EFCOG

2014

SAFEGUARDS AND SECURITY SELF-ASSESSMENT TOOLKIT

Energy Facility Contractors Group

Dedicated to Promoting Excellence
in DOE Operations

SUMMARY

This Toolkit was created by the Energy Facilities Contractors Group (EFCOG) to augment the Office of Health, Safety and Security, Safeguards and Security Survey and Self-Assessment Technical Standard. This Toolkit provides a variety of samples and tools that may be used to complement the overall assessment process. It is not meant to be all-inclusive, but rather provide a basis that can be expanded and built upon.

The Toolkit is divided into four sections: Planning Documentation, Conduct Tools, Topical Area Tools and Post-Assessment Tools. The Planning section provides tools associated with assessment notification, planning, and in-briefings. The Conduct section is broken down into seven topical areas and their respective subtopical areas. This breakdown is similar to that outlined in the U.S. Department of Energy (DOE) F 470.8, *Survey/Inspection Report Form*. While use of this form is not required, it does provide a good outline and is commonly used across the complex. Each topical area contains items such as common deficiencies, sample documents for review, sample lines of inquiry, potential interview candidates, and performance tests. The Post-Assessment section includes sample report formats, report writing guides, exit briefing slides, transmittal memos, sample corrective action plans, and the DOE F 470.8, *Survey/Inspection Report Form*.

This Toolkit is a living document maintained by the EFCOG. In order to make it as user friendly as possible, the table of contents has been hyperlinked and reference documents linked where possible. Should you have tools that have proven effective at your site or facility, please forward them to the EFCOG Safeguards and Security Chair for inclusion. Thank you to those who contributed and to the DOE Office of Health, Safety and Security, Office of Enforcement and Oversight who's Inspectors Guides were heavily relied upon in the development of this document.

USEFUL LINKS

Additional information specific to each topical area may be found on line at the following links:

EFCOG Causal Analysis Guide for Information Security Noncompliances:
http://www.efcog.org/guides/EFCOG%20Cause%20Analysis%20Guide.pdf

HSS Office of Independent Oversight:
http://energy.gov/hss/services/oversight

HSS Technical Standards Program:
http://energy.gov/hss/information-center/department-energy-technical-standards-program

HSS Policy Information Resource:
https://pir.labworks.org/

DOE Directives, Delegations, and Requirements:
https://www.directives.doe.gov/directives/

DOE Forms:
http://energy.gov/cio/office-chief-information-officer/services/forms

ACRONYMS

The following list of acronyms includes those that may or *may not* specifically appear in this toolkit; however, it may be beneficial to become familiar with the terms, as they will be used during the conduct of assessments. For a complete list of acronyms, abbreviations, and glossary of terms related to DOE's Safeguards and Security Program, please refer to https://pir.labworks.org/.

A

ADC	Authorized Derivative Classifier
ANFO	Ammonium Nitrate-Fuel Oil
ANSI	American National Standard Institute
ARAPT	Alarm Response and Assessment Performance Test
ASSE	American Society of Safety Engineers
ASSESS	Analytic System and Software for Evaluating Safeguards and Security
ASTM	American Society for Testing and Materials
ATLAS	Adversary Timeline Analysis System

B

BIT	*Basic Instructor Training*
BMS	Balanced Magnetic Switch
BQC	*Basic Qualification Course*

C

C&A	*Certification and Accreditation*
CAP	Corrective Action Plan
CAS	Central Alarm Station
CAT	Composite Adversary Team
CCI	*Controlled Cryptographic Item*
CCTV	Closed-Circuit Television
CDCO	Classified Document Control Office
CFR	Code of Federal Regulations
CFRD	*Classified Formerly Restricted Data*
CGS	*Classification Guidance System*
CI	Counterintelligence
CMPC	Classified Matter Protection and Control
CNSI	*Confidential/National Security Information*
CNSS	Committee on National Security Systems
CO	Classification Officer
COMSEC	*Communications Security*
CPCI	Central Personnel Clearance Index
CPI	*Critical Program Information*
CRD	*Classified Restricted Data*
CREM	Classified Removable Electronic Media
CSA	Cognizant Security Authority
CSO	Cognizant Security Official
CSCS	Contract Security Classification Specification
CSE	Critical System Element

D

DAA	*Designated Approving Authority*
DBT	Design Basis Threat
DC	Derivative Classifier

