM team training and certification records
100. Operations Security (OPSEC) Plan
101. OPSEC procedures
102. OPSEC program files
103. Local threat statement
104. Critical Program Information
105. Counter-Imagery Program Plan (if applicable)
106. Number of derivative classifiers and declassifiers
107. Appointment letters (e.g., Inquiry Officer, custodians)
108. Training records, reports, and lesson plans
109. Classification guidance
110. Classified Matter Protection and Control (CMPC) procedures
111. Control station procedures
112. List of classified holdings, including documents, electronic media, and matter
113. Number of Special Access Programs (SAPs)
114. Personnel Security
115. Local procedures for terminations, leave of absences, reinstating clearances, clearance processing, exit briefing process
116. Contractor access authorization requests
117. Sample initial, comprehensive, refresher, and termination briefing materials
118. Previous findings and CAPs
119. Reciprocal access authorization documentation
120. Awareness tools (posters, newsletters)
121. Security infraction and violation records

- 122. 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)
- 123. 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
- 124. Visitor control logs
- 125. Local visitor control procedures
- 126. Central Personnel Clearance Index (CPCI) list of individuals overdue for reinvestigation
- 127. Drug testing/handling procedures
- 128. Drug testing records
- 129. Human Reliability Program (HRP) participants
- 130. HRP criteria/plans/procedures
- 131. Random test procedures
- 132. List of individuals on leaves of absence and the associated procedures for tracking
- 133. List of inactive classified contracts
- 134. List of personnel with access authorizations and the associated contract(s)
- 135. List of clearances terminated during the survey period
- 136. 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, shall be compared for discrepancies.
- 137. Foreign Visits and Assignments
- 138. List of foreign visitors from sensitive countries during the survey period
- 139. Specific security plans for foreign visitors from sensitive countries
- 140. Escort procedures
- 141. Local procedures for requesting, processing, and approving visits and assignments
- 142. List of foreign visitors or assignees, including hosts, during survey period
- 143. Incident reports involving foreign nationals

- 144. Requests for foreign national visits
- 145. Indices checks
- 146. Documentation authorizing approval for specific categories of visits and assignments
- 147. Sensitive country listings
- 148. Equivalencies/exemptions pertinent to visits and assignments
- 149. Personnel assignment agreements
- 150. Nuclear Material Control and Accountability (MC&A)
- 151. MC&A plans and procedures
- 152. Training records, reports, and lesson plans
- 153. Performance tests
- 154. Categorization process documentation
- 155. Incident reporting process and procedures
- 156. Emergency response plans and facility procedures
- 157. Database descriptions
- 158. Material Balance Area (MBA) account structure
- 159. Material transfer records
- 160. Internal control procedures
- 161. Nuclear Material Management and Safeguards System (NMMSS) reports
- 162. Shipper/receiver difference procedures and records
- 163. Material control indicator program
- 164. Inventory difference program
- 165. Materials containment documentation
- 166. Facility procedures
- 167. Material access program

- 168. Access authorization lists
- 169. Search procedures
- 170. Material surveillance procedures
- 171. Portal monitor records and procedures
- 172. Daily administrative check program and procedures
- 173. Tamper-indicating device program



**A.2.2 Sample Notification Memos****A.2.2.1 Notification and Data Call**

DATE:

TO:

FROM:

SUBJECT: Notification and Data Call Request – 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 Planning and Management
- 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

**A.2.2.2 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 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 shall 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 shall include the past 12 months unless otherwise noted.

1. Program Planning and Management
2. Organization chart(s) or listings with brief description of organizations functions and responsibilities
3. Current site security plan with all referenced or supplemental plans
4. Recent self-assessment report(s)
5. Copy of findings/CAP tracking procedures
6. Current status of all open and closed findings/CAPs since the last survey (including Office of Independent Enterprise Assessments, Government Accountability Office and Inspector General)
7. 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)
8. List of all subcontractors performing work (name of company, contract number, names of individuals with access authorizations)
9. Copies of all CSCS and FDAR forms related to the facility clearance
10. Protective Force
11. Facility security plans
12. Emergency security operation procedures
13. Security emergency response plan
14. Memoranda of Agreement/Understanding (e.g., with local law enforcement)
15. Physical Protection
16. Security systems test procedures
17. Security systems maintenance procedures
18. Lock and key records and procedures
19. Access control procedures

20. Unscheduled alarm reports for the past three months
21. Information Security
22. List of locations where classified matter is stored and the name and telephone number of the responsible custodian
23. List of locations where classified matter is used/processed
24. List of total number of classified materials and documents in accountability, including level and category
25. OPSEC plans
26. All training materials to support the OPSEC program (have available on request)
27. All documents that support OPSEC briefings for contractor personnel (have available on request)
28. All other internal program procedures that support OPSEC
29. List of derivative classifiers
30. Personnel Security
31. List of all assigned (cleared) employees/subcontractors who have traveled to sensitive countries (official and unofficial)
32. List of all visits and assignments of foreign nationals
33. List of all subcontractors
34. List of uncleared visitors
35. List of outgoing classified visits
36. List of all incoming classified visitors
37. List of HRP participants
38. List of terminated clearances (including name, date termination statement signed, date clearance terminated, CPCI number)
39. Foreign Visits and Assignments
40. List of visits
41. List of foreign national (FN) visitors from sensitive countries

- 42. Specific security plans for FNs visiting from sensitive countries
- 43. Escort procedures
- 44. Local procedures for requesting, processing, and approving visits and assignments
- 45. Nuclear MC&A
- 46. Categorization process documentation
- 47. Material Balance Area account structure
- 48. Inventory difference program plans
- 49. MC&A plan/procedures (may be part of site security plan or separate document(s))

**A.2.2.3 Initial Safeguards and Security Survey**

Date:

To:

From:

Subject: 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 topical areas 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:

1. Program Planning and Management
2. A list reflecting security staffing since (month, year). This list shall include name of person, date of hire/termination, job title, and security functions (responsibilities)
3. Copies of all MOU and management agreements relating to S&S programs
4. A copy of all internal operations procedures/practices, with index
5. Copies of the most recent S&S security risk assessments, including documentation reflecting risk determination methodology
6. A list of all security training courses that have been approved as part of the training approval plan process
7. 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
8. Copies of any procedures or other guidance pertaining to the identification and development of S&S training
9. 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.
10. 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 CSCS form may be used in lieu of a listing.)
11. List of all terminated and completed contracts since (month, year). This listing shall 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.)
12. List of pending FOCI determinations
13. List of FOCI determinations completed since (month, year)

14. List of FOCI approved companies, including the FOCI determination date, mitigation types if any, and date of the latest FOCI update
15. 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
16. 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
17. Copies of all XYZ-generated guidance or direction (hardcopy or electronic) provided for the conduct of self-assessments and other internal evaluations
18. List of all open findings
19. List of open findings pending validation
20. Copy of Incidents of Security Concern program procedures
21. A list of all security incidents, including computer security incidents, occurring since (month, year). This list shall identify the date of the incident, the date of the inquiry report, and the nature of the incident
22. Copies of award fee data (Award Fee Plan, performance criteria)
23. PF
24. 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
25. 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
26. Copies of all 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



27. List of all PF 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)
28. 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 shall be available for review during the survey
29. Copy of any DOE approval of the PF job analysis
30. Copy of the last (and immediately preceding) annual review of the PF job analysis.
31. Copy of the most recent approved Training Plan
32. If available, an approved Training Approval Program Assessment Report
33. A list of permanent and temporary security posts including post number and hours staffed
34. 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, CAS logs and radio checks, weapons issue, weapons maintenance, weapons cleaning, emergency call-out)
35. Copy of plans documenting the physical configuration of security posts
36. Copy of traffic/parking procedures (safety or security PF interface/enforcement)
37. Copy of general and specific patrol orders that define patrol intervals and routes for classified repositories, vaults, and vault-type rooms
38. Weapons inventory list, including serial number and storage location.
39. Quality Assurance program documentation
40. Communications equipment inventory list, including quantity, make, model, and auxiliary equipment, as well as interface capabilities with LLEA
41. Auxiliary equipment inventory list including quantity, make, model of assigned equipment (e.g., gas masks, protective vests)
42. 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)

43. Physical Protection
44. Copy of key control and property pass procedures
45. Copy of documentation that reflects the total value of capital and sensitive/equipment items (include precious metals as applicable)
46. Listing of all controlled substances and locations, including copies of Drug Enforcement
47. Agency certificates
48. 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)
49. List of all alarm points identified by system application (e.g., Argus, Litton) and location that provides protection for classified matter and property
50. Copy of the approved alarm test plan and a copy of the DOE approval correspondence
51. Copy of the procedures for making changes to alarm transmission/monitoring systems databases or software
52. Copies of reports since (month, year) of unscheduled alarm activations
53. Copy of false alarm rate and nuisance alarm rate since (month, year)
54. Copies of maintenance procedures and test results since (month, year)
55. Copies of IDS Analysis and Evaluation report since (month, year)
56. Information Security
57. A list of all current XYZ original and derivative classifiers
58. A list of reviewing officials, including name, title, organization, office location, and telephone number
59. A list of all classification guides, including title and date
60. A list of all XYZ shipping/mailroom logs pertaining to the transmission of classified matter since (month, year)

61. 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
62. List of all CDCSs, including the custodian names, organization, location, and telephone extension.
63. Copy of CMPC procedures (marking, destruction)
64. List of all classified material accountability records
65. Copy of DOE-approved Technical Surveillance Countermeasures (TSCM) Plan
66. Copy of the TSCM officers appointment memoranda
67. Copy of the site-wide procedures for the control and use of potential TSCM equipment
68. Copy of the procedures controlling TSCM equipment, the DOE approval for purchasing and controlling TSCM equipment, and an inventory listing, if appropriate
69. Copy of OPSEC Plan
70. Copy of OPSEC assessment and review reports conducted since (month, year)
71. List of contractors (on- and offsite) under the OPSEC program
72. Copy of OPSEC working group meeting minutes for meetings conducted since (month, year)
73. Personnel Security
74. A list of all cleared personnel whose access authorization has been terminated since (month, year) (Note: This list shall include the date of termination, name of person, and organization for which the individual worked.)
75. A list of names of all consultants/vendors issued security clearances that conduct business with XYZ
76. A list of all individuals by name and clearance number terminated for cause
77. A list of individuals by name and clearance number who have had clearances canceled/terminated prior to completion of the background investigation
78. A list by name and clearance number of all FNs who are/were clearance applicants or incumbents. Include in the listing the country of origin and level of clearance

79. A list by name and clearance number of all dual citizens processed for access authorization (clearance) since (month, year)
80. A list of individuals on leave of absence or extended leave. This list shall include name, clearance number, reason for leave, date leave commenced, expected date of return to duty, and/or date of termination
81. Have available each report submitted for derogatory information since (month, year)
82. Copy of attendance records for initial, comprehensive, and termination briefings for all contractor employees since (month, year)
83. Copies of most current security education briefing/lesson plans for initial, comprehensive, refresher, and termination briefings since (month, year)
84. Copy of the compliance verification numbers associated with the most recent refresher briefing
85. Documentation describing the badging system and operating procedures for classified visits. Provide examples of all badge types in use
86. Copy of the procedures for administering incoming and outgoing classified visits
87. Copies of incoming visit requests since (month, year)
88. Classified visitor logs since (month, year)
89. Copies or log of classified visitor badge requests since (month, year)
90. A listing of the number and dates of each positive substance abuse test report
91. A copy of drug test policy
92. A list of all personnel, by name and clearance number, enrolled in the HRP or other performance assurance program
93. List of all individuals, by name and clearance number, removed from the HRP since (month, year)
94. Justifications for HRP positions and date of last review
95. Procedures for Personal Identify Verification process
96. Foreign Visits and Assignments
97. Lists of all host reports submitted since (month, year) including date submitted

- 98. Local procedures for requesting, processing, and approving visits and assignments
- 99. List of foreign visitors or assignees, including names of hosts, for survey period
- 100. Incident reports involving FNs
- 101. Requests for FN visits
- 102. Indices checks
- 103. Documentation authorizing approval for specific categories of visits and assignments
- 104. Sensitive country listings
- 105. Nuclear MC&A
- 106. MC&A Plan
- 107. Performance test data
- 108. Categorization documentation
- 109. Internal control procedures
- 110. Inventory difference program
- 111. Shipper/receiver difference procedures and records

### A.2.3 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 topical s, security plans, Vulnerability Assessments, and applicable DOE directives.

### A.3 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.

1. Sample Survey Worksheet
2. Instructions for Completing the Sample Survey Worksheet
3. Sample Performance Test Safety Plan
4. Sample Performance Test Plan

**A.3.1.1 Sample Survey Worksheet**

## CLASSIFICATION

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

## CLASSIFICATION

## 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 shall have a unique identification number assigned, which shall 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 shall 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., S&S Initial Survey, Office of Enterprise Assessments, Inspector Government Accountability Office)
5. the sub-topical 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 MC&A



<u>CODE</u>	<u>TYPES OF SURVEY DOCUMENTS</u>
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	Safeguards and Security Termination Surveys
TSCM	TSCM Reports

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

Findings shall be clear, focused, and based on the perceived underlying cause of the protection shortfall, to the most reasonable extent possible; rather than merely stating the occurrence of a protection element failure or weakness. A finding shall 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 shall 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 shall 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) shall 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 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 shall 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 shall be written as DOE O XXX.XX, followed by the specific identification numbers and/or letters (e.g., DOE O 470.4B, Minor Change 2, 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.

**A.3.1.2 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 shall 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 LSPTs WILL BE CONDUCTED IN CONFORMANCE WITH THIS SAFETY PLAN AND ONLY AFTER SPECIFIC APPROVAL TO CONDUCT THE LSPTs 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 PF personnel to detect and prevent contraband and prohibited items from being introduced into Limited Areas, Vault-Type Room, 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 shall 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

☒ 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

☒ 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:**

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

**A.3.2 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), and
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 a.m.
2. Upon notification of the unattended “classified” document, the CDCO will verify that the individual finding the document completed the following actions:
3. Xxxx
4. Xxxx
5. Xxxx

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

6. Xxxx
7. Xxxx
8. Xxxx



## 9. Pass/Fail Criteria

In order to successfully complete the performance test, the following shall 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.

## 10. 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.

## 11. 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:

### 12. Monitor the document

### 13. Monitor the PF response

### 14. Monitor the CDCO

#### 15. 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.

#### 16. 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.

#### 17. Compensatory measures

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

#### 18. 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.

#### 19. REFERENCES

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

1. DOE O XXX.X, Information Security
2. Information Security Standard Operating Procedure #
3. PF Standard Operating Procedure #
4. PF Post Order #

SURVEY TEAM LEADER:

DATE

---

(Signature of Approval)

## **A.4 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. Sub-topical areas,
2. areas of consideration,
3. sample documents list,
4. sample interview candidates, and
5. suggested interview questions.

### **A.4.1 Program Planning and Management**

Sub-topical Areas to Program Planning and Management

1. Protection Program Management
2. Program Planning and Management
3. Personnel Development and Training
4. S&S Planning and Procedures
5. Management Control
  - a. Surveys and Self-Assessment Programs Performance Assurance Program Resolution of Findings
6. Incident Reporting and Management
7. Program-Wide Support
8. Facility Approval and Registration of Activities FOCI Security Management in Contracting

#### **AREAS OF CONSIDERATION**

The topical area team shall 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 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 CAPs?
- 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?
- How many IOSCs were Category A and Category B incidents?

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.4.1.1 Program Planning and Management**

Sub-topical Areas to Protection Program Management

- Program Planning and Management
- 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 shall be carefully reviewed and validated:

- Organization diagrams depicting the management structure
- Functions, Responsibilities and Authorities Manual, S&S 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 (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 shall 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:

- 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 Capital 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 PF)

Sample Interview Questions:

- 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.4.1.2 Safeguards and Security Planning and Procedures**

Sub-topical Areas to S&S Planning and Procedures

None

Sample Document List:

- 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
- SSIMS reports
- Emergency plans
- Contingency plans
- Local procedures
- MC&A 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 shall be thoroughly familiar with the purpose of each document reviewed. The requirement for the document shall be compared with the finished product, and an assessment made of the adequacy of the document in complying with the requirement.

Sample Interview Candidates:

- 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/VA data
- Personnel responsible for developing the various S&S plans
- PF managers

a. Sample Interview Questions:

- 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 (GSP) or Design Basis Threat (DBT) used for addressing threats? If not, is this approved in writing? What basis is used if the GSP/DBT 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?

## 1. MANAGEMENT CONTROL

### Sub-topical Areas to Management Control:

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

### Sample Document List:

- Survey and self-assessment program plans and schedules
- Incidents of Security Concern (IOSC) plans and implementing procedures
- Survey and self-assessment reports
- CAPs 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 CAP packages
- Inquiry Official appointment letters
- Damage assessments
- 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:

- DOE management
- 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
- PF Managers
- IOSC Inquiry Officials

## Sample Interview Questions:

- 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 area and sub-topical area 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 CAPs?
- 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 IOSCs? 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 CAPs 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?
- Were Category A incidents reported and closed out in SSIMS within prescribed timeframes?
- Were Category B incident documented and tracked?
- Does the inquiry report include the facts and circumstances associated with the incident?
- Does the case file include all appropriate information and supporting evidence (e.g. personal statements of the principles, sanitization records, etc.)?
- 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 IOSCs 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 incidents and identify them by category?
- Does the facility maintain a central record of all inquiries into IOSCs 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.4.1.3 PROGRAM-WIDE SUPPORT**

Sub-topical Areas to Program-Wide Support:

- Facility Approval and Registration of Activities
- FOCI
- Security Management in Contracting

Sample Document List:

- 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 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 CSCS F 470.1
- Signed 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 CPCI of access authorizations held by the contractor. The CPCI and contractor lists, including the list of current KMP, shall be compared for discrepancies.
- Internal procedures (facility clearance, FOCI)

- Applicable MOU/Agreement (e.g., MOA documenting responsibilities of DOE and a cognizant other government agency (OGA) for reciprocity of a specific Facility Clearance Level (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 must 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:

- DOE 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:

- 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 weighed 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?

**A.4.2 PROTECTIVE FORCE**

Sub-topical Areas to Protective Force:

1. Management
2. Training
3. Duties
4. Facilities and Equipment

**AREAS OF CONSIDERATION**

The topical area team shall 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?



**A.4.2.1 Management**

Sub-topical Areas to Management:

None

Sample Document List:

- Facility/Site SP
- Approved or pending equivalencies and exemptions
- Staffing plans
- Budget documents
- Overtime allocations
- VA data
- HRP criteria and list of staff assigned to HRP positions
- Response plans
- Recent findings and associated CAPs
- General, Post, and Special orders

Sample Interview Candidates:

- PF Manager
- DOE S&S Director
- PF Training Coordinator
- Individuals responsible for the VA data
- Special Response Team Lead

Sample Interview Questions:

- 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?

**A.4.2.2 TRAINING**

Sub-topical Areas to Training:

None

Sample Document List:

- Annual 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 CAPs (including documented root cause) relevant to this topical area

Sample Interview Candidates:

- PF Manager
- DOE Safeguards and Security Director
- PF Training Coordinator

- Individuals responsible for Vulnerability Assessment data
- Instructors

Sample Interview Questions:

- 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 trained through NTC?
- 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?

**A.4.2.3 DUTIES**

Sub-topical Areas to Duties:

None

Sample Document List:

- Facility/Site SP
- Approved JTAs
- Staffing plans
- Overtime allocations
- List of standard equipment issued
- PF 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
- SRT rosters
- Security Incident Response Plan
- Recent findings and associated CAPs relevant to this topical area
- Security lock and key control procedures

Sample Interview Candidates:

- PF Manager
- DOE 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:

- 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?

#### **A.4.2.4 Facilities and Equipment**

Sub-topical Areas to Facilities and Equipment:

None

## Sample Document List:

- Facility/Site SP
- Equivalencies and exemptions
- Staffing plans
- Budget documents
- Overtime allocations
- List of standard equipment issued and instructions for use
- 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 CAPs relevant to this topical area
- Security Incident Response Plan

## Sample Interview Candidates:

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

## Sample Interview Questions:

- 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?



### A.4.3 **PHYSICAL SECURITY**

Sub-topical Areas to Physical Security:

1. Access controls
2. Intrusion detection and assessment systems
3. Barriers and delay mechanisms
4. Testing and maintenance
5. Communications

#### AREAS OF CONSIDERATION

The topical area team shall 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 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 security 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 SNM, classified matter, and vital equipment adequately addressed in site planning documents?

- How are the GSP/DBT, 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?

**A.4.3.1 ACCESS CONTROLS**

Sub-topical Areas to Access Controls:

None

Sample Document List:

- 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 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:

- 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:

- 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?

**A.4.3.2 Intrusion Detection and Assessment Systems**

Sub-topical Areas to Intrusion Detection and Assessment Systems

None

Sample Document List:

- 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
- CAS/SAS procedures
- Emergency response for CAS/SAS recovery
- Emergency power systems (uninterruptible power supply system) certification and maintenance logs
- Compensatory procedures for equipment outages
- LSPT results
- IDS Analysis and Evaluation Report

During the course of document reviews, the survey team shall 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:

- 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
- PF Managers
- Emergency management planners
- User personnel responsible for walk-testing or other performance testing of alarm systems
- Maintenance personnel

Sample Interview Questions:

- 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?