DD	Derivative Declassifier
DEAR	Department of Energy Acquisition Regulation
DOD	U.S. Department of Defense
DOE	U.S. Department of Energy
E	
EIA	Electronic Industries Alliance
EO	Executive Order
EOC	Emergency Operations Center
ESM	*Electronic Storage Media*
ESS	Engagement Simulation System
F	
FACTS	Foreign Access Central Tracking System
FAR	False Alarm Rate
FCL	Facility Clearance
FDAR	Facility Data and Approval Record
FN	Foreign Nationals
FNVA	Foreign National Visit and Assignment
FOCI	Foreign Ownership, Control, or Influence
FOF	Force on Force
FRD	Formerly Restricted Data
FSO	Facility Security Officer
G	
GAO	Government Accountability Office
GSA	U.S. General Services Administration
GSP	Graded Security Protection
H	
HQ	Headquarters
HRP	Human Reliability Program
HSPD	Homeland Security Presidential Directive
I	
IAEA	International Atomic Energy Agency
ICD	Intelligence Community Directive
IG	Inspector General
IDAS	Intrusion Detection and Assessment System
IDS	Intrusion Detection System
IOSC	Incidents of Security Concern
IRAP	Internal Review and Assessment Plan
ISC	Interagency Security Committee
ISOO	Information Security Oversight Office
J	
JA	Job Analyses
JCATS	Joint Conflict and Tactical Simulation
JTA	Job Task Analyses
K	
KMP	Key Management Personnel

L	
LA	Limited Area
LEID	Limit of Error of the Inventory Difference
LSPT	Limited Scope Performance Test
M	
MAA	Material Access Area
MBA	Material Balance Area
MC&A	Material Control and Accountability
METL	Mission Essential Task List
MILES	Multiple Integrated Laser Engagement System
MOA	Memorandum of Agreement
MOU	Memorandum of Understanding
N	
NAR	Nuisance Alarm Rate
NATO	North Atlantic Treaty Organization
NFPA	National Fire Protection Association
NIJ	National Institute of Justice
NISPOM	National Industrial Security Program Operating Manual
NMMSS	Nuclear Material Management and Safeguards System
NNSA	National Nuclear Security Administration
NSA	*National Security Agency*
NSD	National Security Directive
NSI	*National Security Information*
NTC	National Training Center
NVG	Night Vision Goggles
O	
ODFSA	*Officially Designated Federal Security Authority*
ODSA	*Officially Designated Security Authority*
OFI	Opportunity for Improvement
OPSEC	Operations Security
OUO	Official Use Only
P	
PA	Protected Area
PAP	Performance Assurance Program
PDD	Presidential Decision Directive
PF	Protective Force
PIDAS	Perimeter Intrusion Detection and Assessment System
PIV	*Personal Identity Verification*
PL	Public Law
POC	Point-of-contact
PPA	*Property Protection Area*
PSS	Physical Security System
PTZ	Pan-Tilt-Zoom
R	
RD	Restricted Data
RFI	Representatives of Foreign Interests
RIS	Reporting Identification Symbol
RO	Reviewing Official

S

S&S	Safeguards and Security
SAP	Special Access Program
SAS	Secondary Alarm Station
SCI	Sensitive Compartmented Information
SCIF	Sensitive Compartmented Information Facility
SEC	Securities and Exchange Commission
SECON	Security Condition
SERP	Security Emergency Response Plan
SF	Standard Form
SFRD	*Secret Formerly Restricted Data*
SIRP	Security Incident Response Plan
SNM	Special Nuclear Materials
SNSI	*Secret National Security Information*
SO	Security Officer
SOP	Standard Operating Procedure
SPO	Security Police Officer
SRD	Secret Restricted Data
SRT	Special Response Team
SSIMS	Safeguards and Security Information Management System
SSP	Site Security Plan
STE	*Secure Telephone Equipment*
STU	*Secure Telephone Unit*

T

TIA	Telecommunications Industry Association
TID	Tamper Indicating Device
TNT	Trinitrotoluene
TSCM	Technical Surveillance Countermeasures
TSCMO	Technical Surveillance Countermeasure Officer
TSCMOM	Technical Surveillance Countermeasure Operations Manager
TSFRD	*Top Secret Formerly Restricted Data*
TSNSI	*Top Secret National Security Information*
TSRD	*Top Secret Restricted Data*
TRF	Tactical Response Force

U

UCNI	Unclassified Controlled Nuclear Information
UL	Underwriters Laboratory
UPS	Uninterruptable Power Supply
USC	United States Code

V

VA	Vulnerability Assessment

W

WFO	Work for Others
WMD	Weapons of Mass Destruction

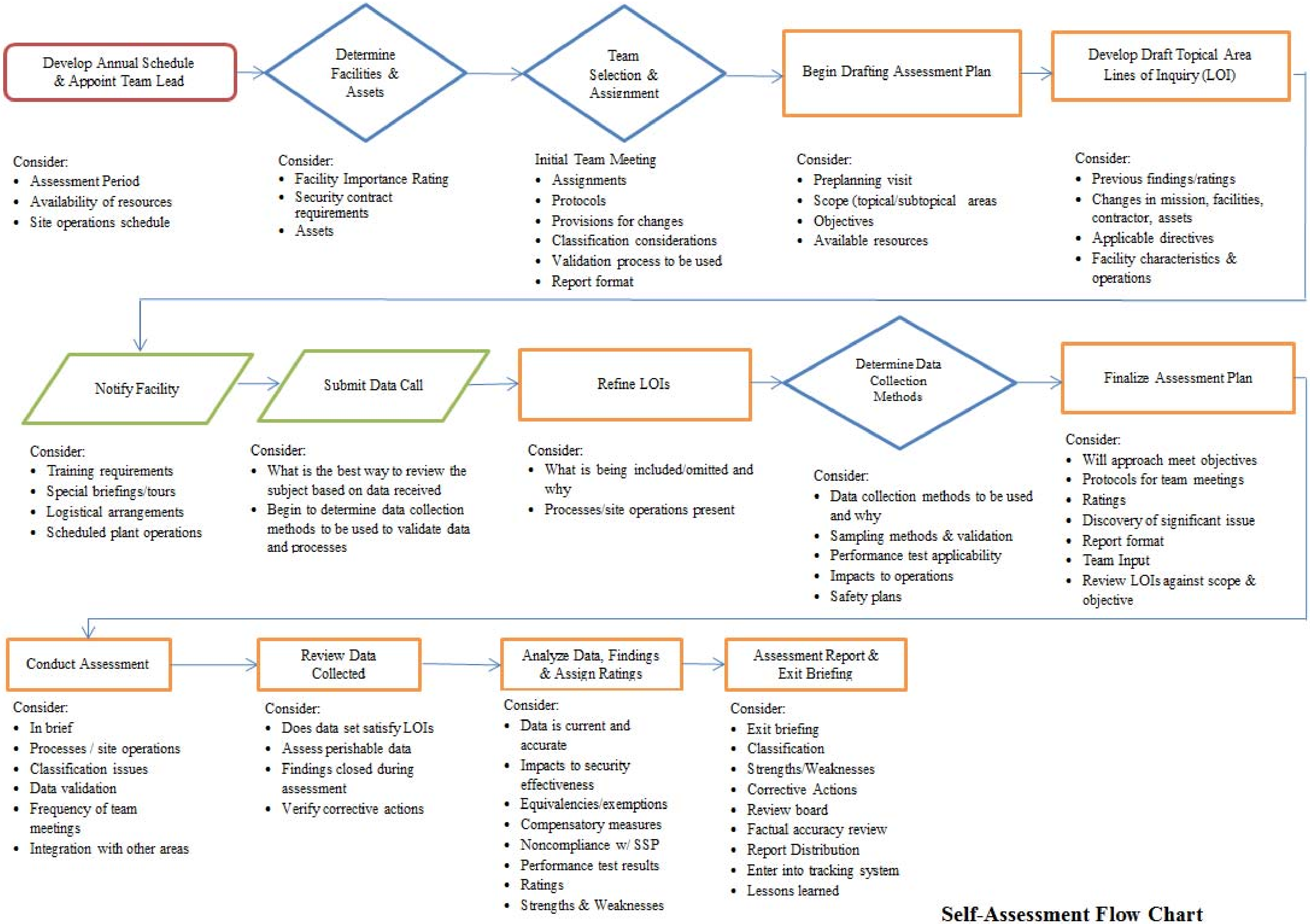
TABLE OF CONTENTS

1.0 PLANNING DOCUMENTATION

IN THIS SECTION:

- Sample Assessment Plans
  - Self-Assessment Flow Chart
  - Assessment Plan Format
  - Assessment Activity Plan
  - Assessment Plan Template
- Documents for Possible Review
- Sample Notification Memorandums
  - Notification Memorandum 1
  - Notification Memorandum 2
- Sample Accommodation Request