**A.4.3.3 Barriers and Delay Mechanisms**

Sub-topical Areas to Barriers and Delay Mechanisms:

None

Sample Document List:

- Facility/Site security plan and 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
- CAS/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:

- 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:

- 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 Material Access Areas (MAA) perimeters sufficient to ensure SNM cannot be removed?
- Do the security containers meet all required DOE and other standards?

#### **A.4.3.4 Testing and Maintenance**

Sub-topical Areas to Testing and Maintenance:

None

Sample Document List:

- 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
- CAS/SAS procedures
- Emergency power systems (uninterruptible power supply system)
- Compensatory procedures for equipment outages
- Inspection procedures

Sample Interview Candidates:

- S&S 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
- PF Managers
- Emergency management planners

Sample Interview Questions:

- 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?

#### **A.4.3.5 Communications**

Sub-topical Areas to Testing Communications:

None

Sample Document List:

- Performance tests of communication equipment
- 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

a. Sample Interview Candidates:

- PF Members
- S&S staff responsible for communication systems
- Alarms maintenance/installation and testing personnel

- CAS/Central Alarm Station (SAS) personnel
- Special Response Team members
- Emergency management planners

Sample Interview Questions:

- 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?

#### A.4.4 **Information Security**

Sub-topical Areas to Information Protection:

1. Basic requirements
2. Technical surveillance countermeasures (TSCM)
3. OPSEC
4. Classification guidance
5. CMPC
6. Control of Classified Matter
7. Special Access Programs and Intelligence Information

#### AREAS OF CONSIDERATION

The topical area team shall 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 Site/Facility 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 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 topical area 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?

**A.4.4.1 BASIC REQUIREMENTS**

Sub-topical Areas to Basic Requirements:

None

Sample Document List

The following documents shall 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:

- Classification Officer
- 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 ask 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?

#### **A.4.4.2 TECHNICAL SURVEILLANCE COUNTERMEASURES**

Sub-topical Areas to Technical Surveillance Countermeasures (TSCM):

None

Sample Document List

The following documents shall be reviewed:

- Formal assignments of TSCM Operations Managers (TSCMOMs) and 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

#### a. 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)?

#### **A.4.4.3 OPERATIONS SECURITY**

Sub-topical Areas to 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 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 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 SNM (or credible rollup of Category II to a Category I quantity), Top Secret, or SAPs information within their boundaries?
- How are OPSEC concerns being disseminated to the staff of the facility?
- Have Critical Information 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?

**A.4.4.4 CLASSIFICATION GUIDANCE**

Sub-topical Areas to Classification Guidance:

None

Sample Document List

The following documents shall 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 shall be scheduled and interviews conducted with the following personnel:

- Classification Officer
- DCs and DDs
- Users of classified matter
- CMPC points of contact and custodians
- 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?

#### **A.4.4.5 Classified Matter Protection and Control**

Sub-topical Areas to CMPC:

1. Control of Classified Matter
2. SAPs 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
- IOSC involving CMPC (e.g. the creation (or origination), classification review, finalization and marking, control and accountability, reproduction, receipt and transmission, storage, and destruction of classified information)
- List of equipment used to reproduce and destroy classified matter with locations and associated approvals
- Accountable matter inventory list(s)
- SAP security plans
- Results of accountable annual inventories
- CAP 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
- 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?

**A.4.5 PERSONNEL SECURITY**

Sub-topical Areas:

1. Access authorizations
2. HRP
3. Control of classified visits
4. S&S awareness

**AREAS FOR CONSIDERATION**

The topical area team shall 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 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 Nondisclosure 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 FNs, 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 FN does not receive access to classified information before approval is received from the appropriate DOE federal official? How do the hosts ensure that the FN is precluded from access to classified information outside the scope of the governing treaty or international agreement?

**A.4.5.1 ACCESS AUTHORIZATIONS**

Sub-topical 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
- CPCI 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
- HRP 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 FNs 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?

**A.4.5.2 Human Reliability Program**

Sub-topical Areas to 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?

#### **A.4.5.3 CONTROL OF CLASSIFIED VISITS**

Sub-topical 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 shall 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? Vault-Type Rooms?

- 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 acknowledgment 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?

**A.4.5.4 Safeguards and Security Awareness**

Sub-topical Areas to S&S 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 shall 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 topical areas 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?

**A.4.6 Foreign Visits and Assignments**

Sub-topical Areas:

1. Sponsor program management and administration
2. Counterintelligence (CI) requirements
3. Export controls/tech transfer requirements
4. Security requirements
5. Approvals and reporting

**AREAS FOR CONSIDERATION**

The topical area team shall 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 sites/facilities adequately controlled?

- Is FN 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? 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 timely, adequate coordination among security, CI, export control, and foreign intelligence (when there is a foreign intelligence element onsite) should an FN 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 FNs 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/site have a 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?

**A.4.6.1 Sponsor Program Management and Administration**

Sub-topical Areas to Sponsor Program Management and Administration:

None

Sample Document List

The following documentation shall 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 in the Security Plan
- Security plans
- Unclassified computer security review
- OPSEC reviews/assessments
- Counterintelligence (CI) program reviews/assessments
- Notification of approval documentation (FACTS)
- Equivalencies/exemptions pertinent to visits and assignments
- Unclassified Foreign 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:

- S&S Manager (DOE and Contractor)

- OPSEC/CI Program Manager (DOE and Contractor)
- Unclassified Computer Security Manager
- Program Managers and/or 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 an FV 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 FVs?

#### **A.4.6.2 Counterintelligence Requirements**

Sub-topical Areas to Counterintelligence (CI) Requirements:

None

#### Sample Document List

The following documentation shall be considered for review:

- Documentation authorizing approval for specific categories of visits and assignments
- Indices checks
- Sensitive countries listing

- Documentation identifying sensitive topical areas
- Security plans
- Documentation of provided CI briefings
- CI Host briefings/debriefings
- Justification-for-visit request review and concurrence
- FACTS submittals
- Local CI reviews

#### Sample Interview Candidates

The following people shall be considered for possible interviews:

- Safeguard and Security Manager (DOE and Contractor)
- CI Program Manager (DOE and Contractor)
- 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 Visitors and Assignments (UFVA) to security areas?
- Is there a process covering the conduct, documentation 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 an FV 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 UFVA requests?



**A.4.6.3 Export Controls/Technology Transfer Requirements**

Sub-topical Areas to Export Controls/Technology Transfer Requirements:

None

Sample Document List

The following documentation shall be considered for review:

- Sensitive countries listing
- Documentation identifying sensitive subjects
- 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 shall be considered for interviews:

- S&S 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 UFVA approval process? How and at what level?
- Who approves the security plans unclassified UFVA to security areas?
- What is the process for ensuring adequate coordination among security, counterintelligence, export control, and foreign intelligence should an FV require

access to a security area or sensitive subject, or if the individual is visiting the site from a sensitive country?

#### **A.4.6.4 SECURITY REQUIREMENTS**

Sub-topical Areas to Security Requirements:

None

Sample Document List

The following documentation shall be considered for review:

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

Sample Interview Candidates

The following people shall be considered for interviews:

- S&S 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/site 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?

#### **A.4.6.5 APPROVALS AND REPORTING**

Sub-topical Areas Approval and Reporting:

None

Sample Document List

The following documentation shall 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 topical areas
- Visit-specific security plans
- Notification of approval documentation
- Deviations pertinent to visits and assignments
- Justification-for-visit request approvals and denials
- List of DOE FACTS entries for site/facility for specified scope of self-assessment

Sample Interview Candidates

The following people shall be interviewed regarding the unclassified UFVA program:

- S&S 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 UFVA to security areas?
- What is the process for ensuring adequate coordination among security, counterintelligence, export control, and foreign intelligence should an FV 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 UFVA program management? Has that point-of-contact information been provided to the DOE cognizant security office?

#### A.4.7 **Materials Control and Accountability**

Sub-topical Areas:

1. Program management
2. Material accountability
3. Materials control
4. Measurement
5. Physical inventory
6. NMMSS Reporting

#### AREAS FOR CONSIDERATION

The topical area team shall 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 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?

Is management providing oversight of NMMSS reporting?

- How is accountable nuclear material reported in NMMSS?
- Were the operator reports of nuclear material storage, processing, reviewed and verified the validated?
- Is accountable nuclear material reported in NMMSS to ensure the effective regulatory control?
- Is the site/facility reporting reportable quantities of an accountable nuclear material when it is recovered during deactivation, decommissioning, or decontamination?
- Is the site/facility reporting reportable quantities of an accountable nuclear material that was previously written off the NMMSS records?
- When NRC licensees' sites have nuclear material holding, is management conducting periodic reviews and assessments of the nuclear material holdings to ensure that NMMSS reporting requirements are being met; unneeded materials are identified and returned to DOE; appropriate disposition paths are identified; and accurate material characterizations are made?

**A.4.7.1 PROGRAM MANAGEMENT**

Sub-topical Areas to Program Administration:

None

Sample Document List

Documentation to be reviewed may include the following:

- Approved MC&A plans and procedures
- Facility/Site Security Plan and VAs
- Equivalencies/exemptions for MC&A with supporting documentation
- Organization charts
- Training records, lesson plans
- MBA operating plans
- Surveys, internal assessments and CAPs
- 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
- MBA 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 SNMs 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 IOSCs?
- Are procedures developed and documented for characterizing materials on inventory to determine categories and attractiveness under the graded safeguards concept?

#### **A.4.7.2 MATERIAL ACCOUNTABILITY**

Sub-topical Areas to Material Accountability:

None

### Sample Document List

Documentation to be reviewed may include the following:

- MC&A plans and procedures related to materials accounting
- Equivalencies/exemptions
- Facility procedures
- Database descriptions
- MBA account structure
- Material transfer records
- Inventory records
- Organization charts
- Internal control procedures
- NMMSS reports
- Training records, reports, lesson plans
- Shipper/receiver agreements
- Shipper/receiver difference procedures and records
- Inventory difference program
- Internal assessments and CAPs

### 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?

#### **A.4.7.3 Materials Control**

Sub-topical Areas to Material Control:

None

Sample Document List

Documentation to be reviewed may include the following:

- Materials containment documentation
- MC&A plans and procedures
- Facility procedures
- Equivalencies and exemptions

- Site/Facility Security Plan and VAs
- Material Access program plan
- Access authorization lists
- Combination change records
- 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 CAPs

#### 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 SNM areas controlled?
- Does the facility have a documented program to provide controls of nuclear material operations relative to 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?

#### **A.4.7.4 Measurement**

Sub-topical Areas to Measurement:

None

Sample Document List

Documentation to be reviewed may include the following:

- Measurement-control procedures
- 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?

#### **A.4.7.5 Physical Inventory**

Sub-topical Areas Physical Inventory

None

Sample Document List

Documentation to be reviewed may include the following:

- Measurement-control procedures
- 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 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 MBA 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?

#### A.4.8 Post-Survey Tools

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

1. Sample initial/periodic survey report format
2. Sample termination survey report
3. Sample slides for exit briefing
4. Sample report transmittal memorandum
5. Doe survey/inspection report form

##### A.4.8.1 Sample Initial/Periodic Survey Report Format

1. 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, shall be included in the report.
2. Report Content.
3. Initial and Periodic Survey Reports and Self-Assessment Reports. Reports shall contain the following items.
4. An executive summary containing:
5. The scope, methodology, period of coverage, duration, date of the exit briefing to management;
6. 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);
7. 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;
8. The overall composite facility rating with supporting rationale; and
9. A reference to a list of findings identified during the survey or self- assessment.
10. An introduction containing:

11. The scope, methodology, period of coverage, duration, date of the exit briefing to management; and
12. 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).
13. Narrative for all rated topical area and sub-topical areas that includes:
14. A description of the site's implementation of the topical/sub-topical area element;
15. The scope of the evaluation;
16. A description of activities conducted;
17. The evaluation results and associated issues (including other Department elements or OGA review or inspection results related to the topical areas/sub-topical areas that were included in the survey);
18. 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
19. An analysis that provides a justification and rationale of the factors responsible for the rating.
20. Attachments, including, for example:
21. A copy of the current DOE F 470.2, FDAR;
22. A listing of all active DOE F 470.1, CSCS, or DD F 254, Contract Security Classification Specification;
23. A listing of all new findings resulting from the survey/self-assessment;
24. A listing of all previous findings that are open, to include the current status of corrective actions;
25. A listing of team members including names, employer, and their assigned area(s) of evaluation; and
26. A listing of all source documentation used to support the survey/self- assessment conduct and results.

**Narrative:** The narrative section of the report shall clearly describe the surveyed facility – its 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 shall 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 shall reflect the compliance and performance segments of the survey. Reports shall 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, MC&A plans, local implementation procedures, etc.).
- All new findings must be identified. Open findings from the previous survey shall 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 shall be included in the body of the narrative.
- Findings, observations, opportunities for improvement, and suggestions, along with supporting data for each, shall be clearly described. The term "finding refers to a factual statement of identified issues and deficiencies (failure to meet a documented legal, regulatory, performance, compliance, or other applicable requirement) in the S&S program at a facility, resulting from an inspection, survey, self-assessment, or any other S&S review activity.
- Descriptions of the facility's strengths and weaknesses shall correlate to the survey results and establish the basis for the ratings. The survey report shall reflect validated and defensible ratings. The narrative description shall be consistent with and support the composite and topical area ratings (including "Does Not Apply").
- The report shall identify findings corrected on the spot. These findings and corrective actions shall be clearly described in the narrative.
- The status of corrective actions for open findings and findings from the previous survey shall be included in the narrative.
- A concluding analysis of each topical area shall be included in the narrative.
- Reasons for a less-than-satisfactory rating shall be explained in detail.

#### **A.4.8.2 Sample Termination Survey Report**

##### **SCOPE**

This report documents the results of the 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 onsite effort designed to review and ensure the proper and effective disposition and transfer of 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 SNM stored and processed at the facility. The end users were assigned individual MBA numbers under the SSD RIS. The SSD did not store SNM directly; it was stored at the end-user locations, which included XXXX and Hawkins 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 MC&A 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.

##### **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 FDAR 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.

**A.4.8.3 SAMPLE SLIDES FOR EXIT BRIEFING**

Slides that should be included for each topical area and sub-topical area.


**Classification**

**SAFEGUARDS AND  
SECURITY  
PERIODIC SURVEY**

Name of Facility Surveyed  
Facility Code

Dates of Survey

Conducted by  
Surveying Office

Surveying Office 


**Classification**

**Classification**

**Topical and Sub-topical Ratings**

PROGRAM MANAGEMENT & SUPPORT	Rating
------------------------------	--------

Protection Program Management	Rating
S&S Planning & Procedures	Rating
Management Control	Rating
Program Wide Support	Rating

Surveying Office 

**Classification**



**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**

**A.4.8.4 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 area and sub-topical 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 CAPs 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.

**A.4.8.5 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: <input checked="" type="radio"/> Initial <input type="radio"/> Periodic <input type="radio"/> Special <input type="radio"/> Termination <input type="radio"/> EA Reviews: <input checked="" type="radio"/> NPR <input type="radio"/> EPR <input type="radio"/> Self-Assessment		2. Report #:	
3. Facility Name:		4. a. Facility Code: b. RIS Code:	
5. Survey Date(s):	6. a. Findings: <input type="radio"/> Yes <input type="radio"/> No b. Findings Against Other Facilities:		7. Composite Rating:
8. Previous Survey Date(s): Next Survey Date:	9. Unresolved Findings: <input type="radio"/> Yes <input type="radio"/> No		10. Previous Rating:
11a. Surveying Office:	11b. Cognizant Security Office:		11c. Other Offices with Interests:
<div style="display: flex; justify-content: space-between;"> <div style="width: 48%;"> <p>12. Ratings:</p> <p>a) PROGRAM MANAGEMENT OPERATIONS</p> <p>PROTECTION PROGRAM MANAGEMENT _____</p> <p>Program Management and Administration _____</p> <p>Resources and Budgeting _____</p> <p>Personnel Development and Training _____</p> <p>S&amp;S PLANNING AND PROCEDURES _____</p> <p>MANAGEMENT CONTROL _____</p> <p>Surveys and Self Assessment Programs _____</p> <p>Performance Assurance Program _____</p> <p>Resolution of Findings _____</p> <p>Incident Reporting and Management _____</p> <p>PROGRAM WIDE SUPPORT _____</p> <p>Facility Approval and Registration of Activities _____</p> <p>Foreign Ownership, Control or Influence _____</p> <p>Security Management in Contracting _____</p> <p style="text-align: right;">OVERALL RATING _____</p> <p>b) PROTECTIVE FORCE _____</p> <p>MANAGEMENT _____</p> <p>TRAINING _____</p> <p>DUTIES _____</p> <p>FACILITIES AND EQUIPMENT _____</p> <p style="text-align: right;">OVERALL RATING _____</p> <p>c) PHYSICAL PROTECTION _____</p> <p>ACCESS CONTROLS _____</p> <p>INTRUSION DETECTION &amp; ASSESSMENT SYSTEMS _____</p> <p>BARRIERS AND DELAY MECHANISMS _____</p> <p>TESTING AND MAINTENANCE _____</p> <p>COMMUNICATIONS _____</p> <p style="text-align: right;">OVERALL RATING _____</p> </div> <div style="width: 48%;"> <p>d) INFORMATION SECURITY _____</p> <p>BASIC REQUIREMENTS _____</p> <p>TECHNICAL SURVEILLANCE COUNTERMEASURES _____</p> <p>OPERATIONS SECURITY _____</p> <p>CLASSIFICATION GUIDANCE _____</p> <p>CLASSIFIED MATTER PROTECTION &amp; CONTROL _____</p> <p>Control of Classified Matter _____</p> <p>Special Access Programs and Intelligence Information _____</p> <p style="text-align: right;">OVERALL RATING _____</p> <p>e) PERSONNEL SECURITY _____</p> <p>ACCESS AUTHORIZATIONS _____</p> <p>HUMAN RELIABILITY PROGRAMS _____</p> <p>CONTROL OF CLASSIFIED VISITS _____</p> <p>SAFEGUARDS AND SECURITY AWARENESS _____</p> <p style="text-align: right;">OVERALL RATING _____</p> <p>f) MATERIALS CONTROL &amp; ACCOUNTABILITY _____</p> <p>PROGRAM MANAGEMENT _____</p> <p>MATERIAL ACCOUNTABILITY _____</p> <p>MATERIALS CONTROL _____</p> <p>MEASUREMENT _____</p> <p>PHYSICAL INVENTORY _____</p> <p style="text-align: right;">OVERALL RATING _____</p> <p>g) FOREIGN VISITS AND ASSIGNMENTS _____</p> <p>SPONSOR PROGRAM MANAGEMENT &amp; ADMIN _____</p> <p>COUNTERINTELLIGENCE REQUIREMENTS _____</p> <p>EXPORT CONTROLS/TECH TRANSFER REQUIREMENTS _____</p> <p>SECURITY REQUIREMENTS _____</p> <p>APPROVALS AND REPORTING _____</p> <p style="text-align: right;">OVERALL RATING _____</p> </div> </div>			
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

---

## **Appendix B — WORKPLACE VIOLENCE/ACTIVE SHOOTER PROGRAM (EXAMPLE)**

### **B.1 Program Policy**

It is the Department of Energy's (DOE's) policy to promote a safe environment for its employees by working with its employees to prevent workplace violence. Violence, domestic violence, sexual assault, stalking, threats of violence, harassment, intimidation, bullying and other disruptive behavior in the DOE workplace will not be tolerated. Such behavior can include oral or written statements, gestures, or expressions that communicate a direct or indirect threat of harm. All reports of incidents or concerns will be taken seriously and will be dealt with appropriately by supervisors and managers. Individuals who commit such acts may be removed from the premises and may be subject to disciplinary action, criminal penalties, or both.

### **B.2 Scope**

This program applies to all federal and contractor employees.

### **B.3 Responsibilities**

1. The (Site Manager) is responsible for establishing the Workplace Violence Program policy and for administration of this program.
2. The (ODFSA), is responsible for overall implementation of this program document and guidance on program procedures. Workplace Violence and Active Shooter Plan is part of the site/facility Security Plan and requires ODFSA approval.
3. The (Director, Human Capital) is responsible for:
  - a. Responding to questions regarding employee rights and obligations under this policy.
  - b. Conducting effective employee screening and background checks.
  - c. Providing information on counseling services available to employees.
4. The (Coordinator, Training) is responsible for developing and conducting periodic training for all personnel, including annual employee briefings, and maintaining training records on all employees.
5. The (Coordinator, Emergency Management), is responsible for:
  - a. Providing day-to-day procedural guidance and coordination of this program.

- b. Developing an active shooter awareness campaign.
  - c. Assisting the Training staff with development of training and briefings.
6. (Facility Managers) are responsible for:
- a. Instituting access controls (i.e., keys, security system pass codes).
  - b. Distributing critical items to appropriate managers/employees, including floor plans, keys, and facility personnel lists and telephone numbers.
  - c. Coordinating with the facility's security staff to ensure the physical security of the location.
  - d. Placing removable floor plans near entrances and exits for emergency responders.
  - e. Activating the emergency notification system when an emergency occurs.
7. Supervisory Employees are responsible for monitoring their employees for changes in attitude, disposition, or any actions that could indicate potential violent behavior, and immediately notifying the General Manager or Deputy General Manager when they are made aware of any act/threat of workplace violence.
8. Employees are required to attend annual training that will assist them in identifying aberrant behavior and the proper course of action to take in such cases, and shall report acts/threats or information pertaining to acts/threats to their immediate supervisor.

## **B.4 Rules and Procedures**

### **B.4.1 Defining Workplace Violence**

Workplace violence can be any threat or act of violence against persons or property; or verbal threats, intimidation, harassment, bullying; or other inappropriate, disruptive behavior that causes fear for personal safety inside or outside of the work site.

A number of different actions in the work environment can trigger or cause workplace violence (e.g., anger over disciplinary actions or the loss of a job, resistance by a customer to regulatory actions, disagreement by a member of the public with DOE policy or practices, etc.). It may even be the result of non-work-related situations, such as domestic violence, road rage, or hate crimes (i.e., violence, intolerance or bigotry, intend to hurt and/or physically/psychologically intimidate someone because of their age, race, ethnicity, national origin, religion, sexual orientation, or disability). Workplace violence can be inflicted by an abusive employee, supervisor, co-worker, customer, family member, or

even a stranger. Whatever the cause or whoever the perpetrator, workplace violence is not acceptable and will not be tolerated at any DOE location.

There is no sure way to predict human behavior, and while there may be warning signs, there is no specific profile of a potentially dangerous individual. The best prevention comes from identifying and addressing any possible problems early.

#### **B.4.2 Workplace Violence Red Flags**

Potentially violent behaviors by an employee may include one or more of the following (this list of behaviors is not intended to be all-inclusive and is not intended as a mechanism for diagnosing violent tendencies):

- Increased use of alcohol and/or legal/illegal drugs
- Unexplained increase in absenteeism; vague physical complaints
- Noticeable decrease in attention to appearance and hygiene
- Depression/withdrawal
- Resistance and overreaction to changes in policy and procedures
- Repeated violations of company policies
- Increased severe mood swings
- Noticeably unstable, emotional responses
- Explosive outbursts of anger or rage without provocation
- Suicidal; comments about “putting things in order”
- Behavior that is suspect of paranoia (“everybody is against me”)
- Increasing talk of problems at home
- Escalation of domestic problems into the workplace; talk of severe financial problems
- Talk of previous incidents of violence
- Empathy with individuals committing violence
- Increase in unsolicited comments about firearms, other dangerous weapons, or violent crimes

### B.4.3 Preventing Workplace Violence

There are no fail-safe measures to ensure that violence will not occur. Chances to prevent acts of violence greatly improve with increased awareness of potential warning signs and rapid response to a potential problem. Employees and supervisors are encouraged to do their part and report any inappropriate or unacceptable behavior that is disruptive, provoking, harassing, threatening, or unsafe. Early action and intervention can serve to diffuse a potentially dangerous situation and prevent the occurrence of violence.

Prevention is an essential approach to minimize the occurrence of workplace violence. Prevention efforts are not limited to those discussed in this document; these are only suggested ways to handle adverse circumstances.

Identify and Evaluate Unacceptable Behavior. The employee's immediate supervisor is responsible for evaluating signs of unacceptable behavior or misconduct and taking appropriate action to put the employee on notice that such acts will not be tolerated. In most cases, the supervisor will face behavior or misconduct that can be handled administratively. There may also be instances when the supervisor will need to make a quick decision on whether the situation creates an immediate danger and requires the removal of the employee from the work site and/or the assistance of appropriate security personnel or law enforcement officials. Contingency plans for such occurrences will be developed and disseminated locally so supervisors will know whom to contact in cases of emergency. It is imperative that supervisors work closely with the senior management and Human Capital staff to ensure actions taken are in accordance with personnel management guidance.

Potential Warning Signs and Examples of Unacceptable Behavior. Recent studies indicate violent occurrences rarely happen without some warning. Before actually becoming violent, there are patterns of behavior or other activities that may serve as warning signs of violence. However, not everyone exhibiting warning signs will become violent. Examples of violent behavior range from property damage to verbal abuse, threats, harassment or physical assault. The following list is not intended to be all-inclusive, but provides some examples.

- Concealing or using a weapon
- Obsession with weapons
- Physically assaulting a co-worker
- Making direct or indirect threats, either in person or in writing, through phone calls or electronic mail
- Stalking, harassing or showing undue focus on another person

- Intimidating or instilling fear in others
- Talking about “getting even”
- Throwing or striking objects
- Actions that damage, destroy, or sabotage property.
- Physically aggressive acts like shaking fists at another person, kicking, verbally cursing at others, pounding on desks, punching a wall, angrily jumping up and down, or screaming at others

#### **B.4.4 Reporting Workplace Violence**

All employees must report acts of violence and potential violence to their supervisor.

Employee complaints shall be handled in accordance with Employee Complaints procedures. The supervisor will intervene quickly to investigate when a potential act of violence is reported. The most valuable information can often be obtained from co-workers who may be more familiar with a particular employee than the employee’s supervisor.

Supervisors shall never give the employee being investigated the name of the person who made the report due to the potential for adverse consequences. Additionally, identifying the reporting employee may discourage other employees from reporting acts of violence.

Appropriate action will be taken when standards of conduct are violated, when the employee’s job performance or the job performance of others is affected, or when the mission and efficiency of the service are affected.

If necessary, contact the Occupational Medical Director or an Employee Assistance Program counselor.

Employees will not be retaliated against for reporting acts or potential acts of violence, threats, harassment or property damage.

Any employee charged by law enforcement or other similar organization with a violent act will be placed on a Stop Order and escorted to Human Capital prior to returning to work.

#### **B.4.5 Intervention Techniques**

Key elements to successful intervention include treating employees fairly and with dignity and in no instance giving the employee the perception of provocation or personal attack. It is difficult to predict human behavior. Different scenarios are possible depending upon the personality types and mood of the individuals involved. Some individuals are overly reactive but nonviolent, while others may react violently with little apparent provocation.



When an employee exhibits signs of violence and the situation is not life threatening, diffuse the anger by using the following techniques.

- Meet with the employee in private to discuss the inappropriate behavior. Build trust by listening and treating the employee with respect.
- Do not argue, get defensive, or be sarcastic.
- Take all threats or acts of violence seriously.
- Counsel the employee, discuss the misconduct and how it affects the work of other employees; give a specific warning on future disciplinary action if the behavior continues. Appropriate discipline may be warranted for a first offense, depending on the facts involved.
- Inform the employee that the services of the Site Occupational Medical Director or the Employee Assistance Program are available and recommend or, depending on the circumstances, direct that the employee take advantage of them.

If unable to defuse the situation and the threat of violence persists:

1. Remain calm and do not put yourself or any staff member in a position to be injured.
2. If meeting alone with the employee, ask the employee to remain and excuse yourself from the meeting.
3. Call the next line supervisor, Human Capital staff, and the PF for assistance, and notify an Employee Assistance Program counselor.

After the situation has calmed down, counsel the employee in writing on the effect the violent behavior had and initiate appropriate disciplinary action based on the misconduct and/or disruption.

#### **B.4.6 Responding to a Violent Situation**

Remain calm and do not put yourself or any staff member in a position to be injured.

Call the PF, the next line supervisor, Human Capital staff, and/or an Employee Assistance Program counselor.

Once the danger has passed, take appropriate disciplinary action.

#### **B.4.7 Active Shooter Event**

According to the U.S. Department of Homeland Security, an active shooter is an individual actively engaged in killing or attempting to kill people in a confined and populated area. In

most cases, active shooters use firearms and there is no pattern or method to their selection of victims. Active shooter situations are unpredictable and evolve quickly. Typically, the immediate deployment of law enforcement is required to stop the shooting and mitigate harm to victims.

#### **B.4.8 Responding to an active shooter event**

Because active shooter situations are often over within 10 to 15 minutes, before law enforcement arrives on the scene, individuals shall be prepared both mentally and physically to deal with an active shooter situation. Individuals present during an active shooting incident shall be prepared to:

1. Assess the situation
2. React
3. Evacuate
4. Hide out/Shelter-in-Place
5. Take action
6. Call 911 when it is safe to do so

Assess the Situation and React. Quickly determine the most reasonable way to protect your own life. Remember that customers/clients are likely to follow the lead of employees and managers during an active shooter situation.

Evacuate. If there is an accessible escape path, attempt to evacuate the premises. Be sure to:

1. Have an escape route and plan in mind
2. Evacuate regardless of whether others agree to follow
3. Leave your belongings behind
4. Help others escape, if possible
5. Prevent individuals from entering an area where the active shooter may be
6. Keep your hands visible
7. Follow the instructions of any police officers
8. Do not attempt to move wounded people

9. Call 911 when you are safe
10. Hide out. If evacuation is not possible, find a place to hide where the active shooter is less likely to find you.

Your hiding place should be out of the active shooter's view, provide protection if shots are fired in your direction (e.g., an office with a closed and locked door), and not trap you or restrict your options for movement.

To prevent an active shooter from entering your hiding place, lock the door and blockade it with heavy furniture.

If the active shooter is nearby, lock the door, silence your cell phone and/or pager, turn off any source of noise (e.g., radios, televisions), hide behind large items (e.g., cabinets, desks), and remain quiet.

If evacuation and hiding are not possible, remain calm and dial 911, if possible, to alert police to the active shooter's location. If you cannot speak, leave the line open and allow the dispatcher to listen.

Take action against the active shooter. As a last resort, and only when your life is in imminent danger, attempt to disrupt and/or incapacitate the active shooter by:

1. Acting as aggressively as possible against him/her
2. Throwing items and/or using improvised weapons
3. Yelling
4. Committing to your actions/doing whatever it takes to save your life
5. When calling 911 or talking to law enforcement, provide the following information:
  - a. Location of the active shooter
  - b. Number of shooters, if more than one
  - c. Physical description of shooter/s
  - d. Number and type of weapons held by the shooter/s
  - e. Number of potential victims at the location
6. When law enforcement arrives

- a. Law enforcement's purpose is to stop the active shooter as soon as possible. Officers will proceed directly to the area in which the last shots were heard.
  - b. Officers may wear regular patrol uniforms or external bulletproof vests, Kevlar helmets, and other tactical equipment
  - c. Officers may be armed with rifles, shotguns, handguns
  - d. Officers may use pepper spray or tear gas to control the situation
  - e. Officers may shout commands and may push individuals to the ground for their safety
7. Employees/victims shall remain calm, follow officers' instructions, and:
- a. Put down any items in your hands (e.g., bags, jackets)
  - b. Immediately raise hands and spread fingers
  - c. Keep hands visible at all times
  - d. Avoid making quick movements toward officers such as attempting to hold on to them for safety
  - e. Avoid pointing, screaming and/or yelling
  - f. Do not stop to ask officers for help or direction when evacuating, just proceed in the direction from which officers are entering the premises

The first officers to arrive to the scene will not stop to help injured persons. Expect rescue teams comprised of additional officers and emergency medical personnel to follow the initial officers. These rescue teams will treat and remove any injured persons. They may also call upon able-bodied individuals to assist in removing the wounded from the premises.

Once you have reached a safe location or an assembly point, you will likely be held in that area by law enforcement until the situation is under control and all witnesses have been identified and questioned. Do not leave the safe location or assembly point until law enforcement authorities have instructed you to do so.

Managing the Consequences of an Active Shooter Situation. After the active shooter has been incapacitated and is no longer a threat, Human Capital staff and/or management shall engage in post-event assessments and activities, including:

- 1. An accounting of all individuals at a designated assembly point to determine who, if anyone, is missing and potentially injured.

2. Determining a method for notifying families of individuals affected by the active shooter, including notification of any casualties.
3. Assessing the psychological state of individuals at the scene and referring them to health care specialists accordingly.
4. Identifying and filling any critical personnel or operational gaps left in the organization following the active shooter event.

## **B.5 Required Training**

Supervising Employees - Workplace Violence Awareness Training, via the Federal Emergency Management Agency (FEMA) website at <https://training.fema.gov/is/>

All employees are briefed on Workplace Violence during annual training.

- FEMA: <https://training.fema.gov/is/courseoverview.aspx?code=IS-907;>
- DHS: <https://www.dhs.gov/active-shooter-preparedness>

## **B.6 References**

DOE P 444.1, *Preventing and Responding to All Forms of Violence in the Workplace*

DOE G 444.1-1, *Guide to Preventing and Responding to All Forms of Violence in the Workplace*

DOE O 470.3C, *Design Basis Threat*

DOE O 470.4B, Minor Change 2, *Safeguards and Security Program*, Security Plans

DOE O 473.3A, Minor Change 1, *Protection Program Operations*, Workplace Violence and Active Shooter Plan

DHS Cybersecurity and Infrastructure Security Agency Emergency Action Plan: Active Shooter Template: <https://www.cisa.gov/sites/default/files/publications/active-shooter-emergency-action-plan-template-112017-508.pdf>

---

## **Appendix C — PROTECTIVE FORCE OPERATIONS ACTIVE SHOOTER PLAN (TEMPLATE)**

### **C.1 Purpose**

The purpose of this Active Shooter Plan is to provide guidance to DOE Protective Force (PF) personnel during active shooter response activities and/or emergency conditions. This plan is designed to be annually reviewed and amended as Security Conditions and Department of Energy directives dictate.

### **C.2 Scope**

This plan provides guidance for Security Police Officers (SPO), Security Officers (SO), Central Alarm Station (CAS) Operators and PF Supervision.

### **C.3 Objective**

The primary objective of this plan is to provide PF Supervision and SPOs with initial response direction and information essential for rapid deployment of security forces.

### **C.4. Definitions and Acronyms**

#### **C.4.1 Definitions**

N/A

#### **C.4.2 Acronyms**

CAS	Central Alarm Station
CCTV	Closed Circuit Television
CMA	Corrective Maintenance Action
DOE	Department of Energy
FPS	Federal Protective Services
IMT	Incident Management Team
LLEA	Local Law Enforcement Agency
OSC	On-Scene Commander
PF	Protective Force
SO	Security Officer

SPO      Security Police Officer

## **C.5    Responsibilities**

### **C.5.1    General Manager**

- (1)      Responsible for the content of this plan and the response actions of the PF to address applicable situations.
- (2)      Approve changes to this plan and if this plan is activated, will serve as Senior PF contact for response and/or follow up actions.

### **C.5.2    Director of Operations**

- (1)      Review and approve changes to this plan and is responsible for its implementation.
- (2)      Ensure Facility Commanders and Facility Captains adhere to this plan.

### **C.5.3    Facility Commanders and Facility Captains**

- (1)      Will have the full operational knowledge of the contents of this plan and provide guidance to first line supervisors for implementation.
- (2)      Ensure that PF Supervisors are familiar and comply with this plan.

### **C.5.4    PF Supervisors**

- (1)      Shall be knowledgeable of contents within this plan and be prepared to implement requirements without prior notice.
- (2)      Ensure all SPOs, SOs and CAS Operators are knowledgeable of the contents in this plan.

### **C.5.5    Protective Force Personnel**

PF Officers, CAS Operators and Training personnel must be knowledgeable and perform according to the contents of this plan. Any questions or uncertainties of the duties and responsibilities as outlined in this plan will be directed to PF Supervision.

## **C.6    Overview**

- (1)      PF Supervision in charge will provide command and control guidance.
- (2)      SPOs will conduct assessment, containment, interdiction and reporting activities while disseminating essential elements of information. SPOs will utilize individual/team tactics and tactical decision making capabilities to apply overlapping fields of fire and

observation to appropriate response locations, deny hostile actions and employ neutralization strategies.

- (3) If response actions warrant escalation, SPOs are authorized to use the minimum force necessary, up to and including deadly force, to stop the suspects' actions. Note: SPOs must employ all DOE policy and guidance pertaining to use of force, before applying deadly force.
- (4) If at all possible, SPOs will maintain cover and/or concealment while maintaining observation and reporting capabilities until responding Federal Protective Forces (FPS) and/or Local Law Enforcement Agencies (LLEA) have arrived.
- (5) SOs will assist in observation and reporting.
- (6) PF Supervision will brief the principal agency on the current situation and the placement of containment units as part of the command and control handoff to LLEA.
- (7) This plan will be applied during all potential and actual active shooter situations.
- (8) Upon receipt of a report of an active shooter:
  - (A) CAS will disseminate pertinent information to PF personnel and PF Supervisor in charge to initiate response actions.
  - (B) CAS will use available resources (i.e. alarm system, closed-circuit television (CCTV), quick reaction checklist, verbal reports).
  - (C) Intelligence gathered will be relayed to the PF Supervisor in charge for determination on whether responding forces should escalate or de-escalate response actions. Command and control will be the responsibility of the PF Supervisor in charge.
  - (D) The CAS will make announcements using the pre-scripted messages on the Public Address System.
  - (E) All completed actions will be communicated to the PF Supervisor for validation and resolution before being directed to clear response actions.

#### **C.6.1 Authority**

- (1) SPOs are permitted to apply Limited Arrest Authority and Use of Force in accordance with 10 CFR 1047 and to prohibit criminal trespass under 42 USC 2278a.
  - (A) The PF will be the initial response, command and control and security operations within the building(s) during an active shooter situation.



- (B) Responders' primary goal is to stop and/or contain the suspect(s). Rescuing injured and non-injured employees/citizens will be secondary to stopping the active shooter.
- (C) (FPS/LLEA \_\_\_\_\_) is the primary law enforcement organization for response. The PF can assist both FPS and/or LLEA in emergency situations.

## **C.7 Instructions**

### **7.1 General Alarm Response Plan**

All active shooter responses will be treated as potentially deadly and hostile situations.

### **7.2 Annunciation and Response**

#### **CAS Operator**

Upon receipt of a report of an active shooter, CAS will immediately dispatch in accordance with the initial response procedures.

#### **PF Supervisor**

- (1) The PF Supervisor in charge will acknowledge notification of alarm via radio and if required, move to an area of advantage with good communications to coordinate alarm response actions.
- (2) Based on information received, the PF Supervisor in charge may determine additional post(s) to secure in order to re-deploy SPOs to respond, block, interdict, or search for hostile individual(s) in accordance with the initial response procedures where applicable.
- (3) Posts may be locked down per the PF Supervisor in charge.
- (5) Additional response and/or containment units may be required. Requests for such assistance will be relayed through CAS to the PF Supervisor in charge for determination and resolution.

#### **SPO**

- (1) Responding SPOs will acknowledge notification of active shooter response via radio, proceed to affected area rapidly and by the most tactically sound and direct route available, or a route directed by the PF Supervisor in charge as changing event information is identified.

- (2) PF responders shall employ proper individual and/or team tactics when responding to alarms, while maintaining appropriate response actions for each situation.
- (3) Responding SPOs will advise CAS and the PF Supervisor in charge upon arrival at designated location. All radio communications from responders will be short and concise.
- (4) Responders will assess the immediate and surrounding area(s) to establish containment and/or neutralization of suspect(s) and location. If applicable, responders will supply essential elements of information to CAS and the PF Supervisor in charge for decision on additional requirements.
- (5) Additional response and/or containment units may be required. Requests for such assistance will be relayed through CAS to the PF Supervisor for determination and resolution.

#### **Other PF**

- (1) During an active shooter response, all radio traffic by PF members not directly involved in the response will cease.
- (2) All other posts and patrols will communicate to CAS only information relating to the present threat or additional operational emergencies that arise.

#### **C.7.3 Active Shooter Assessment and Resolution**

Only PF Supervision has the authority to clear response actions during any security related response and/or alarm. Federal Oversight will be made aware of situations as soon as possible.

#### **C.7.4 Confirmed Hostile Actions**

- (1) Entering an affected active shooter area will expose SPOs to imminent danger, (e.g., armed suspect) the PF Supervisor in charge and/or CAS will advise responding units of all known hostile actions and conditions.
- (2) During all responses, responding SPOs will approach with caution and take positions of advantage, e.g. cover.
- (3) SPOs will always attempt to respond and interdict undetected.
- (4) SPOs will use the appropriate level of force based on their “Objective Reasonableness”.

Note: “Objective Reasonableness” is based upon the totality of circumstances known to the SPOs at the moment force was used. When the need for the application of force has been determined, the SPOs shall make their force-option decision based on the actions of the threat or suspect.

- (5) Primary responsibilities will be to seek out and neutralize the threat while maintaining cover and/or concealment, continuing situation containment, observation and reporting capabilities until response actions from FPS and/or LLEA are activated.
  - (A) CAS personnel will notify PF Supervisor in charge upon arrival of LLEA.
- (6) Information gathered during response actions from SPOs and CAS will immediately be disseminated to the PF Supervisor in charge for establishing and implementing a plan of action and/or resolution.
- (7) PF Supervisor in charge will determine actions necessary to mitigate and/or resolve the situation and confirm appropriate measures have transpired before clearing response actions.
- (8) If applicable, PF members will ensure the affected area is secured preventing unauthorized personnel into the area until relieved by PF Supervisor.
- (9) PF shall be aware that when the facility is under lockdown, there is no entry into the facility.
  - (A) The PF Supervisor and/or a SPO, at the direction of the supervisor, will facilitate the entry of LLEA.
  - (B) SPOs shall be aware of the potential for employees and/or the public to panic and make a decision to evacuate instead of sheltering in place during an active shooter situation.
  - (C) It is imperative for SPOs to be highly alert that the adversary may travel further into the facility and/or attempt to exit the facility while concealed within a group or crowd.
- (10) Notifications will be made in accordance with Site/Facility Emergency Response Plan.

#### **C.7.5 Post Emergency Reconstitution**

- (1) This phase is characterized by actions taken by the PF Supervision, the DOE Facility Security Manager, FPS and/or LLEA response forces to restore normal operations and reestablish normal security services to the facility.

- (A) Initiate recall process as necessary.
- (B) Conduct radio checks and accountability of PF personnel.
- (C) Await direction to reestablish normal security operations. (i.e. opening and/or closing posts, establishing comp measures as needed, augmenting personnel requirements, etc.).
- (D) Maintain all crime scenes until directed otherwise.
- (E) Assist as directed with arrival of press, public onlookers and/or family members. Note: There is a “No Comment” policy for all PF members.
- (F) Conduct an after-action analysis, (as soon as possible following the event), with all emergency, response and supervisory personnel, for the purpose of evaluating the effectiveness of emergency plans and actions taken during the event.

#### **C.8 Attachments**

In the event of an active shooter situation, the sites/facilities initial response procedures shall be used as a guide for establishing initial containment positions for the associated posts.

#### **C.9. References**

- 10 CFR 1047, Limited Arrest Authority and Use of Force by Protective Force Officers
- 42 USC 2278a, Trespass on Commission Installations
- DOE O 473.3A, Protection Program Operations
- Site/Facility, Alarm Response Plan
- Site/Facility, Emergency Response Plan

#### **C.10 Forms**

Site/Facility Pre-Scripted Emergency Announcements (Quick Reaction Checklists)

#### **C.11. Records**

All records will be maintained according to the DOE Records Retention and Disposition Schedule.

## **Appendix D — INTERAGENCY SECURITY COMMITTEE RISK MANAGEMENT PROCESS APPLICABILITY**

### **D.1 Policy**

All U. S. Government (DOE) owned or leased properties which do not have security assets (e.g., classified information or matter, SNM, or other assets requiring an Facility Clearance Level (FCL) in accordance with the Facility Clearance section of DOE Order (O) 470.4B, Chg 2), but to which DOE Federal employees are assigned, the standards set forth by the Interagency Security Committee (ISC) under E.O. 12977, ISC, is to be used as the baseline for developing the security plan.

### **D.2 Applicability**

DOE implements the tenets of the ISC Standards, risk identification and management, through the Department's Safeguards and Security Program directives, specifically, DOE O 470.4B Minor Change 2, *Safeguards and Security Program*; DOE O 470.3C, *Design Basis Threat*; and DOE O 473.3A, Change 1, *Protection Program Operations*.

The ISC Standard, *Facility Security Level Determination for Federal Facilities*; and ISC Report, *Design Basis Threat*, are applicable generically to all DOE Federal facilities occupied by Federal employees that meets the tenets set forth by DOE policy.

### **D.3 Compliance Determination:**

- (1) Do facilities operating under your authority have an ISC facility security level (FSL) or DOE Protection Level (PL) determination?
- (2) How often are the FSL/PL determinations and security risk assessments conducted in accordance with ISC/DOE-directed intervals?
- (3) What is the status of the establishment of a protocol to document all decisions, including risk acceptance, pursuant to the ISC Risk Management Process (RMP) and DOE DBT?
- (4) Does the security risk assessment methodology compare to established ISC RMP and DOE DBT criteria (i.e., credible, reproducible, and defensible)?
- (5) Does the security organization use the ISC Design-Basis Threat (DBT) Report or DOE DBT to support the calculation of the facility risk (threat, vulnerability, consequence) when determining the appropriate level of protection?
- (6) Has the program office established communication with the facility security committee (FSC) (or similar decision-making body) for each multi-tenant federal facility they occupy space in?

- (7) Has the FSC representative(s) completed mandated training?
- (8) Has ISC/DOE compliance been verified by the cognizant security office?
- (9) Does the site/facility have written procedures to assist FSCs in resolving issues?
- (10) How often does the site/facility utilize compliance inspections such as Federal survey or independent oversight appraisal?
- (11) Does the site/facility maintain records, inspection reports, and metrics of each of their facilities?
- (12) Does the site/facility maintain a current real property inventory that includes FSL or PL designations?

#### D.4 References

- DOE O 470.4B Minor Change 2, *Safeguards and Security Program*
- DOE O 470.3C, *Design Basis Threat*
- DOE O 473.3A, Change 1, *Protection Program Operations*
- DOE-STD-1192-2018, *Security Risk Management Technical Standard*
- Department of Homeland Security (DHS) ISC Standard, *Facility Security Level Determination for Federal Facilities*
- DHS ISC Report, *Design Basis Threat*
- Interagency Security Committee Policies, Standards, Best Practices, Guidance, and White Papers (<https://www.cisa.gov/isc-policies-standards-best-practices>):
  - *Interagency Security Committee Agency and Facility Compliance Benchmarks*
  - *November 2016/2<sup>nd</sup> Edition – Risk Management Process: An Interagency Security Committee Standard*; including Appendices A through F
  - *2019 Edition – Violence in the Federal Workplace: A Guide for Prevention and Response*

## Appendix E - SECURITY PLAN TEMPLATE

1. OBJECTIVE. The Security Plan (SP) is a risk management document that provides summary information used to describe safeguards and security (S&S) programs and vulnerability and risk assessments at applicable sites. The objective of this section is to delineate SP content and establish a standard approach to presenting site protection information and vulnerability assessment (VA) or Security Risk Assessment (SRA) results. The results and conclusions contained in the plan are intended to guide long-term planning for S&S operations. This is accomplished during plan development by identifying: key protection elements; annually (at least every 12 months) evaluating protection in terms of its adequacy to meet continued mission and threat parameters; and, identifying resource requirements.
2. APPLICATION. The SP is used to evaluate site and facility program elements and resources as they relate to identified threats and risks. The protection measures identified in approved SPs become the basis for executing, and reviewing protection programs.
3. SCOPE. The approved SP provides assurance that S&S measures address identified threats and risks. To provide this assurance, the plan shall reiterate the assumptions identified to and agreed upon by line management. These assumptions shall include reference to the contract under which the site is operated and those contractual issues that may impact S&S, applicable contract requirements, the threat upon which VAs and/or SRAs are based, the methodology used to conduct VAs and/or SRAs, deviations and proposed deviations, and any unique S&S impacting issues and assumptions that were addressed and agreed to by the responsible parties.
4. PURPOSE. The SP describes the graded protection of DOE assets required to be implemented by line management. The SP identifies site risks, cost-benefit analyses, and comparison of proposed upgrades. The resource plan (RP) shall identify near- and long-term resource requirements needed to ensure the integrity of existing and planned S&S upgrades. The annual (at least every 12 months) review serves as the basis for tracking the implementation of protection measures and strategies necessary to maintain system effectiveness and identifies unfunded requirements.
5. PLAN COMPOSITION. The SP includes:
  - a. references to implementing documents and evidence files;
  - b. descriptions of site protection strategies, key site S&S programs, approved and pending deviations, plans and procedures designed to implement, manage and maintain S&S programs;
  - c. system effectiveness determinations for the protection of special nuclear material (SNM), prevention of mitigation of sabotage events, and prevention and/or timely detection of the loss of classified information or matter based on

- the status of performance indicators, such as results of VAs and/or SRAs, performance tests, surveys, inspections, and evaluations of personnel qualifications and training;
- d. proposed S&S program upgrades;
  - e. VA/SRA results that support conclusions reported in the SP;
  - f. assumptions used as part of the VA/SRA process;
  - g. threat parameters used for VAs and/or SRAs that are described in the current DBT, regional threat assessments, and impacts made by local area threat assessments, if applicable;
  - h. the details of the changes in the protection through the spectrum of SECON (1-5), to include effects on the calculated baseline system effectiveness;
  - i. a description of the evidence files containing material that supports the VAs and/or SRAs; and
  - j. a RP that describes S&S upgrades programmed for completion, upgrades being introduced as a result of planned and unplanned site changes impacting the protection program or deficiencies identified as a result of the annual (at least every 12 months) review of the SP, a description of the funding source to implement the upgrades, and unfunded requirements.
6. EVIDENCE FILES. Supporting documentation that validates data/information used in the VA/SRA process and in other protection program planning presented in the plan and that may require corroboration shall be available in evidence files. Evidence files shall be maintained to provide VA/SRA process and other protection program planning documentation in a logical and readily retrievable form to validate assumptions, modeling input data, test results, and other data that may be used to support protection systems design or conclusions regarding protection effectiveness.
7. DATA COLLECTION. The effective date (snapshot in time) of the data contained in the SP shall be specified.
8. FORMAT. Information provided in the SP shall be brief, accurate, and concise. Implementing plans and procedures shall be referenced in the plan where appropriate. A brief overview of a plan or procedure is adequate.

Duplication of information shall be avoided. Information already included in other sections of the plan may be referenced or summarized for clarity.

A cover letter shall be attached to the plan indicating that the plan has been reviewed, risks acknowledged and accepted (if appropriate), and signed by line management. For example, the SP shall be approved by the Head of the Field Element and submitted for



concurrence to the Departmental element. If high or marginal risk acceptance is needed, the correspondence shall be routed for signature to the Secretary of Energy or Deputy Secretary or Under Secretaries, respectively.

The use of charts, plats, graphs, drawings, videos, photographs, and matrixes is encouraged wherever appropriate to clarify or satisfy the intent of plan objectives. References to sources of information and the location of supporting documentation shall be provided to assist in verifying information contained in the plan.

The SP is divided into 12 chapters. Each chapter provides specific information relevant to site security. Use of this layout will ensure a uniform SP for review and comment or during an emergency.

a. Chapter 1, Site Description and Mission.

- (1) Site Mission Statement. Describe the site mission and how the mission relates to national security and the health and safety of the public, employees, and the environment. Describe the major programs or activities performed at the site in terms of mission and their relationship to the DOE national security mission.
- (2) Site Description and Area Layout. Describe the physical and geographical area in which the site and the S&S program are located. Provide a map, photograph, or drawing of the site that identifies locations of Category I facilities, facilities with credible roll-up of SNM to a Category I quantity, the central alarm station (CAS) and secondary alarm stations (SAS), security-related communications facilities, and other facilities of security interest. Show the location of barriers defining the site protected area (PA). A small-scale map or drawing shall be used to show the relationship of the site to the surrounding area and be of sufficient detail to orient the user.
- (3) Management Organization, Planning Assumptions and Evidence File.
  - (a) Site Management Organizations. Identify the contract name, number, and other information that describes the authority under which the contractor executes management functions. Identify site contractors responsible for S&S programs and describe their S&S activities. Provide Federal and contractor organization charts and identify key positions and the relationships between the organizations for S&S activities. Provide a list of roles and responsibilities for key positions. Describe Federal and contractor involvement in the development of S&S resource requirements.
  - (b) Management and Planning Assumptions. Describe those assumptions that were addressed and agreed to during the SP scoping, preparation, or other SP management related meetings.

Describe all relevant S&S-related planning assumptions that were formerly agreed to and included in a Memorandum of Agreement (MOA) by the responsible organization representatives who are party to the development and review of the SP. These assumptions shall address the following issues:

- 1 site SECON;
  - 2 VA/SRA methodology used for insider, neutralization, outsider, and collusion analyses;
  - 3 identified credible targets;
  - 4 protection strategies;
  - 5 approved compensatory measures; and
  - 6 performance testing conducted or to be conducted.
- (c) Evidence Files. Describe and identify the contents, location, and control mechanisms for the SP evidence files. Reference approved local standard operating procedures (SOPs) as applicable. Supporting documentation that validates data/information used in the VA/SRA process shall not be included in the SP. However, this data/documentation shall be available in a logical and readily retrievable arrangement in evidence files, for use in review and validation of the SP.

b. Chapter 2, Site Threat Description and Target Identification.

- (1) Threat Description. Establish a graded approach to protection for Category I SNM and SNM facilities with credible roll-up of SNM to a Category I quantity and facilities having radiological, biological, or chemical sabotage event potential and facilities having disruption of critical mission event potential. Use the DBT as the baseline for threat determination, along with higher levels of threat dictated by local and regional threats (when available), and describe the site-specific threats used as the basis for conducting VAs and/or SRAs and for which the protection program is designed.
- (2) Target Identification. Identify, describe, and prioritize targets of security interest that meet the following criteria.
  - (a) Category I quantities of SNM and the facilities with credible roll-up of SNM to a Category I quantity.

- (b) A radiological, biological, or chemical sabotage inventory that, if released, would cause an unacceptable impact on national security or the health and safety of employees, the public, or the environment.
- (c) Critical national security facilities, and assets (as defined in the DBT), designated by the Department (e.g., or each disruption of critical mission target) that would impact DOE programs supporting national defense and security.
- (d) Those facilities possessing automated information systems that process or contain Sensitive Compartmented Information (SCI), Special Access Program (SAP), and weapon data classified Secret/Restricted Data (S/RD) Sigma 1, 2, 14, and 15 or higher.
- (e) Temporary recurring targets. When predictable programmatic operations can reasonably be expected to present temporary SNM, sabotage, or information targets such as those permanent locations previously described, these targets shall be described and analyzed at the same level of detail and in the same manner as permanent locations.

Provide a brief introductory description of the targets and a chart or list, such as shown below, that indicates the type of target, its location, attractiveness level, size, and configuration.

- (3) Theft or Diversion of SNM. Describe how Category I SNM targets and credible roll-up quantities of SNM to a Category I quantity have been identified and evaluated as potential abrupt theft targets. Also, describe how these SNM targets have been identified and assessed for protracted theft (diversion), if applicable.

For each identified SNM target, provide a description of the following, using a table similar to Table E-1, SNM Theft/Diversion Targets: physical location of identified SNM; the type of material, such as pure products, high-grade material, weapons, including pits, ingots, oxide fuel elements, etc.; and the Category (I through II) and attractiveness level (A through E) of the target material.

**ATTACHMENT 12:**

*Name of Site/Facility/Activity Covered by the Security Plan*  
*Document Number/Revision Number*  
*Date of Federal Approval*

**1 INTRODUCTION****1.1 Overview of Site****1.1.1 Mission****1.1.2 Location/Address****1.2 Scope****1.3 Purpose****2 ROLES AND RESPONSIBILITIES****2.1 Program Office****2.2 Field/Site Office****2.3 Contractors****2.4 ODFSA/ODSA Delegations<sup>i</sup>****3 APPROVAL OF SECURITY PLAN****3.1 Federal Approval of Security Plan<sup>ii</sup>****4 RESIDUAL RISK IDENTIFICATION AND ACCEPTANCE****4.1 Identification of Residual Risk<sup>iii</sup>****4.1.1 Basis for residual risk determination****4.2 Federal Acceptance of Residual Risk<sup>iv</sup>****5 ASSETS****5.1 List of Assets<sup>v</sup>****5.2 Prioritization of Assets<sup>vi</sup>****6 SECURITY PLAN DEVELOPMENT AND REVIEW****6.1 Analytical Basis<sup>vii</sup>**

- 6.1.1 Plan based on DOE O 470.3C, Design Basis Threat, or Interagency Security Committee standards, as applicable<sup>viii</sup>**
    - 6.1.2 DOE Tactical Doctrine, as applicable<sup>ix</sup>**
    - 6.1.3 Security Risk Assessment / Vulnerability Assessment Overview**
  - 6.2 Review and Update<sup>x</sup>**
    - 6.2.1 Review – procedures regarding plan review**
    - 6.2.2 Update – procedures to provide updates and revisions to the plan**

## **7 PROGRAM PLANNING AND MANAGEMENT**

- 7.1 PPM Overview<sup>xi</sup>**
  - 7.1.1 Federal Oversight (Field and Program Office)**
  - 7.1.2 Contractors**
  - 7.1.3 Work-for Others**
- 7.2 Facility Clearance Program<sup>xii</sup>**
  - 7.2.1 Procedures applicable to the FCL program**
- 7.3 Foreign Ownership, Control, or Influence<sup>xiii</sup>**
  - 7.3.1 Procedures applicable to the FOCI program**
- 7.4 Classified Visits<sup>xiv</sup>**
  - 7.4.1 Procedures applicable to classified visits and assignments**
- 7.5 Unclassified Foreign Visitors and Assignments**
  - 7.5.1 Procedures applicable to unclassified foreign visits and assignments<sup>xv</sup>**
- 7.6 Incidents of Security Concern<sup>xvi</sup>**
  - 7.6.1 Overview of the Incident of Security Concern program**
- 7.7 Equivalencies and Exemptions<sup>xvii</sup>**
  - 7.7.1 Overview of the process to create and submit equivalencies and exemptions in accordance with DOE O 251.1D, Departmental Directives Program and other requirements contained in requirements**
  - 7.7.2 List of Approved Equivalencies and Exemptions incorporated in Security Plan<sup>xviii</sup>**
- 7.8 Memorandums of Agreement/Understanding<sup>xix</sup>**
  - 7.8.1 Approval process**
  - 7.8.2 Review Process**
  - 7.8.3 List of all MOAs/MOUs**
- 7.9 SECON<sup>xx</sup>**
  - 7.9.1 Overview of the SECON plan and procedures**

**7.10 Performance Assurance<sup>xxi</sup>****7.10.1 Performance Assurance planning****7.10.2 Performance testing**

## 7.10.2.1 Test schedules

## 7.10.2.2 Results analysis and documents

**7.10.3 System degradation****7.10.4 Reviews and updates****7.11 Safeguards and Security Training<sup>xxii</sup>****7.11.1 Overview of the Safeguards and Security Training program****7.12 Security Awareness Program<sup>xxiii</sup>****7.12.1 Overview of the Security Awareness program****7.13 Security-Funded Technologies, if applicable<sup>xxiv</sup>****7.13.1 Overview of the process to transfer security-funded technologies****7.14 Demonstrator and Protestor Plan<sup>xxv</sup>****7.14.1 Responsibilities****7.14.2 Memoranda of Agreement or Understanding****7.14.3 Event notification****7.14.4 Minimum requirements****7.15 Workplace Violence Plan<sup>xxvi</sup>****7.15.1 Responsibilities****7.15.2 Memoranda of Agreement or Understanding****7.15.3 Event notification****7.15.4 Minimum requirements****8 PHYSICAL SECURITY****8.1 General Site Access<sup>xxvii</sup>****8.1.1 Employees**

## 8.1.1.1 DOE Security Badges

## 8.1.1.2 Local Site-Specific Only Badge

**8.1.2 Visitors<sup>xxviii</sup>**

## 8.1.2.1 Cleared

## 8.1.2.2 Uncleared

## 8.1.2.3 Foreign Nationals

**8.1.3 Other Federal Agency Badges****8.2 Prohibited and Controlled Articles<sup>xxix</sup>****8.2.1 Prohibited Articles****8.2.2 Controlled Articles**

**8.3 Entry and Exit Inspections<sup>xxx</sup>****8.3.1 Entry Inspections procedures****8.3.2 Exit inspection procedures****8.3.3 Property Removal****8.4 Security Areas (as applicable)<sup>xxxi</sup>****8.4.1 General Access Areas**

8.4.1.1 Security Requirements as determined by ODFSA<sup>xxxii</sup>

**8.4.2 Property Protection Areas**

8.4.2.1 Security Requirements as determined by ODFSA, should address, as applicable:<sup>xxxiii</sup>

8.4.2.1.1 Access Control

8.4.2.1.2 Personnel Access

8.4.2.1.3 Vehicle Access

8.4.2.1.4 Intrusion Detection Systems

8.4.2.1.5 Barriers and Delay

**8.4.3 Limited Areas**

8.4.3.1 Access Control<sup>xxxiv</sup>

8.4.3.1.1 Types of access controls employed

8.4.3.1.2 Automated access control

8.4.3.1.2.1 Validation of DOE security badges<sup>xxxv</sup>

8.4.3.1.2.2 Protection of badge verification data<sup>xxxvi</sup>

8.4.3.2 Personnel Access

8.4.3.2.1 Employees – clearance requirements

8.4.3.2.2 Visitors – cleared

8.4.3.2.3 Visitors - uncleared

8.4.3.2.3.1 Escort ratios<sup>xxxvii</sup>

8.4.3.2.3.2 Logging, as applicable<sup>xxxviii</sup>

8.4.3.3 Vehicle Access

8.4.3.3.1 Government vehicles

8.4.3.3.2 Non-Government vehicles<sup>xxxix</sup>

8.4.3.3.3 Emergency vehicles

8.4.3.3.4 Inspection process<sup>xl</sup>

8.4.3.4 Intrusion Detection System, if applicable<sup>xli</sup>

8.4.3.4.1 Types of sensors

8.4.3.4.2 Locations of sensors

8.4.3.4.3 Types of cameras, if applicable

8.4.3.4.4 Locations of cameras, if applicable

8.4.3.4.5 Alarm monitoring

- 8.4.3.4.6 Lighting requirements<sup>xlii</sup>
- 8.4.3.5 Barriers and Delay, as applicable<sup>xliii</sup>
  - 8.4.3.5.1 Hardware<sup>xliv</sup>
  - 8.4.3.5.2 Fencing configuration
  - 8.4.3.5.3 Perimeter barrier gates
    - 8.4.3.5.3.1 Motorized gate controls<sup>xlv</sup>
  - 8.4.3.5.4 Exterior walls
  - 8.4.3.5.5 Ceilings and floors
  - 8.4.3.5.6 Doors<sup>xlvi</sup>
  - 8.4.3.5.7 Windows
  - 8.4.3.5.8 Miscellaneous openings/Penetrations
- 8.4.4 Vaults/Vault-Type Rooms**
  - 8.4.4.1 Access Control<sup>xlvii</sup>
    - 8.4.4.1.1 Types of access controls employed
    - 8.4.4.1.2 Automated access control
      - 8.4.4.1.2.1 Validation of DOE security badges<sup>xlviii</sup>
      - 8.4.4.1.2.2 Protection of badge verification data<sup>xlix</sup>
    - 8.4.4.1.3 Data transmission configuration/control
  - 8.4.4.2 Personnel Access
    - 8.4.4.2.1 Employees – clearance requirements
    - 8.4.4.2.2 Visitors – cleared
    - 8.4.4.2.3 Visitors – uncleared
      - 8.4.4.2.3.1 Escort ratios<sup>l</sup>
      - 8.4.4.2.3.2 Logging, as applicable<sup>li</sup>
  - 8.4.4.3 Vehicle Access, if applicable
    - 8.4.4.3.1 Government vehicles
    - 8.4.4.3.2 Non-Government vehicles
    - 8.4.4.3.3 Inspection process
  - 8.4.4.4 Intrusion Detection System, if applicable<sup>lii</sup>
    - 8.4.4.4.1 Type of sensors
    - 8.4.4.4.2 Locations of sensors
    - 8.4.4.4.3 Types of cameras, if applicable
    - 8.4.4.4.4 Locations of cameras, if applicable
    - 8.4.4.4.5 Alarm annunciation and monitoring
    - 8.4.4.4.6 Lighting requirements<sup>liii</sup>
  - 8.4.4.5 Barriers and Delay, as applicable<sup>liv</sup>



- 8.4.4.5.1 Hardware
- 8.4.4.5.2 Floors and Walls, Type of construction
- 8.4.4.5.3 Windows
- 8.4.4.5.4 Doors
- 8.4.4.5.5 Ceilings

#### **8.4.5 Sensitive Compartmented Information Facilities**

- 8.4.5.1 Overview of security measures provided at the SCIF in accordance with DNI ICD/ICS 705, Technical Specifications for Construction and Management of Sensitive Compartmented Information Facilities<sup>lv</sup>

#### **8.4.6 Special Access Program Facilities**

- 8.4.6.1 Overview of security measures provided at the SAPF in accordance with DOE O 471.5, Special Access Programs<sup>lvi</sup>

#### **8.4.7 Protected Areas**

- 8.4.7.1 Access Control<sup>lvii</sup>
  - 8.4.7.1.1 Types of access controls used
    - 8.4.7.1.1.1 Automated access control
      - 8.4.7.1.1.1.1 Validation of doe security badges<sup>lviii</sup>
      - 8.4.7.1.1.1.2 Protection of badge verification data<sup>lix</sup>
      - 8.4.7.1.1.1.3 Compensatory measures if automated access control system is not functional/implemented<sup>lx</sup>
    - 8.4.7.1.1.2 Armed Protective Force
- 8.4.7.2 Personnel Access
  - 8.4.7.2.1 Employees – clearance requirements<sup>lxi</sup>
  - 8.4.7.2.2 Visitors – cleared
  - 8.4.7.2.3 Visitors – uncleared
    - 8.4.7.2.3.1 Escort ratios<sup>lxii</sup>
    - 8.4.7.2.3.2 Logging<sup>lxiii</sup>
  - 8.4.7.2.4 Entrance/Exit inspection process
    - 8.4.7.2.4.1 Explosive detection
    - 8.4.7.2.4.2 Metal detection
    - 8.4.7.2.4.3 SNM detection
- 8.4.7.3 Vehicle Access
  - 8.4.7.3.1 Government vehicles

- 8.4.7.3.2 Vendor vehicles
- 8.4.7.3.3 Emergency vehicles
- 8.4.7.3.4 Entrance/Exit inspection process
  - 8.4.7.3.4.1 Explosive detection
  - 8.4.7.3.4.2 Metal detection
  - 8.4.7.3.4.3 SNM detection
- 8.4.7.4 Intrusion Detection System
  - 8.4.7.4.1 Types of sensors
  - 8.4.7.4.2 Locations of sensors
  - 8.4.7.4.3 Types of cameras
  - 8.4.7.4.4 Locations of cameras
  - 8.4.7.4.5 Alarm monitoring
  - 8.4.7.4.6 Lighting requirements
- 8.4.7.5 Barriers and Delay
  - 8.4.7.5.1 Overview of the barriers and delays implemented in accordance with the DOE Tactical Doctrine
- 8.4.8 Material Access Areas**
  - 8.4.8.1 Access control
    - 8.4.8.1.1 Types of access controls used
      - 8.4.8.1.1.1 Automated access control
        - 8.4.8.1.1.1.1 Validation of DOE security badges<sup>lxiv</sup>
        - 8.4.8.1.1.1.2 Protection of badge verification data<sup>lxv</sup>
        - 8.4.8.1.1.1.3 Compensatory measures if automated access control systems are not functional/implemented
      - 8.4.8.1.1.2 Armed protective force
  - 8.4.8.2 Personnel Access
    - 8.4.8.2.1 Employees – clearance requirements
    - 8.4.8.2.2 Visitors – cleared
    - 8.4.8.2.3 Visitors – uncleared
      - 8.4.8.2.3.1 Escort ratios
      - 8.4.8.2.3.2 Logging
    - 8.4.8.2.4 Entrance/Exit inspection process

8.4.8.2.4.1 Explosive detection

8.4.8.2.4.2 Metal detection

8.4.8.2.4.3 SNM detection

#### 8.4.8.3 Vehicle Access

8.4.8.3.1 Government vehicles

8.4.8.3.2 Vendor vehicles

8.4.8.3.3 Emergency vehicles

8.4.8.3.4 Entrance/Exit inspection process

8.4.8.3.4.1 Explosive detection

8.4.8.3.4.2 Metal detection

8.4.8.3.4.3 SNM detection

#### 8.4.8.4 Intrusion Detection System

8.4.8.4.1 Types of sensors

8.4.8.4.2 Locations of sensors

8.4.8.4.3 Types of cameras

8.4.8.4.4 Locations of cameras

8.4.8.4.5 Alarm monitoring

8.4.8.4.6 Lighting requirements

#### 8.4.8.5 Barriers and Delay

8.4.8.5.1 Overview of the barriers and delays implemented in accordance with the DOE Tactical Doctrine

### 8.5 Lock and Key Program<sup>lxvi</sup>

#### 8.5.1 Overview of lock and key program

##### 8.5.1.1 Level I

8.5.1.1.1 Issuance

8.5.1.1.2 Control<sup>lxvii</sup>, <sup>lxviii</sup>

8.5.1.1.3 Storage<sup>lxix</sup>

8.5.1.1.4 Destruction

##### 8.5.1.2 Level II

8.5.1.2.1 Issuance

8.5.1.2.2 Control

8.5.1.2.3 Storage<sup>lxx</sup>

8.5.1.2.4 Destruction

##### 8.5.1.3 Level III

8.5.1.3.1 Issuance

8.5.1.3.2 Control

8.5.1.3.3 Storage

8.5.1.3.4 Destruction

8.5.1.4 Use/control/protection of Grand-Master, Master, Sub-Master, and Control keys<sup>lxxi</sup>

**8.5.2 Inventory system<sup>lxxii</sup>**

**9 PROTECTIVE FORCE, IF APPLICABLE<sup>lxxiii</sup>**

**9.1 Management**

**9.1.1 Overview of Pro Force management**

**9.1.2 Non-uniformed staffing**

**9.2 Training**

**9.2.1 Initial**

**9.2.2 Annual**

**9.2.3 Firearms**

9.2.3.1 Training

9.2.3.2 Qualification

**9.3 Certification**

**9.3.1 Medical & Physical**

9.3.1.1 Physical Protection Medical Director Certification

9.3.1.2 Physical Readiness Qualification

**9.4 Staffing**

**9.4.1 Security Officer**

**9.4.2 Fixed Post**

**9.4.3 Security Police Officer (SPO) Is**

**9.4.4 SPO IIs**

**9.4.5 SPO IIIs**

**9.5 Duties**

**9.5.1 Normal duties**

**9.5.2 Emergency duties**

**9.6 Equipment**

**9.6.1 Duty Equipment**

9.6.1.1 Firearms

9.6.1.1.1 Storage

9.6.1.1.2 Transportation

9.6.1.1.3 Pre-positioning

9.6.1.2 Explosives/Pyrotechnics/Ammunition

9.6.1.2.1 Storage

9.6.1.2.2 Transportation

9.6.1.2.3 Pre-positioning

- 9.6.1.3 Non-Lethal
- 9.6.1.4 Body Armor
- 9.6.1.5 Protective Mask
- 9.6.1.6 Radio/Communications
- 9.6.1.7 Personal Protective Equipment

#### **9.6.2 Vehicles**

- 9.6.2.1 Patrol
- 9.6.2.2 Armored, if applicable
- 9.6.2.3 Other

### **10 NUCLEAR MATERIAL CONTROL AND ACCOUNTABILITY, IF APPLICABLE<sup>lxxiv</sup>**

#### **10.1 Characterization of the Nuclear Control and Accountability program<sup>lxxv</sup>**

- 10.1.1 Shall address probability of detection of loss of Category I SNM with 95% probability, if applicable<sup>lxxvi</sup>
- 10.1.2 Shall define loss detection capability for other Categories of SNM<sup>lxxvii</sup>

### **11 PERSONNEL SECURITY<sup>lxxviii</sup>**

- 11.1 Procedures for new clearances
- 11.2 Clearance transfers, extensions, upgrades, downgrades, and cancellations
- 11.3 Reporting requirements

### **12 INSIDER THREAT MITIGATION PROGRAM<sup>lxxix</sup>**

- 12.1 Procedures applicable to the Insider Threat Mitigation Program
- 12.2 Description of Local Insider Threat Working Group (LITWG)
- 12.3 Human Reliability Program, if applicable<sup>lxxx</sup>
  - 12.3.1 Overview of HRP program
  - 12.3.2 Roles and Responsibilities
  - 12.3.3 HRP Certification
  - 12.3.4 HRP Removal
    - 12.3.4.1 Permanent
    - 12.3.4.2 Temporary
    - 12.3.4.3 Reinstatement

### **13 INFORMATION SECURITY**

#### **13.1 Classified Matter Protection and Control<sup>lxxxi</sup>**

- 13.1.1 Procedures utilized to protect classified matter, to include:

13.1.1.1 Document specific techniques to demonstrate that working papers and drafts are “living” documents<sup>lxxxii</sup>

13.1.1.2 Response procedures to respond to IDS alarms<sup>lxxxiii</sup>

13.1.1.3 Electronic transmission<sup>lxxxiv</sup>

13.1.1.4 Nonconforming storage<sup>lxxxv</sup>

13.1.1.5 Destruction

## **13.2 Controlled Unclassified Information<sup>lxxxvi</sup>**

### **13.2.1 Procedures utilized to protect CUI information**

13.2.1.1 UCNI

13.2.1.2 OUO

## **14 CYBER SECURITY<sup>lxxxvii</sup>**

### **14.1 Overview of cyber security program**

### **14.2 Roles and Responsibilities**

#### **14.2.1 Authorizing Official**

## **15 OPERATIONS SECURITY<sup>lxxxviii</sup>**

### **15.1 Overview of the Operations Security program**

### **15.2 Identification and release of controlled information**

## **16 TECHNICAL SECURITY PROGRAM, IF APPLICABLE<sup>lxxxix</sup>**

### **16.1 Overview of the Technical Security program**

## **17 SURVEYS AND ASSESSMENTS<sup>xc</sup>**

### **17.1 Surveys**

#### **17.1.1 Site Office**

#### **17.1.2 Program Office**

### **17.2 Self-Assessments**

### **17.3 Findings and Corrective Actions**

### **17.4 Reviews, Reports and Ratings**

- 
- i. DOE O 470.4B, Paragraph 7.b. and 7.c.
  - ii. DOE O 470.4B, Appendix A, Section 1 Paragraph 5.b. and Attachment 2, Section 1, Paragraph 5.b.
  - iii. DOE O 470.4B, Appendix A, Section 1, Chapter I, Paragraph 1. and Attachment 2, Section 1, Chapter I, Paragraph 1.
  - iv. DOE O 470.4B, Appendix A, Section 1 Paragraph 5.c. and Attachment 2, Section 1, Paragraph 5.b.
  - v. DOE O 470.4B, Appendix A, Section 1, Chapter I, Paragraph 4.a. and Attachment 2, Section 1, Chapter 1, Paragraph 4.a.

- vi. DOE O 470.4B, Appendix A, Section 1, Chapter I, Paragraph 4.a. and Attachment 2, Section 1, Chapter 1, Paragraph 4.a.
- vii. DOE Appendix A, Section 1, Chapter I, Paragraph 3. and Attachment 2, Section 1, Chapter I, Paragraph 3.
- viii. DOE O 470.4B, Appendix A, Section 1, Chapter I, Paragraphs 1.c.-e. and Attachment 2, Section 1, Chapter I, Paragraph 1.c.-e.
- ix. DOE O 470.4B, Appendix A, Section 1, Chapter I, Paragraphs 1.f. and Attachment 2, Section 1, Chapter I, Paragraph 1.f.
- x. DOE O 470.4B, Appendix A, Section 1, Paragraph 5.d. and Attachment 2, Section 1, Paragraph 5.c.
- xi. DOE O 470.4B, Appendix A, Section 1, Chapter I, Paragraph 4.a. and Attachment 2, Section 1, Chapter I, Paragraph 4.a.)
- xii. DOE O 470.4B, Appendix B, Section 1, Paragraph 5 and Attachment 3, Section 1, Paragraph 5.
- xiii. DOE O 470.4B, Appendix B, Section 2, Paragraph 5. and Attachment 3, Section 2, Paragraph 5.
- xiv. DOE O 470.4B, Appendix B, Section 4, Paragraph 5 and Attachment 3, Section 4, Paragraph 5
- xv. DOE O 142.3, Paragraph 4.c.
- xvi. DOE O 470.4B, Appendix B, Section 4, Paragraph 5 and Attachment 3, Section 4, Paragraph 5
- xvii. DOE O 470.4B, Appendix B, Section 4, Paragraph 5 and Attachment 3, Section 4, Paragraph 5
- xviii. DOE O 470.4B, Paragraph 3.c.(2)
- xix. DOE O 473.3A, Appendix A, Annex 3, Paragraph 1.e. and Attachment 2, Annex 2, Paragraph 1.f.
- xx. DOE O 470.4B, Appendix A, Section 1, Chapter II, Paragraph 4 and Attachment 2, Section 1, Chapter II, Paragraph 4
- xxi. DOE 470.4B, Appendix A, Section 1, Chapter III, Paragraph 1 and Attachment 2, Section 1, Chapter III, Paragraph 1
- xxii. DOE O 470.4B, Appendix B, Section 5, Paragraph 5 and Attachment 3, Section 5, Paragraph 5
- xxiii. DOE O 470.4B, Appendix B, Section 4, Paragraph 5 and Attachment 3, Section 4, Paragraph 5
- xxiv. DOE O 470.4B, Appendix B, Section 6, Paragraph 4 (listed as 9) and Attachment 3, Section 6, Paragraph 4
- xxv. DOE O 473.3A, Appendix A, Annex 5 and Attachment 2, Annex 5
- xxvi. DOE O 473.3A, Appendix A, Annex 5 and Attachment 2, Annex 5
- xxvii. DOE O 473.3A, Attachment 3, Section A, Chapter II, Paragraphs 2., 3., 4.
- xxviii. DOE O 473.3A, Attachment 3, Section A, Chapter XI, Paragraph 1.
- xxix. DOE O 473.3A, Attachment 3, Section A, Paragraph 8.
- xxx. DOE O 473.3A, Attachment 3, Section A, Chapter X, Paragraph 1.
- xxxi. DOE O 470.4B, Appendix A, Section 1, Chapter I, Paragraph 1 and
- xxxii. DOE O 473.3A, Attachment 3, Section A, Chapter IV, Paragraph 2.a.
- xxxiii. DOE O 473.3A, Attachment 3, Section A, Chapter IV, Paragraph 3.a
- xxxiv. DOE O 473.3A, Attachment 3, Section A, Chapter II, Paragraphs 2., 3., 4.
- xxxv. DOE O 473.3A, Attachment 3, Section A, Chapter II, Paragraph 4.c.(3)(a)
- xxxvi. DOE O 473.3A, Attachment 3, Section A, Chapter II, Paragraph 4.c.(3)(e)
- xxxvii. DOE O 473.3A, Attachment 3, Section A, Chapter II, Paragraph 4.c.(1)
- xxxviii. DOE O 473.3A, Attachment 3, Section A, Chapter II, Paragraph 4.c.(2)(a)
- xxxix. DOE O 473.3A, Attachment 3, Section A, Chapter II, Paragraph 4.d.(2)
- xl. DOE O 473.3A, Attachment 3, Section A, Chapter II, Paragraph 4.d.(3)
- xli. DOE O 473.3A, Attachment 3, Section A, Chapter II, Paragraphs 2., 3., 4. and DOE O 473.3A, Attachment 3, Section A, Chapter III, Paragraph 1
- xl.ii. DOE O 473.3A, Attachment 3, Section A, Chapter III, Paragraph 4.b.
- xl.iii. DOE O 473.3A, Attachment 3, Section A, Chapter II, Paragraphs 2., 3., 4.
- xl.iv. DOE O 473.3A, Attachment 3, Section A, Chapter VI, Paragraph 3
- xl.v. DOE O 473.3A, Attachment 3, Section A, Chapter VI, Paragraph 5
- xl.vi. DOE O 473.3A, Attachment 3, Section A, Chapter VI, Paragraph 8
- xl.vii. DOE O 473.3A, Attachment 3, Section A, Chapter VIII, Paragraph 1.b.(2)
- xl.viii. DOE O 473.3A, Attachment 3, Section A, Chapter II, Paragraph 4.c.(3)(a)
- xl.ix. DOE O 473.3A, Attachment 3, Section A, Chapter II, Paragraph 4.c.(3)(e)
- l. DOE O 473.3A, Attachment 3, Section A, Chapter II, Paragraph 4.c.(1)
- li. DOE O 473.3A, Attachment 3, Section A, Chapter VIII, Paragraph 1.b.(3)
- lii. DOE O 473.3A, Attachment 3, Section A, Chapter II, Paragraphs 2., 3., 4. and DOE O 473.3A, Attachment 3, Section A, Chapter III, Paragraph 1
- lii.iii. DOE O 473.3A, Attachment 3, Section A, Chapter III, Paragraph 4.b.

- liv. DOE O 473.3A, Attachment 3, Section A, Chapter II, Paragraphs 2., 3., 4.
- lv. DOE O 473.3A, Attachment 3, Section A, Chapter II, Paragraph 5.c.
- lvi. DOE O 473.3A, Attachment 3, Section A, Chapter II, Paragraph 5.a.
- lvii. DOE O 473.3A, Attachment 3, Section A, Chapter VIII, Paragraph 1.b.(2)
- lviii. DOE O 473.3A, Attachment 3, Section A, Chapter II, Paragraph 4.c.(3)(a)
- lix. DOE O 473.3A, Attachment 3, Section A, Chapter II, Paragraph 4.c.(3)(e)
- lx. DOE O 473.3A, Attachment 3, Section C, Chapter I, Paragraph 4.c.
- lxi. DOE O 473.3A, Attachment 3, Section C, Chapter I, Paragraph 4.c.(1)(c)
- lxii. DOE O 473.3A, Attachment 3, Section C, Chapter I, Paragraph 4.c.(1)(b)1
- lxiii. DOE O 473.3A, Attachment 3, Section C, Chapter I, Paragraph 4.c.(1)(b)3
- lxiv. DOE O 473.3A, Attachment 3, Section A, Chapter II, Paragraph 4.c.(3)(a)
- lxv. DOE O 473.3A, Attachment 3, Section A, Chapter II, Paragraph 4.c.(3)(e)
- lxvi. DOE O 470.4B, Appendix A, Section 1, Chapter I, Paragraph 1. and Attachment 2, Section 1, Chapter I, Paragraph 1.
- lxvii. DOE O 473.3A, Attachment 3, Section A, Chapter IV, Paragraph 5.b.
- lxviii. DOE O 473.3A, Attachment 3, Section A, Chapter IV, Paragraph 4.d.
- lix. DOE O 473.3A, Attachment 3, Section A, Chapter IV, Paragraph 5.c and Paragraph 6.b.
- lxx. DOE O 473.3A, Attachment 3, Section A, Chapter IV, Paragraph 5.c and Paragraph 6.b.
- lxxi. DOE O 473.3A, Attachment 3, Section A, Chapter IV, Paragraph 1.b.
- lxxii. DOE O 473.3A, Attachment 3, Section A, Chapter IV, Paragraph 4.a.
- lxxiii. DOE O 473.3A, Attachment 3, Section A, Chapter II, Paragraphs 2., 3., 4.
- lxxiv. DOE O 470.4B, Appendix A, Section 1, Chapter I, Paragraph 1 and
- lxxv. DOE O 474.2, Attachment 3, Paragraph 1.u.
- lxxvi. DOE O 474.2, Attachment 3, Paragraph 2.d.
- lxxvii. DOE O 474.2, Attachment 3, Paragraph 2.e.
- lxxviii. DOE O 470.4B, Appendix A, Section 1, Chapter I, Paragraph 2
- lxxix. DOE O 470.4B, Appendix A, Section 1, Chapter I, Paragraph 1. and Attachment 2, Section 1, Chapter I, Paragraph 1.
- lxxx. DOE O 473.3A, Attachment 3, Section A, Chapter II, Paragraphs 2., 3., 4.
- lxxxi. DOE O 471.6, Paragraph 4.a.(3)
- lxxxii. DOE O 471.6, Paragraph 4.b.(2)(g)
- lxxxiii. DOE O 471.6, Paragraph 4.b.(5)(i)
- lxxxiv. DOE O 471.6, Paragraph 4.b.(7)(a)5
- lxxxv. DOE O 471.6, Paragraph 4.b.(5)(j)
- lxxxvi. DOE O 470.4B, Appendix A, Section 1, Chapter I, Paragraph 1. and Attachment 2, Section 1, Chapter I, Paragraph 1.
- lxxxvii. DOE O 470.4B, Appendix A, Section 1, Chapter I, Paragraph 1. and Attachment 2, Section 1, Chapter I, Paragraph 1.
- lxxxviii. DOE O 470.4B, Appendix B, Section 4, Paragraph 5 and Attachment 3, Section 4, Paragraph 5
- lxxxix. DOE O 470.4B, Appendix B, Section 4, Paragraph 5 and Attachment 3, Section 4, Paragraph 5
- xc. DOE O 470.4B, Appendix A, Section 2, Paragraph 5 and Attachment 2, Section 2, Paragraph 5



**Table E-1 Example of SNM Theft/Diversion Targets**

<b>Location</b>	<b>SNM Type</b>	<b>Category/Attractiveness Level</b>	<b>Goal Quantity/Portability</b>
Bldg. 1, Vault	Pu-239 ingots	Cat. I/B	2 ingots/man portable
Bldg. 1, Assay Room	Pu-239 ingots	Cat. I/B	2 ingots/man portable
Bldg. 1, Fabrication Room	Pu-238 oxide powder	Cat. II/D	2 canisters/ man portable
Bldg. 2	U-235 fuel elements	Cat. II, roll-up to Cat. I/C	20 fuel elements/not man portable
Bldg. 3	U-235 fuel elements	Cat. II, roll-up to Cat. I/C	20 fuel elements/not man portable

- (4) **Radiological Sabotage.** Indicate the process or methodology used to identify and evaluate radiological sabotage targets.

For each identified radiological sabotage target, provide a description using a table similar to Table E-2, Radiological Sabotage Targets, of the following: the physical location of all identified targets; the type of material; the maximum inventory level; and the material size and configuration.

- (5) **Biological or Chemical Sabotage.** Describe the methodology used to evaluate biological or chemical targets. Using the criteria referenced in the DBT, determine the sabotage threat level (STL) for each location. Reference the plans and procedures that govern the biological or chemical sabotage assessment program.

For each identified target type not addressed by the commercial equivalency protection program, provide a description of the following using a table similar to Table E-3, Biological/Chemical Sabotage Targets: the physical location of additional identified biological or chemical sabotage material targets; the type of material; the maximum inventory level; the material size and configuration; and, the exposure level at the near-site boundary (NSB) for maximum inventory release.

**Table E-2. Example of Radiological Sabotage Targets**

Location	Material Type	Maximum Inventory	Material Size and Configuration
Bldg. 1, Fabrication Room	Pu-238 oxide powder	10kg	Paint cans, at 50g each
Bldg. 4	H <sub>3</sub> gas	10kg	Cylinders, at 500g each

**Table E-3. Example of Biological/Chemical Sabotage Targets**

Location	Material Type	Maximum Inventory	Material Size and Configuration	Exposure Level at NSB
Bldg. 5	Chlorine	10,000 lb.	55-gal drums at 350 lb. each	>ERPG III Levels

- (6) Disruption of Critical Mission Sabotage. Describe how potential disruption of critical mission sabotage production and process components (machinery, equipment, flow process, power sources, ventilation, waste handling, etc.) have been identified and evaluated for inclusion as disruption of critical mission targets. Ensure that the evaluation includes how the sabotage event would affect production (at the facility, on intersite processes, and on overall national level inventory needs) and, if so, what areas, processes, and/or components within the facility affect those necessary production level capabilities and inventory needs.

For each disruption of critical mission target, provide a description, using a chart similar to Table E-4, of the following: the physical location of essential production components; the type of equipment, process, power sources, or vital components; and the dollar value or production capability loss.

- (7) Intra-Site Transportation of SNM. Describe in a brief narrative the Category I SNM targets and credible Category II SNM targets that roll up to Category I quantity that are moved from one location to another on the site on a recurring basis.

Using a chart, identify the type of SNM, attractiveness level, and size and configuration of the material.

**Table E-4. Example of Disruption of Critical Mission Targets**

<b>Location</b>	<b>Equipment Type</b>	<b>Loss of DOE Mission Capability and Mission Impact</b>
Bldg. 1, Fabrication Room	Fuel Fabrication Presses	100% loss of capability for 360 days with moderate mission impact
Lab. A	Laser Tunnel	100% loss of capability for 360 days with low mission impact

- c. Chapter 3, Site Protection Strategies. Identify the protection strategies employed that address the overall protection program and enhance the concept of graded protection. Describe the protection program strategies employed. The basic strategies pertaining to protection are denial of access, denial of task and containment that upon failure could evolve into recapture/recovery or pursuit strategies. Protection programs and tactical deployments designed to prevent unauthorized control of material and devices and to prevent acts of radiological, biological, chemical, and disruption of critical mission shall be integrated with protection strategies. These activities could include protection layers of intrusion detection systems (IDS) and concentric security areas, access control measures, compartmentalization, insider protection programs, and procedural measures. The plan shall clearly convey the strategy to be employed, and plan reviewers will anticipate that procedures are available to ensure implementation of these strategies. Display in a chart similar to Table E-5, Site-Wide Protection Strategies, the protection strategy used, the facility and target involved, and the title and responsible office for each plan or procedure. Ensure the information provided is consistent with that found in Chapter 2, Site Threat Description and Target Identification.
- d. Chapter 4, Physical Protection Systems.
- (1) Summary of Physical Protection Systems Used for Category I and Credible Roll-Up Quantities of SNM to a Category I Quantity, Sabotage, Classified Information or Matter, and Classified Automated Information Protection. Describe the physical protection systems for each facility that has Category I quantities of SNM; credible roll-up quantities of SNM to a Category I quantity; and radiological, biological, chemical, and sabotage targets (including disruption of critical mission) and those facilities possessing automated information systems that process or contain SCI, SAP, weapon data classified S/RD Sigma 1, 2, 14, and 15, or higher. Provide a narrative description of the physical protection systems and how these systems are integrated at the site and facility level. Describe how physical protection systems (access control, intrusion detection, assessment, etc.) are implemented to allow the PF to focus resources on its primary mission of defeating an armed terrorist threat. Describe how the barriers are protected by an IDS, security

lighting, protective force (PF), and assessment systems and how structures located in or on the barrier are protected so as not to degrade protective systems. Describe the design of barrier systems used to deny vehicle approach routes to critical targets.

Following the narrative, complete a chart similar to Table E-6, Facility Protection Systems, that includes the following facility protection systems: security areas and their barriers, access controls (automated card access for both interior and exterior locations and contraband screening by the PF at Protected and Material Access Areas); assessment (closed circuit television (CCTV) and/or PFs both interior and exterior); security computer system integrator/ processor; CAS and SAS; CCTV cameras monitoring and switching systems; security lighting; electrical and backup power sources (emergency batteries and/or generators); and communications. In the chart, list the major physical protection systems, the location of the systems, and a brief description of the type of equipment installed.

**Table E-5. Example of Site-Wide Protection Strategies**

<b>Protection Strategy</b>	<b>Facility or Activity</b>	<b>Target Type</b>	<b>Implementing Plan or Procedure</b>	<b>Responsible Office</b>
Denial of Access	Facility ABC	Cat. I: Pu metal oxide Cat. II: nitrate UF <sub>6</sub>	Plan ABC 1.3	Protective Force Manager
Containment	Vault Storage Areas 301, 302, and 303	Weapon Parts and Pu metallic buttons	Plan ADC.1	Protective Force Manager
Denial of Task	SNM in Transit	Weapons Parts	Plan CFE 1.5	Protective Force Manager

- (2) Physical Protection Measures for Category I and Credible Roll-up Quantities of SNM to a Category I Quantity in Transit (Onsite). Describe the types, frequency, and protection measures used for the intra-site shipment of Category I SNM and credible roll-up quantities to a Category I quantity. Provide a narrative that describes the typical physical protection measures taken to ensure the integrity of those shipments from their point of loading, through transit, and at the off-load destination. If other materials are transported onsite that would represent a STL-1 concern, provide a narrative that describes the typical physical protection measures from their point of loading, through transit, and at the off-load destination.

**Table E-6. Example of Facility Protection Systems**

<b>Protection System</b>	<b>Equipment Description</b>	<b>Location</b>	<b>Responsible Office</b>
Exterior Intrusion Detection	“H” Field	Protected Area Perimeter Associated Areas	Office of the Plant Engineer
Exterior Assessment/CCTV	Microwave Taut Wire CCTV System	Protected Area Perimeter Associated Areas	Office of the Plant Engineer
Interior Intrusion Detection	Volumetric Infrared Motion Detectors	All Material Access Areas	Office of the Plant Engineer

e. Chapter 5, Site PF.

- (1) PF Mission, Organization, and Capabilities. Describe the PF organization and equipment deployed to perform 24-hour-per-day protection. Confirm that the basis for PF organization and planning is based on the identified site threat. Provide a narrative summary of the PF mission(s), capabilities, and deployment concepts used for site protection. Describe the methods used to review and prioritize post assignments priorities and eliminate posts that detract from combat readiness at high priority sites. Indicate the availability of plans and procedures that address normal and emergency deployment. Describe the PF equipment used including firearms, communications, vehicles, and any special items. Provide an organization chart of the PF, including response forces, showing the management and organization structure and key organizational interface positions with the cognizant security authorities and site operations and safety organizations. Using a schematic, display the PF communications network and include available secure networks and linkages to offsite law enforcement organizations with whom support agreements exist. In a chart, show the weapons and special equipment assigned to PF personnel, including members of the response force.
- (2) Qualifications and Training. Indicate that the qualifications for hire and training of the PF conform to current policy requirements. In a chart similar to Table E-7, Qualifications and Training, list the titles and offices responsible for implementing and maintaining the plans or procedures that describe the following pertaining to the PF: qualifications for employment and the hiring process; initial, specialized and advanced training; tactical performance testing program; and other relevant written documentation, such as post and general orders that enhance the efficiency and effectiveness of the PF.
- (3) Special Response Teams (SRT) and Plans. Ensure the availability of SRTs and current response plans and procedures for implementing site-specific S&S program strategies and tactics for denial of access, denial of

task, containment, recapture/recovery, pursuit, and contingency operations, as described in current DOE policy. Indicate that requalification training and exercises are used to verify the effectiveness of SRTs. Identify and document agreements and MOUs with local, State and Federal law enforcement agencies regarding requests for on-site support during a contingency event. Ensure that a VA was used to assist management in determining the equipment and deployment of SRTs. In a brief narrative, confirm the availability of personnel and response plans and procedures that provide assurance of adequate protection. Indicate that contingency plans and procedures are available to respond to the activities listed below.

- (a) Containment/denial of access/denial of task (includes a range of tactical options designed to either preclude adversary force access to nuclear weapons/materials or to deny unauthorized removal).
- (b) Recapture/recovery or pursuit operations (used when containment/denial fail and could involve SRTs and other force options including the use of off-site law enforcement agencies).

Describe the organization, equipment, and training provided to SRTs and how training and performance testing are used to verify the effectiveness of SRT planning in the strategies described above. Describe the role of vulnerability analysis in determining SRT deployment, equipment, and training.

In a chart similar to Table E-7, list tactical response plans and procedures and the office responsible for implementing and maintaining them.

Use a similar chart to list memoranda or letters of understanding and other agreements with local, State, or Federal law enforcement agencies regarding requests for onsite support during a contingency event.

**Table E-7. Example of Qualifications and Training**

<b>Plans/Procedures Title</b>	<b>Responsible Office</b>
Specialized Training Plan	Training Department
Tactical Response Plan	

- f. Chapter 6, MC&A Program. Describe the MC&A management program and summarize the results of the MC&A vulnerability analyses and other MC&A program planning activities. Describe the mission of the site MC&A organization. Summarize current and planned nuclear materials processing and storage activities. Using an organization chart, show the MC&A organization

and management structure and the lines of authority and points of interface with other S&S programs, facility operations, and the cognizant security authorities' MC&A organization. Describe the functions and responsibilities of safeguards personnel and indicate how MC&A activities are integrated with those of site protection programs and other facility organizations; include organizational responsibilities for those program elements that support multiple S&S programs (e.g., portal monitors and access controls). Confirm that MC&A personnel complete required training.

List, in a chart similar to Table E-8, MC&A Plans and Procedures, the facilities required to develop and maintain MC&A plans and procedures, the titles of those plans and procedures, and the office(s) responsible for approving and maintaining them.

**Table E-8. Example of MC&A Plans and Procedures**

Facility Name	Plan/Procedure Title	Responsible Office
ABC Facility	ABC Facility MC&A Plan, 1/1/99	S&S Director
XYZ Facility	XYZ Facility MC&A Plan, 6/9/99	S&S Director

Give the name(s) and date(s) of reports of MC&A VAs and/or SRAs and other planning exercises. Summarize the results of these assessment(s). Identify those components of the MC&A system that provide the greatest effectiveness against theft and diversion. Describe actions taken to remediate identified program deficiencies or to prepare for planned changes in facility nuclear materials processing and storage activities.

- g. Chapter 7, Site Personnel Security/Human Reliability Programs (HRP). Describe the site-wide program for personnel security that, in conjunction with information and physical security programs, ensures only authorized access to classified information or matter, or SNM and confirms that the personnel security program is in conformance with and implements the requirements prescribed in current DOE policy. Describe the key elements of the site-wide personnel security program for access authorizations and, if applicable, the key elements of the site's HRP. Describe the method(s) used at the site to ensure the appropriate level of access authorizations are issued for the category of material processed or stored at the site and for approving justification, processing, and reevaluating the need for such access authorizations. Indicate how the effectiveness of the program is assessed. Indicate the site procedures that require contractors to perform pre-hire checks to ensure proper qualifications and suitability of the applicant before submitting requests for access authorizations. Briefly describe the programs used to mitigate the effectiveness of potential



“insider” activities and the application of these programs in addressing insider concerns. Provide an organization chart showing the location of the personnel security organization in relationship to the cognizant security authority and other contractor S&S organizations. Provide an organization chart identifying the designated HRP management official in relationship to the cognizant security authority and the designated HRP certifying official. Verify that the site has a current HRP implementation plan. List, in a chart similar to Table E-9, Personnel Security/Human Reliability Program Implementation, the titles of site-wide personnel security-related plans and procedures, the HRP implementation plan, if applicable, and the office(s) responsible for implementing and maintaining them.

**Table E-9. Example of Personnel Security/Human Reliability**

Plan/Procedure Title	Responsible Office
XYZ Implementation Plan	Security Department

- h. Chapter 8, Automated Information Security Program. Briefly describe the automated information systems for those facilities possessing automated information systems that process SCI, SAP, weapons data classified S/RD Sigma 1, 2, 14, and 15, or higher. Provide an organization chart showing the responsible automated information systems security program and its relationship to the cognizant security authority and contractor organizations.

List, in a chart similar to Table E-10, Automated Information Systems Security Programs, the title of the automated information systems security program plans and procedures with the associated office responsible for implementing and maintaining the plan and procedures, the plans and procedures governing the automated information system VAs and/or SRAs with the associated office responsible for implementing and maintaining the plan and procedures, and the reports containing the results of the VAs and/or SRAs.

- i. Chapter 9, S&S Equipment Maintenance and Testing Programs. Describe maintenance and testing programs and life cycle planning, designed to enhance the continuous operability of S&S-related equipment used in the protection of Category I SNM, (including areas with credible rollup of SNM to a Category I quantity), and classified automated information systems. Summarize, in a narrative, the maintenance and testing programs that ensure the availability and operability of S&S-related equipment and systems. Indicate the availability of compensatory measures/procedures that are used when equipment is taken out of service or otherwise not available. Describe how S&S maintenance and testing programs are incorporated into the Performance Assurance Program Plans.



Indicate how the performance testing and other S&S site and facility maintenance programs comply with DOE policy.

Describe the life cycle planning conducted for major S&S equipment and component replacement. Relate how this planning is used to support and validate S&S equipment budget requirements.

**Table E-10. Example of Automated Information Systems Security Programs**

Plan/Procedure/Report Title	Responsible Office	Date (if pertinent)

List, in a chart similar to Table E-11, the maintenance, testing, and records management programs; the relevant plans and procedures that implement the programs; and the responsible office, as these programs apply to equipment used by the PF, security related systems, and equipment and instrumentation used for MC&A. Many of these may be addressed in a single maintenance and testing program.

Describe the records management program used for scheduling, recording, and tracking identified S&S maintenance requirements, deficiencies, and testing schedules.

- j. Chapter 10, Site Protection Evaluation Program. Chapter 10 is designed to ensure the availability and use of testing and evaluation programs for site S&S programs and systems.

In a narrative, describe the programs available and used to evaluate the effectiveness of S&S protection programs and the interaction of these evaluation tools (i.e., surveys may focus on shortfalls found in security inspections). Include in this narrative outline the PF tactical performance testing program describing the evaluation mechanisms used by line management. At a minimum, the programs described in Chapters 4, 5, 6, and 8 of the SP shall be addressed and the evaluation plan or procedure identified. In a chart similar to Table E-12, Site Protection Program Evaluation Program, list the names of the evaluation plans/procedures used by the cognizant security authority to assist in determining the effectiveness of site and facility protection programs and systems. List the office responsible for the evaluation plan/procedure and its purpose.

Indicate, in a brief description, that performance testing is used to verify the effectiveness of S&S systems/programs and to validate vulnerability analysis

activities. Additionally, briefly describe barriers and other systems that cannot be adequately performance tested to demonstrate protection capabilities and their integration into protection strategies due to physical, operational, or policy parameters.

- k. Chapter 11, Deviations from DOE Contractor Requirements. List all deviations that have been approved. In a table similar to Table E-13, Deviations from DOE contractor requirements, list the deviation, the officially assigned deviation number, the directive reference (DOE contractor requirement and section within the contractor requirement), and the dates the deviation was approved and expires.

Provide similar information for those deviations pending approval. This information shall be displayed in a chart similar to Table E-14, Pending Deviations from DOE Contractor Requirements.

- l. Chapter 12, Summary of VA and SRA Results.
- (1) Executive Summary. Summarize the vulnerability analyses and risk assessments results for Category I SNM, (including credible roll up of SNM to a Category I quantity), theft targets, radiological, biological, and chemical sabotage targets, and disruption of critical missions. Confirm in the narrative that performance testing was used to validate VA/SRA input data and the results of the vulnerability analyses. Following the narrative, complete a matrix similar to Table E-15, Summary of Identified Risks, which identifies the risk associated with the results of the VA and/or SRA. In Part 10 of the matrix, summarize the proposed corrective actions or upgrades. For line item construction project (LICP) work or other major capital expenditures, cite the source of the required funding. Use the RP information as the basis for this summary.
  - (2) Scope. Describe the targets to be covered, the items/issues to be excluded, and the limits on the conduct of the VAs and/or SRAs in this SP.

**Table E-11. Example of S&S-Related Maintenance, Testing, and Records Management Programs**

Program Area	Plan/Procedure Title	Test Plan or Management Plan	Responsible Office/Organization
PF			
- Equipment			
- Training Courses			
- Firearms Qualification			
- Other			
Vehicles/Aircraft			
Communications			
MC&A			
Security Systems			
- Personnel Access and Inspection Equipment			
- Security Lighting			
- Intrusion Detection and Assessment Systems			
- Electrical Power Supplies			
Sensitive Area Access Control			
Survey/Inspection Deficiencies			

**Table E-12. Example of Site Protection Program Evaluation Program**

Plan/Procedure Title	Responsible Office	Plan or Procedure Goal/Purpose
Performance Assurance Program	Contractor Manager	Establish/confirm system effectiveness
DOE/Contractor Self-Assessment Program	Program Manager	Identify program strengths /weaknesses
Facility Approval, Security Surveys	Cognizant Security Authority	Confirm availability and adequacy of required S&S programs
Force on Force Exercises	Contractor Manager	Confirm system effectiveness
Limited Scope Performance Tests	Contractor Manager	Confirm system effectiveness
Joint Tactical Simulation Model	Contractor Manager	Confirm system effectiveness

**Table E-13. Example of Deviations from DOE Contractor Requirements**

Deviation Description	Deviation Number	CRD Directive Reference	Approval and Expiration Dates

**Table E-14. Example of Pending Deviations from DOE Contractor Requirements**

Deviation Description	Deviation Number	CRD Directive Reference	Approval and Expiration Dates

(3) Methodology.

- (a) Theft or Diversion of SNM. Identify the SNM targets subject to theft and/or diversion. Describe the rationale and mechanism used to identify these targets.

Using a table similar to Table E-16, SNM Theft/Diversion Targets, provide a description for each identified SNM target consisting of the following: the physical location of identified SNM; the type of material (such as pure products, high grade material, weapons, etc.) which could include pits, ingots, oxide fuel elements, etc.; the Category (I through II) and attractiveness level (A through E) of the target material; and the size and portability of the theft target.

- (b) Radiological Sabotage. Identify the radiological targets subject to sabotage. Describe the rationale and mechanism used to identify these targets. A key source of information to assist in the identification and/or elimination of radiological targets is the facility safety analysis report. Using a table similar to Table E-17, Credible Radiological Sabotage Targets, provide a description for each identified radiological sabotage target consisting of the following: the physical location of all identified targets, the type of material, the maximum inventory level, and the material size and configuration.
- (c) Biological Sabotage. Identify the biological targets subject to sabotage. Describe the rationale and mechanism used to identify these targets. Reference any policy and analyses external to the

SP that address biological targets. Using a table similar to Table E-18, Credible Biological Sabotage Targets, provide a description for each identified biological sabotage target consisting of the following: the physical location of all identified targets, the type of material, the maximum inventory level, and, the material size and configuration.

- (d) Chemical Sabotage. Identify the chemical targets subject to sabotage. Describe the rationale and mechanism used to identify these targets. Indicate whether security protection provided for chemical sabotage targets is comparable to that provided by the commercial sector for similar materials. A key source of information to assist in the identification and/or elimination of chemical targets is the facility safety analysis report. Reference any policy and analyses external to the SP that address chemical targets.

Using a table similar to Table E-19, Credible Chemical Sabotage Targets, provide a description for each identified chemical sabotage target consisting of the following: the physical location of all identified chemical sabotage targets, the type of material, the maximum inventory level, how the security provided is not comparable to that of the commercial sector, the material size and configuration, and the exposure level at the NSB for maximum inventory release.

- (e) Disruption of Critical Mission. Identify the disruption of critical mission targets. Describe the rationale and mechanism used to identify these targets. Ensure that the evaluation includes how the disruption would cause an unacceptable impact on national security.

Using a table similar to Table E-20, Disruption of Critical Mission Targets, provide a description for each identified target consisting of the following: the physical location of the target; a description of the function of the target; the impact to national security; and the estimated time for recovery.

**Table E-15. Example of Identified Risks Summary**

Target Number	Target Location and Description	Threat Type and Number	Risk Rating (High, Moderate, Low)						Remarks	Analyses Validated by Perf. Testing
			Base Case	Current Modif. Rating (date)	Protected Action and Adjusted Rating: Near-Term (<2 yr) (date)		Protected Action and Adjusted Rating: Long-Term (>2 yr) (date)			
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)
SNM Theft Targets										
1	Glovebox 112-A Bldg. 222	Terrorist, X outsiders with help of insider	High	High	Relocate SI to access door	Mod	Harden access portal	Low	Install hardware to allow SL relocation (FY-89 GPP)	Yes
2	Test samples in NDA room, Bldg. 222	Criminal Insiders	High	High	Enhance HRP for NDA technicians and supervisors	High	Install CCTV recording for post-review of activities in NDA room	Mod	SNM protection unchanged, but probability of attempt reduced thru HRP and delayed assessment capability	Yes
Radiological Sabotage Targets										
3	Test reactor #5 North Area, Bldg. 408	Insider	Mod	Mod	Reinforce SI number when in use	Low	None	Low	Use overtime when reactor in use-3 times per year	No
Chemical Sabotage Targets										
4	Laboratory Bldg. 4	Insider	Mod	Mod	None	Low	None	Low	None	No
Biological Sabotage Targets										
5	Fabrication Room, Bldg. 1	Insider	Mod	Mod	None	Low	None	Low	None	No
Disruption of Critical Mission Targets										
6	Access port 4 D-line process line, Bldg. 460	Disgruntled employee	High	Mod	Implement 2-man rule	Low	Harden and remote control of portal	Low	Install hardware to reduce high manpower costs (use FY-92 GPP)	Yes
7	Extrusion equipment in fuel manufacturing area, Bldg. 97	Psychotic employee	High	High	Establish spares inventory for long lead time parts	Mod	Identify alternate extrusion capability off-site	Low	Additional physical protection not cost-effective. Improved spares also provide repair capability for non-sabotage outages	Yes

**Table E-16. SNM Theft/Diversion Targets**

Location	SNM Type	Category/Attractiveness Level	Goal Quantity/Portability
Bldg. 1, Vault	Pu-239 ingots	Cat. I/B	2 ingots/ man portable
Bldg. 1, Assay Room	Pu-239 ingots	Cat. I/B	2 ingots/ man portable
Bldg. 1, Fabrication Room	Pu-238 oxide powder	Cat. II/D	2 canisters/ man portable
Bldg. 2	U-235 fuel elements	Cat. II, Roll-up to Cat I/C	20 fuel elements/ not man portable
Bldg. 3	U-235 fuel elements	Cat. II, Roll-up to Cat I/C	20 fuel elements/ not man portable

**Table E-17. Example of Credible Radiological Sabotage Targets**

Location	Material Type	Maximum Inventory	Material Size and Configuration
Bldg. 1, Fabrication Room	Pu-238 oxide powder	10kg	Paint cans/50g each
Bldg. 4	H <sub>3</sub> gas	10kg	Cylinders/500g each

**Table E-18. Example of Credible Biological Sabotage Targets**

Location	Material Type	Maximum Inventory	Material Size and Configuration
Bldg. 1, Fabrication Room	Anthrax solution	10g	20 petri dish/.5g each
Bldg. 4	Botulism aerosol	20g	10 2-liter cylinders/5kg each

**Table E-19. Example of Credible Chemical Sabotage Targets**

Location	Material Type	Maximum Inventory	Commercial Sector Security Difference	Material Size and Configuration	Exposure Level at NSM
Bldg. 5	Chlorine	10,000 lb.	Lack of access control	55-gallon drums/350 lbs. each	>ERPG III levels

**Table E-20. Example of Disruption of Critical Mission Targets Table**

Location	Target Function	Impact to National Security	Estimated Time for Recovery
Site A, Bldg. 4	Fuel cell production	Increased reliance on fossil fuels	180 days

- (f) VA/SRA Parameters and Planning Assumptions. Describe/list the baseline parameters and planning assumptions used in conducting the VAs and/or SRAs. Provide a summary list of parameters and planning assumptions used in completing VAs and/or SRAs. These shall include assumptions discussed and concurred in by appropriate DOE offices or planning assumptions identified as a result of data collection/discovery during the VA/SRA process.
- (g) Critical Path Protection Elements. Describe the process used to identify critical path protection elements and the types of tests to which site protection elements are subjected (procedural, simulation, barrier, equipment, PF, etc.). Using a table similar to Table E-21, Performance Testing Results of Site Specific Essential Protection Element Values, provide a list of: physical security system components for each protection layer (Limited Area (LA), PA, material access area (MAA), and Target Area), the critical protection element tested, if any, as determined from performance testing. Also, indicate the number of tests conducted to obtain results and the testing frequency used to monitor the protection element specific value.

- (h) Single Point Failure Analysis. Describe the analyses used to determine any single-point failures identified during the VA. Describe/list the single-point failure(s) to include the nature of the vulnerability, measures to mitigate the vulnerability and the potential exploitability by an adversary.
- (i) Critical Path Scenarios. Describe and provide the critical path scenarios, including the bounding scenarios, developed during the VA for each target. Identify the protection system effectiveness (Pe) value for each of these targets. Describe and identify the critical detection points along each adversary path.

Shall multiple targets exist within the same security area, such as several SNM targets within the same MAA and same building, bounding critical path scenarios may be described. Provide justification that supports bounding cases.

For each critical path scenario, provide floor plans, diagrams, sketches, or an adversary path description (as shown in Table E-22), or, if appropriate, refer to the descriptions that may have been used previously to illustrate the critical path and protection elements described in the scenarios.

Identify and describe the point along the adversary path at which detection is required to allow for sufficient response time for adversary neutralization to be effected for each of the critical path scenarios (i.e., critical detection point).



**Table E-21. Example of Performance Testing Results of Site-Specific**

Protection Layer and Physical Security System Components Tested	Critical Elements Tested	No. of Tests used as Basis for VA values	Test Frequency	Value used in VA
PA – Identification and Intrusion Element	Attempt to smuggle firearms through Portal 1.	36	Quarterly	0.6
	Attempt to defeat door contacts Bldg. 1, door 3.	34	Quarterly	0.7
MAA-Search Component	Attempt to smuggle firearms through MAA Portal	24	Once every 2 months	0.8
Target Area – Identification Component	Attempt to gain unauthorized vault access	48	Monthly	0.9

- (j) Protection System Effectiveness (P<sub>E</sub>). Verify that the P<sub>E</sub> values identified for each critical path scenario were used to calculate conditional risk for each identified target. Using tables similar to those on the following pages (Table E-23, Protection Effectiveness (P<sub>E</sub>) for the Theft of Diversion of SNM, Table E-24, Protection Effectiveness (P<sub>E</sub>) for Radiological Sabotage, Table E-25, Protection Effectiveness (P<sub>E</sub>) for Biological Sabotage; Table E-26, Protection Effectiveness (P<sub>E</sub>) for Chemical Sabotage; Table E-27, Protection Effectiveness (P<sub>E</sub>) for Disruption of Critical Missions; Table E-28, Protection Effectiveness (P<sub>E</sub>) for Theft or Espionage of Classified Information or Matter; and Table E-29, Protection Effectiveness (P<sub>E</sub>) for Other Losses), show the targets and P<sub>E</sub> values for each target.
- (k) Neutralization Analyses. Identify and describe the mechanism(s) used to determine/calculate the neutralization value(s) used in the risk evaluation. Identify and describe the basis for the neutralization values, parameters that impact the neutralization calculations and any site-specific issues that modify neutralization calculations.
- (l) Insider Analysis. Describe the analysis for determining the insider threat for each target class included in the SP. This analysis shall include the programs supporting the elimination/mitigation of select insider groups from the threat spectrum, identification of the potential insider population, and

insider protection programs that were not included in other protection system elements. Describe the programs that are factored into the VA process and provide justification for their use. Identify, by position and title, the participants in the HRP.

- (m) Conclusions. Provide a summary of system effectiveness for the identified targets. Document VA analyst's observations and recommendations developed as a result of the VA process. Summarize the system effectiveness using a table similar to E-30, System Effectiveness Summary.

**Table E-22. Example of Critical Path Scenarios**

Scenario Title:		Base Case 1		Results	
Facility:		Building XYZ		P <sub>I</sub>	.
Target Location:		Room.123 State, Open		P <sub>N</sub>	
Adversary Threat/Adversary:		Terrorist w/insider: X# outsider, Y# insiders			
Goal Type/Quantity:		Oxide, Xx kg		P <sub>E</sub>	
VA Path Analysis Tool:		ASSESS		C	
Computer File ID:		.PPS, .OUT; .NEU		Sys. Eff.:	
Neutralization Tool:		JTS		Sys. Eff.:	
Time (Sec)			SCENARIO ACTIONS		
Total	ADV	PF			
			Adversary pre-positions escape vehicles		
			Adversary mails weapons and explosives into PA (No x ray or explosives detection capability)		
			Adversary proceeds to access control portal		
0	20		Adversary attempt to deceit through portal (P <sub>D</sub> = 0.xx – badge check with xxxx at access portal). If detected, adversary begins overt actions CRITICAL DETECTION POINT		
		25	CAS receives alert and begins to annunciate alert.		
20	25		Adversary proceeds to target building XYZ, door 7 on the NE corner		
25			Protective Force units begin response.		
		70	Unit A responds to NE corner of building XYZ		
		55	Unit B responds to SE corner of building XYZ		
		80	Unit C responds to SE corner of building XYZ		
		60	Unit D responds to SE corner of building XYZ		
45	5		Adversary reaches door 7 to building XYZ, insider opens door 7 into building XYZ (P <sub>D</sub> = 0.xx – BMS)		
50	5		Adversaries enter building XYZ and transverse to vault room 123. CAS receives BMS door alarm and annunciates the alarm		
55	50		Adversaries collect target material		
80			Unit B reaches response position		
85			Unit D reaches response position		
95			Unit A reaches response position		
105	5		Adversaries proceed to door 7 to exit building XYZ. Unit C reaches response position.		
110			Adversary exits building XYZ via door 7. (P <sub>D</sub> = xxx - , )		
112			Unit A engages adversary		
			Etc.		

**Table E-23. Example of Protection Effectiveness (PE) for Theft or Diversion of SNM**

Location	Material Type	Facility Condition	Adversary Type	Adversary Scenario Summary	Protective Force Response Summary	PE Value
Bldg. 1 Vault	Pu-239 ingots	Open	Terrorist	Vault open. Outsider deceit into PA. Insider crashes out of Bldg. 1 MAA with material. Hands off to outsiders. Adversaries leave PA/site by vehicle.	Armed response to BMS door alarm. Containment at MAA boundary. Positioning of blocking forces at PA boundary if MAA containment defeated. Pursuit in PPA if escape from facility.	.7
Bldg. 1 Assay Room	Pu-239 ingots	Open	Terrorist	Scenario same as vault open scenario.	Scenario same as vault open scenario.	.7
Bldg. 1, Fabrication Room	Pu-238 oxide powder	Open	Terrorist	Scenario same as vault open scenario.	Scenario same as vault open scenario.	.7

**Table E-24. Example of Protection Effectiveness (PE) for Radiological Sabotage**

Location	Material Type	Facility Condition	Adversary Type	Adversary Scenario Summary	Protective Force Response Summary	PE Value
Bldg. 1, Fabrication Room	Pu-238 oxide powder	Open	Terrorist	Building open. Outsider's deceit into PA. Outsiders force MAA boundary by foot. Insider allows access into Building 1. Outsiders enter fabrication room, obtain Pu-238 oxide, defeat HEPA filters, and vent material to environment through building ventilation.	Armed response to MAA boundary alarm.	.4
Bldg. 4	H <sub>3</sub> gas	Open	Terrorist	Building open. Outsider's deceit into PA. Outsiders force MAA boundary by foot. Insider allows access into Building. 4. Outsiders disperse H <sub>3</sub> to the environment with explosives.	Armed response to MAA boundary alarm.	.4

**Table E-25. Example of Protection Effectiveness (PE) for Biological Sabotage**

Location	Material Type	Facility Condition	Adversary Type	Adversary Scenario Summary	Protective Force Response Summary	P <sub>E</sub> Value
Bldg. 5	Anthrax	Open	Terrorist	Building open. Outsiders deceit into PA. Insider allows access into Building 5. Outsiders disperse anthrax to the environment with explosives.	Building Containment	.2
		Close	Terrorist	Outsiders deceit into PA. Outsiders breach door into Building 5. Outsiders disperse anthrax to the environment with explosives.	Building Containment	.2

**Table E-26. Example of Protection Effectiveness (PE) for Chemical Sabotage**

Location	Material Type	Facility Condition	Adversary Type	Adversary Scenario Summary	Protective Force Response Summary	P <sub>E</sub> Value
Bldg. 5	Chlorine	Open	Terrorist	Building open. Outsiders deceit into PA. Insider allows access into Building 5. Outsiders disperse chlorine to the environment with explosives.	Building Containment	.2
		Close	Terrorist	Outsiders deceit into PA. Outsiders breach door into Building 5. Outsiders disperse chlorine to the environment with explosives.	Building Containment	.2

**Table E-27. Example of Protection Effectiveness (PE) for Disruption of Critical Missions**

Location	Equipment Type	Facility Condition	Adversary Type	Adversary Scenario Summary	Protective Force Response Summary	P <sub>E</sub> Value
Bldg. 1, Fabrication Room	Fuel Fabrication	Open	Nonviolent Insider	Insider enters fabrication room. Starts fire to destroy equipment located in room.	Building Containment	.2

**Table E-28. Example of Protection Effectiveness ( $P_E$ ) for Theft/Espionage of Classified Information/Matter**

Location	Classified Information or Matter	Facility Condition	Adversary Type	Worst-case Scenario Summary	Protective Force Response Summary	$P_E$ Value
Bldg. 5, Office Area	TSRD Documents	Open	Nonviolent Insider	Insider obtains TSRD, makes copies, encloses copies in envelope, and hand-carries out of Bldg. 5. Insider mails classified documents out of PA to off-site location.	None	.2

**Table E-29. Example of Protection Effectiveness ( $P_E$ ) for Other Losses**

Location	Item	Facility Condition	Adversary Type	Worst-case Scenario Summary	Protective Force Response Summary	$P_E$ Value
Bldg. 5 Lab Area	R&D Laboratory	Open	Nonviolent Insider	Insider starts fire in laboratory.	Building Containment	.2

**Table E-30. Example of System Effectiveness Summary**

Goal	Target	Location	Operations	$P_E$
Theft of SNM	Bldg. 1	Vault	Day Shift	.8
Theft of SNM	Bldg. 1	Assay Room	Day Shift	.8
Theft of SNM	Bldg. 1	Fab. Room	Day Shift	.75
Rad. Sabotage	Bldg. 1	Fab. Room	Day Shift	.85
Rad. Sabotage	Bldg. 4	Bldg. 4	Day Shift	.9
Chem. Sabotage	Bldg. 5	Laboratory	Day Shift	.8
Bio. Sabotage	Bldg. 5	Laboratory	Day Shift	.8
Indust. Sabotage	Bldg. 1	Fab. Room	Day Shift	.8
Espionage of Classified	Bldg. 5	Office Area	Day Shift	.8
Other Losses	Bldg. 5	Laboratory	Day Shift	.8

## Appendix F —SAFEGUARDS & SECURITY MANAGEMENT PLAN TEMPLATE

The Safeguards and Security (S&S) Management Plan provides a description of the implementation of S&S policy and provides detailed information on the assignment of roles, responsibilities, and authorities, as well as the development of budgets and allocation of resources. The following outline delineates the content requirements and provides a suggested format.

### 1. EXECUTIVE SUMMARY.

- a. Program Mission Statement. Briefly describe the program mission and how the mission relates to national security. Describe the major elements or activities performed in terms of program mission and its relationship to the DOE national security mission.
- b. S&S Program Structure. Briefly describe the strategy and organizational elements used to implement the S&S program under their cognizance.
- c. Management and Planning Assumptions. Briefly describe those assumptions that affect the management and planning of the implementation of the S&S program. These assumptions shall include items such as:
  - (1) future of the program (mission, staffing levels, site status, etc.);
  - (2) current and planned S&S projects; and
  - (2) status of the organization's S&S budget.

### 2. PART 1 – ORGANIZATIONAL STRUCTURE AND ACCOUNTABILITY

- a. Line Management Organization. Describe the structure and relationship of line management. Identify the roles, responsibilities, and authorities of these line management elements to include organizational charts.
- b. Cognizant Security Authority Organization. Describe the structure of line management that is specifically responsible for implementing the Departmental element's S&S program. Identify the individuals and positions responsible for committing resources and directing the activities of personnel associated with the S&S program.
  - (1) Headquarters Organizational Structure. For the Headquarters elements, provide an organizational chart to show the S&S organization and management structure and the lines of authority and points of interface with other programs which affect S&S (e.g., safety, facility operations,

and the cognizant security authority's material control and accountability (MC&A) organization, if independent of the security organization). Describe the functions and responsibilities of S&S personnel and indicate how S&S activities are integrated with those of other facility organizations; include organizational responsibilities for line management overseeing the program as well as the interface points with the respective Departmental element.

- (2) Field Organizational Structure. For the Field elements, provide an organizational chart to show the S&S organization and management structure and the lines of authority and points of interface with other programs which affect S&S (e.g., safety, facility operations, and the cognizant security authorities' MC&A organization, if independent of the security organization). Describe the functions and responsibilities of S&S personnel and indicate how S&S activities are integrated with those of other facility organizations; include organizational responsibilities for line management overseeing the program as well as the interface points with the respective Departmental element.

- c. Contractor Sites. Provide the contract name, number, and other information that describes the authority under which the contractor executes management functions for facilities under the cognizance of a Departmental element. Identify the site contractor elements responsible for S&S programs and describe their S&S activities. Provide Federal and contractor organization charts and identify key positions and the relationships between the organizations responsible for S&S activities. Describe Federal and contractor involvement in the development of S&S resource requirements.

3. PART 2 – ROLES, RESPONSIBILITIES, DELEGATIONS, AND AUTHORITIES. Delegations must be documented in writing and delineate all assigned S&S roles, responsibilities, and authorities for the S&S program. This section:

- a. documents offices/positions affected by the S&S Management Plan;
- b. establishes the approval chain for S&S plans, procedures and implementation policy;
- c. establishes the approval chain for S&S policy deviations;
- d. assigns reporting requirements for incidents of security concern; and
- e. provides a list of roles and responsibilities for key positions and the delegated authorities for each.

- 
4. PART 3—S&S PROGRAM IMPLEMENTATION. This section of the S&S Management Plan documents the processes and methods used to implement the Department's security policies. This section identifies:
- a. the methods used for ensuring all applicable programmatic requirements are implemented throughout the organizational element;
  - b. the methods used for ensuring effective integration of S&S programmatic elements; and
  - c. Security Plans used to implement S&S policy requirements.
5. PART 4—PLANNING AND BUDGET (INCLUDING PERSONNEL RESOURCES). This section of the S&S Management Plan documents the key processes of planning and budgeting, including strategic planning, budget formulation, budget execution, and program evaluation.
- a. Describe the strategic planning assumptions used to ensure the S&S program will meet mission objectives.
  - b. Provide a 5-year plan that describes the budget formulation priorities for future S&S resources and programs.
  - c. Provide the current year plan for executing the S&S budget. This plan details the allocation of resources that support S&S functions and missions.
  - d. Provide a program evaluation plan that details how the cognizant security authority will assess the implementation of the S&S program and the organization's progress toward meeting established missions/goals. The program evaluation plan must cover both the Federal and contractor elements of the Departmental element. This plan can be used to support award fee decisions by the Departmental element.
  - e. Briefly describe any changes to operational requirements which affect S&S program operations or would require increments or decrements to operational accounts (e.g., program direction, operational support, etc.).



## Appendix G —RESOURCE PLAN TEMPLATE

1. **OBJECTIVE.** The Resource Plan (RP) identifies safeguards and security (S&S) resources necessary to ensure protection of Department assets and identifies changes in resource requirements (i.e., operational requirements, capital equipment, general plant projects (GPPs) and line item construction projects (LICPs) that directly impact risk, indirectly impact risk, or derive from changing S&S policy, directives, guidance, or other Department or other Departmental direction.
  - a. **Operational Requirements.** Briefly describe operational requirements relating to S&S operations that would require increments or decrements to operational accounts (e.g., program direction, operational support, etc.). Operational requirements shall include, but are not limited to, material consolidation, facility mission changes, changes in the Design Basis Threat (DBT) impacting site operations, protective force (PF) redeployments, maintenance and testing changes, PF manning levels, procuring technical expertise and support personnel, and additional training requirements. Summarize the pertinent information in a table such as outlined in Table G-1, Operational Requirements. The table and supporting narrative shall include the following:
    - (1) the title of each operational requirement;
    - (2) the basis of the requirement (drivers behind the requirement);
    - (3) the funding profile and the impacts if not funded (if possible, state the impact in terms of probability of system effectiveness (P<sub>E</sub>) and indicate if this is a new resource requirement); and
    - (4) provide a status of operational requirements that were previously authorized but have not yet been completed.

Provide a separate section for each operational requirement.

**Table G-1. Example of the Operational Requirements for the Resource Plan**

Requirement (section)	Basis	Funding Request/Profile						Currently in Budget (Y or N)	Type of Expense
		FY xxxx (current year)	FY + 1	FY + 2	FY + 3	FY + 4	FY + 5		

- b. Capital Equipment. Briefly describe identified/proposed capital equipment procurements and funding requirements that are not part of a LICP or GPP, and support S&S programs and operations. These procurements could include, but are not limited to, alarm and assessment system components, material control and accountability (MC&A) systems, access control system components, and equipment necessary to complete the S&S mission (e.g., breaching tools, vehicles, PF armaments, additional capabilities necessary to address changes in the DBT). Summarize the pertinent information in a table as outlined in Table G-2, Capital Equipment. The table and supporting narrative shall include the following:

- (1) a title for each capital equipment procurement;
- (2) the basis of the requirement (drivers behind the requirement);
- (3) the funding profile and the impacts if not funded (if possible, state the impact in terms PE, and indicate if this is a new resource requirement); and,
- (4) a status of capital equipment upgrades that were previously authorized but have not yet been completed.

Provide a separate section for each capital equipment procurement.

**Table G-2. Example of the Capital Equipment for the Resource Plan**

Capital Equipment (section)	Basis	Funding Request/Profiles						Currently in Budget (Y or N)
		FY xxxx (current year)	FY + 1	FY + 2	FY + 3	FY + 4	FY + 5	

- c. GPP. Describe significant identified/proposed GPPs that are not part of an LICP or capital equipment expense but that are necessary to support S&S programs and operations. These GPPs could include, but are not limited to, alarm and assessment systems/components, MC&A systems, access control systems/components, or infrastructure improvements. Summarize the pertinent information in a table as outlined in Table G-3, General Plan Projects. The table and supporting narrative must include:

- (1) a title for each GPP;
- (2) the basis of the requirement (drivers behind the requirement);
- (3) the funding profile and the impacts if not funded (if possible, state the impact in terms PE, and indicate if this is a new resource requirement);
- (4) a status of general plan project upgrades that were previously authorized but have not yet been completed.

Provide a separate section for each GPP.

**Table G-3. Example of the General Plant Projects for the Resource Plan**

General Plant Projects (section)	Basis	Funding Request/Profiles						Currently in Budget (Y or N)
		FY xxxx (current year)	FY + 1	FY + 2	FY + 3	FY + 4	FY + 5	

- d. LICPs. Describe current and proposed LICPs that are not part of a GPP or capital equipment procurement but are necessary to support S&S programs and operations. Summarize the pertinent information in a table as outlined in Table G-4, Line Item Construction Projects. The table and supporting narrative must include:
- (1) a title for each LICP;
  - (2) the basis of the requirement (drivers behind the requirement);
  - (3) the funding profile and the impacts if not funded (if possible, state the impact in terms PE, and indicate if this is a new resource requirement); and
  - (4) the status of S&S upgrades that were authorized but have not yet been completed. Discuss any changes to cost estimates [i.e., total estimated cost (TEC) versus total project cost (TPC)] identified in the previous RP.

Provide a separate section for each LICP.

**Table G-4. Example of the Line Item Construction Projects for the Resource Plan**

LICP Title (section)	Basis	Funding Request/Profiles						Total Costs		Schedule		Currently in Budget (Y or N)
		FY xxxx (current year)	FY + 1	FY + 2	FY + 3	FY + 4	FY + 5	TEC	TPC	Start Date	Finish Date	

**Table G-5. Example of the Unfunded/Unsupported Requirements for the Resource Plan**

Requirement (section)	Basis	Resource Type	Base FY	Original Funding Request/Profiles						Impact
				FY xxxx	FY + 1	FY + 2	FY + 3	FY + 4	FY + 5	

2. UNFUNDED/UNSUPPORTED REQUIREMENTS. Briefly describe proposed S&S operational requirements, capital equipment procurements, GPPs, or LICPs that had been previously identified and have not been funded supported. Summarize the pertinent information in a table such as Table G-5, Unfunded/Unsupported Requirements. The table and supporting narrative shall include:

- a. a title for each unfunded requirement;
- b. the basis for the requirement (drivers behind the requirement);
- c. the type of resource requested (operating expense, capital equipment, GPP, or LICP);
- d. the fiscal year the requirement was originally identified;
- e. the proposed funding profile and impacts due to lack of funding (if possible, state the impact in terms of PE).

Provide a separate section for each unfunded requirement.

3. REFERENCES FOR THE RESOUCCE PLAN.

- a. Facility Security Plan. Provide a reference to the most recent/current Site Security Plan.
- b. Programmatic Documentation. Provide a reference (include title, date, and responsible organization) for any programmatic policy, directive, or guidance necessitating the allocation of additional resources.

4. HEADINGS AND TERMS FOR TABLES G-1 THROUGH G-5. Following are the types of data to be included in the RP.

- a. Basis.
  - (1) Compliance.
  - (2) Risk reduction.
  - (3) SP derived.
  - (4) Cost-efficiency.
  - (5) Operational efficiency.
  - (6) Enhanced operations.
  - (7) DBT change.

- b. Type of Expense.
  - (1) Operational = annual recurring cost that will need to be added to the budget baseline.
  - (2) Single = one time only expense paid from operating dollars.
- c. Total Costs.<sup>1</sup>
  - (1) TEC = Total estimated cost.
  - (2) TPC = Total project cost.
- d. Resource Type.
  - (1) OE = operational expense.
  - (2) CE = capital expense.
  - (3) GPP = general plant project.
  - (4) LICP = line item construction project.
  - (5) BASE FY = fiscal year in which the resources were identified and requested.
- e. Impact.
  - (1) Continued risk.
  - (2) Cost escalation.
  - (3) Unable to comply with xxxx (list applicable directive).
  - (4) Programmatic impact.
  - (5) Operational impact.
  - (6) Other (list).

**Appendix H --PERFORMANCE ASSURANCE PROGRAM TEMPLATE**

1. **OBJECTIVE.** To demonstrate the effectiveness of the protection provided Departmental safeguards and security (S&S) interests by systematically evaluating all protection program essential elements.
2. **REQUIREMENTS.** Each performance assurance program must be developed to validate the performance of all essential S&S protection elements.
  - a. **Operability and Effectiveness.** Performance assurance programs must provide for operability and effectiveness testing of each protection program essential element or component.
    - (1) Operability tests provide measures of integrity and must check the essential elements or total system to confirm operability.
    - (2) Performance tests provide comprehensive assurance that protection program elements are performing as designed and provide the required levels of protection.
      - (a) Performance tests results are used to validate the effectiveness of all elements of a layered S&S system.
      - (b) Performance tests are not substitutes for compliance with requirements.
  - b. **Continuity.** Performance assurance programs must evaluate operational continuity of all S&S essential elements. Limited Scope Performance Tests (LSPTs) and/or force-on-force (FoF) tests may be used as a means of meeting specific performance assurance testing requirements. Performance assurance programs must be evaluated as part of the DOE survey and the facility self-assessment programs.
    - (1) New protection program essential elements and components must be validated through acceptance testing before operational use.
    - (2) Essential elements that have been repaired or undergone maintenance must be validated through testing before use.
    - (3) The protective force (PF) must be performance tested both individually and in small tactical units.

- (4) Performance tests must ensure that approved protection strategies of denial, containment, recapture, recovery, and pursuit can be accomplished by the PF.
  - (5) Essential elements of the protection program security systems and subsystems are performance tested to ensure that system detection, assessment, and response to alarms and adversarial actions meet stated requirements.
- c. Reliability. Each essential element whose failure would reduce protection to an unacceptable level must be tested at frequencies that provide high assurance of operability and reliability.
  - (1) Testing frequencies must reflect site-specific conditions and operational needs.
  - (2) Testing frequencies must be documented for each essential element.
- d. Performance Tests. At least every 365 days, an integrated performance test encompassing all essential protection elements associated with a comprehensive site or facility threat scenario must be conducted to evaluate the overall facility S&S effectiveness.
  - (1) Those Category I facilities requiring denial protection strategies must conduct integrated performance testing on a quarterly basis (at least every 3 months).

OR

- (2) Those sites with multiple Category I facilities requiring denial protection strategies may rotate quarterly performance testing so that at least one facility is tested on a quarterly basis (at least every 3 months). However, an integrated performance test for all Category I facilities shall occur at least once every 365 days.
- e. Documentation.
  - (1) Performance Assurance Program Plan. This plan shall be an integral part of the security plan (SP), or material control and accountability (MC&A) plan, as applicable. The performance assurance program plan shall describe the program and its administration and implementation by:
    - (a) identifying protection elements for the protection of Category I and II special nuclear material (SNM) and Top Secret matter;



- (b) describing how the performance of these elements is to be ensured, including the manner in which credit is taken for activities performed by external oversight organizations;
  - (c) addressing how deficiencies identified during performance assurance activities are to be corrected.
- (2) Performance Assurance Reports. The results of performance assurance program testing must be documented.
- (3) Document Retention. Record keeping systems shall provide an audit trail for performance assurance activities and reports.

---

i DOE O 470.4B, Paragraph 7.b. and 7.c.

ii DOE O 470.4B, Appendix A, Section 1 Paragraph 5.b. and Attachment 2, Section 1, Paragraph 5.b.

iii DOE O 470.4B, Appendix A, Section 1, Chapter I, Paragraph 1. and Attachment 2, Section 1, Chapter I, Paragraph 1.

iv DOE O 470.4B, Appendix A, Section 1 Paragraph 5.c. and Attachment 2, Section 1, Paragraph 5.b.

v DOE O 470.4B, Appendix A, Section 1, Chapter I, Paragraph 4.a. and Attachment 2, Section 1, Chapter 1, Paragraph 4.a.

vi DOE O 470.4B, Appendix A, Section 1, Chapter I, Paragraph 4.a. and Attachment 2, Section 1, Chapter 1, Paragraph 4.a.

vii DOE Appendix A, Section 1, Chapter I, Paragraph 3. and Attachment 2, Section 1, Chapter I, Paragraph 3.

viii DOE O 470.4B, Appendix A, Section 1, Chapter I, Paragraphs 1.c.-e. and Attachment 2, Section 1, Chapter I, Paragraph 1.c.-e.

ix DOE O 470.4B, Appendix A, Section 1, Chapter I, Paragraphs 1.f. and Attachment 2, Section 1, Chapter I, Paragraph 1.f.

x DOE O 470.4B, Appendix A, Section 1, Paragraph 5.d. and Attachment 2, Section 1, Paragraph 5.c.

xi DOE O 470.4B, Appendix A, Section 1, Chapter I, Paragraph 4.a. and Attachment 2, Section 1, Chapter I, Paragraph 4.a.)

xii DOE O 470.4B, Appendix B, Section 1, Paragraph 5 and Attachment 3, Section 1, Paragraph 5.

xiii DOE O 470.4B, Appendix B, Section 2, Paragraph 5. and Attachment 3, Section 2, Paragraph 5.

xiv DOE O 470.4B, Appendix B, Section 4, Paragraph 5 and Attachment 3, Section 4, Paragraph 5

xv DOE O 142.3, Paragraph 4.c.

xvi DOE O 470.4B, Appendix B, Section 4, Paragraph 5 and Attachment 3, Section 4, Paragraph 5

xvii DOE O 470.4B, Appendix B, Section 4, Paragraph 5 and Attachment 3, Section 4, Paragraph 5

xviii DOE O 470.4B, Paragraph 3.c.(2)

xix DOE O 473.3A, Appendix A, Annex 3, Paragraph 1.e. and Attachment 2, Annex 2, Paragraph 1.f.

xx DOE O 470.4B, Appendix A, Section 1, Chapter II, Paragraph 4 and Attachment 2, Section 1, Chapter II, Paragraph 4

xxi DOE 470.4B, Appendix A, Section 1, Chapter III, Paragraph 1

xxii DOE O 470.4B, Appendix B, Section 5, Paragraph 5 and Attachment 3, Section 5, Paragraph 5

xxiii DOE O 470.4B, Appendix B, Section 4, Paragraph 5 and Attachment 3, Section 4, Paragraph 5

xxiv DOE O 470.4B, Appendix B, Section 6, Paragraph 4 (listed as 9) and Attachment 3, Section 6, Paragraph 4

xxv DOE O 473.3A, Appendix A, Annex 5 and Attachment 2, Annex 5

xxvi DOE O 473.3A, Appendix A, Annex 5 and Attachment 2, Annex 5

xxvii DOE O 473.3A, Attachment 3, Section A, Chapter II, Paragraphs 2., 3., 4.

xxviii DOE O 473.3A, Attachment 3, Section A, Chapter XI, Paragraph 1.

xxix DOE O 473.3A, Attachment 3, Section A, Paragraph 8.

xxx DOE O 473.3A, Attachment 3, Section A, Chapter X, Paragraph 1.

xxxi DOE O 470.4B, Appendix A, Section 1, Chapter I, Paragraph 1 and

xxxii DOE O 473.3A, Attachment 3, Section A, Chapter IV, Paragraph 2.a.

xxxiii DOE O 473.3A, Attachment 3, Section A, Chapter IV, Paragraph 3.a

xxxiv DOE O 473.3A, Attachment 3, Section A, Chapter II, Paragraphs 2., 3., 4.

xxxv DOE O 473.3A, Attachment 3, Section A, Chapter II, Paragraph 4.c.(3)(a)

xxxvi DOE O 473.3A, Attachment 3, Section A, Chapter II, Paragraph 4.c.(3)(e)

xxxvii DOE O 473.3A, Attachment 3, Section A, Chapter II, Paragraph 4.c.(1)

xxxviii DOE O 473.3A, Attachment 3, Section A, Chapter II, Paragraph 4.c.(2)(a)

---

xxxix DOE O 473.3A, Attachment 3, Section A, Chapter II, Paragraph 4.d.(2)

xl DOE O 473.3A, Attachment 3, Section A, Chapter II, Paragraph 4.d.(3)

xli DOE O 473.3A, Attachment 3, Section A, Chapter II, Paragraphs 2., 3., 4. and DOE O 473.3A, Attachment 3, Section A, Chapter III, Paragraph 1

xlII DOE O 473.3A, Attachment 3, Section A, Chapter III, Paragraph 4.b.

xlIII DOE O 473.3A, Attachment 3, Section A, Chapter II, Paragraphs 2., 3., 4.

xliv DOE O 473.3A, Attachment 3, Section A, Chapter VI, Paragraph 3

xlV DOE O 473.3A, Attachment 3, Section A, Chapter VI, Paragraph 5

xlvi DOE O 473.3A, Attachment 3, Section A, Chapter VI, Paragraph 8

xlVII DOE O 473.3A, Attachment 3, Section A, Chapter VIII, Paragraph 1.b.(2)

xlVIII DOE O 473.3A, Attachment 3, Section A, Chapter II, Paragraph 4.c.(3)(a)

xlIX DOE O 473.3A, Attachment 3, Section A, Chapter II, Paragraph 4.c.(3)(e)

l DOE O 473.3A, Attachment 3, Section A, Chapter II, Paragraph 4.c.(1)

li DOE O 473.3A, Attachment 3, Section A, Chapter VIII, Paragraph 1.b.(3)

lii DOE O 473.3A, Attachment 3, Section A, Chapter II, Paragraphs 2., 3., 4. and DOE O 473.3A, Attachment 3, Section A, Chapter III, Paragraph 1

liii DOE O 473.3A, Attachment 3, Section A, Chapter III, Paragraph 4.b.

liv DOE O 473.3A, Attachment 3, Section A, Chapter II, Paragraphs 2., 3., 4.

lv DOE O 473.3A, Attachment 3, Section A, Chapter II, Paragraph 5.c.

lvi DOE O 473.3A, Attachment 3, Section A, Chapter II, Paragraph 5.a.

lvII DOE O 473.3A, Attachment 3, Section A, Chapter VIII, Paragraph 1.b.(2)

lvIII DOE O 473.3A, Attachment 3, Section A, Chapter II, Paragraph 4.c.(3)(a)

lix DOE O 473.3A, Attachment 3, Section A, Chapter II, Paragraph 4.c.(3)(e)

lx DOE O 473.3A, Attachment 3, Section C, Chapter I, Paragraph 4.c.

lxi DOE O 473.3A, Attachment 3, Section C, Chapter I, Paragraph 4.c.(1)(c)

lxii DOE O 473.3A, Attachment 3, Section C, Chapter I, Paragraph 4.c.(1)(b)1

lxiii DOE O 473.3A, Attachment 3, Section C, Chapter I, Paragraph 4.c.(1)(b)3

lxiv DOE O 473.3A, Attachment 3, Section A, Chapter II, Paragraph 4.c.(3)(a)

lxv DOE O 473.3A, Attachment 3, Section A, Chapter II, Paragraph 4.c.(3)(e)

lxvi DOE O 470.4B, Appendix A, Section 1, Chapter I, Paragraph 1. and Attachment 2, Section 1, Chapter I, Paragraph 1.

lxvII DOE O 473.3A, Attachment 3, Section A, Chapter IV, Paragraph 5.b.

lxvIII DOE O 473.3A, Attachment 3, Section A, Chapter IV, Paragraph 4.d.

lxix DOE O 473.3A, Attachment 3, Section A, Chapter IV, Paragraph 5.c and Paragraph 6.b.

lxx DOE O 473.3A, Attachment 3, Section A, Chapter IV, Paragraph 5.c and Paragraph 6.b.

lxxI DOE O 473.3A, Attachment 3, Section A, Chapter IV, Paragraph 1.b.

lxxii DOE O 473.3A, Attachment 3, Section A, Chapter IV, Paragraph 4.a.

lxxiii DOE O 473.3A, Attachment 3, Section A, Chapter II, Paragraphs 2., 3., 4.

lxxiv DOE O 470.4B, Appendix A, Section 1, Chapter I, Paragraph 1 and

lxxv DOE O 474.2, Attachment 3, Paragraph 1.u.

lxxvi DOE O 474.2, Attachment 3, Paragraph 2.d.

lxxvII DOE O 474.2, Attachment 3, Paragraph 2.e.

lxxvIII DOE O 470.4B, Appendix A, Section 1, Chapter I, Paragraph 2

lxxix DOE O 470.4B, Appendix A, Section 1, Chapter I, Paragraph 1. and Attachment 2, Section 1, Chapter I, Paragraph 1.

lxxx DOE O 473.3A, Attachment 3, Section A, Chapter II, Paragraphs 2., 3., 4.

lxxxi DOE O 471.6, Paragraph 4.a.(3)

lxxxii DOE O 471.6, Paragraph 4.b.(2)(g)

lxxxiii DOE O 471.6, Paragraph 4.b.(5)(i)

lxxxiv DOE O 471.6, Paragraph 4.b.(7)(a)5

lxxxv DOE O 471.6, Paragraph 4.b.(5)(j)

lxxxvi DOE O 470.4B, Appendix A, Section 1, Chapter I, Paragraph 1. and Attachment 2, Section 1, Chapter I, Paragraph 1.

lxxxvII DOE O 470.4B, Appendix A, Section 1, Chapter I, Paragraph 1. and Attachment 2, Section 1, Chapter I, Paragraph 1.

lxxxvIII DOE O 470.4B, Appendix B, Section 4, Paragraph 5 and Attachment 3, Section 4, Paragraph 5

lxxxix DOE O 470.4B, Appendix B, Section 4, Paragraph 5 and Attachment 3, Section 4, Paragraph 5

xc DOE O 470.4B, Appendix A, Section 2, Paragraph 5 and Attachment 2, Section 2, Paragraph 5