Tab 1



Develop Annual Schedule & Appoint Team Lead

Consider:
- Assessment Period
- Availability of resources
- Site operations schedule

Determine Facilities & Assets

Consider:
- Facility Importance Rating
- Security contract requirements
- Assets

Team Selection & Assignment

Initial Team Meeting
- Assignments
- Protocols
- Provisions for changes
- Classification considerations
- Validation process to be used
- Report format

Begin Drafting Assessment Plan

Consider:
- Preplanning visit
- Scope (topical/subtopical areas
- Objectives
- Available resources

Develop Draft Topical Area Lines of Inquiry (LOI)

Consider:
- Previous findings/ratings
- Changes in mission, facilities, contractor, assets
- Applicable directives
- Facility characteristics & operations

Notify Facility

Consider:
- Training requirements
- Special briefings/tours
- Logistical arrangements
- Scheduled plant operations

Submit Data Call

Consider:
- What is the best way to review the subject based on data received
- Begin to determine data collection methods to be used to validate data and processes

Refine LOIs

Consider:
- What is being included/omitted and why
- Processes/site operations present

Determine Data Collection Methods

Consider:
- Data collection methods to be used and why
- Sampling methods & validation
- Performance test applicability
- Impacts to operations
- Safety plans

Finalize Assessment Plan

Consider:
- Will approach meet objectives
- Protocols for team meetings
- Ratings
- Discovery of significant issue
- Report format
- Team Input
- Review LOIs against scope & objective

Conduct Assessment

Consider:
- In brief
- Processes / site operations
- Classification issues
- Data validation
- Frequency of team meetings
- Integration with other areas

Review Data Collected

Consider:
- Does data set satisfy LOIs
- Assess perishable data
- Findings closed during assessment
- Verify corrective actions

Analyze Data, Findings & Assign Ratings

Consider:
- Data is current and accurate
- Impacts to security effectiveness
- Equivalencies/exemptions
- Compensatory measures
- Noncompliance w/ SSP
- Performance test results
- Ratings
- Strengths & Weaknesses

Assessment Report & Exit Briefing

Consider:
- Exit briefing
- Classification
- Strengths/Weaknesses
- Corrective Actions
- Review board
- Factual accuracy review
- Report Distribution
- Enter into tracking system
- Lessons learned

Self-Assessment Flow Chart

SAMPLE ASSESSMENT PLANS

Assessment plans can vary in detail depending on the type/scope of assessment being conducted. The following format is useful when a traditional review is conducted. (Traditional assessments are conducted during a set window, i.e., a two-week conduct period, and are normally comprehensive in nature.)

SAMPLE ASSESSMENT PLAN FORMAT

1. Title
2. Location of facility
3. Purpose
4. Date of conduct
5. General facility information /description
   a. Facility data
   b. Work/activities performed
   c. Operating organization (contractor)
   d. Safeguards and Security (S&S) interests
   e. Work for Others (WFO) or other security activities
6. Scope
   a. Period of review
   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. Planning and preparation
   a. Performance tests (associated safety plans)
   b. Assessment guide information
   c. Pre-assessment information
8. Conduct approach and methodology
   a. Documents to be reviewed
   b. Performance tests
   c. Individuals to be interviewed
9. Schedule of activities
   a. 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. External support
   d. Points of contact (POCs) at the facility
11. Expectations
   a. Conduct
   b. Team meetings
   c. Report preparation
12. Authority/governing documents
   a. Directives
   b. References (unclassified/classified)
13. Report format
14. Administration, support, and logistics
   a. Work facilities
   b. Transportation
   c. Computer support
   d. Administrative support
   e. Classification support
   f. Training requirements
15. Appendices
   a. Performance tests (including Safety Plans)
   b. Assessment guides
   c. Forms

SAMPLE ASSESSMENT ACTIVITY PLAN

A smaller assessment plan might be appropriate if the site has adopted an ongoing assessment process where a single assessment activity might be completed in a day or even a few hours.

Scope: A statement reflecting the scope of the assessment activity. This should include any topical or subtopical areas that were not evaluated and the reason for this omission.

Topical Area(s): The area(s) being assessed should be based on the overall assessment plan as it will serve to guide individual activities.

Assessment Team: Lead: [name, organization, contact information]
[name, organization, contact information]
[name, organization, contact information]

Methodology: Describe the type of data collection to be used (e.g., document reviews, field observations of work, interviews).

Focus/Objectives: Describe the focus or area that will be assessed. For example: a performance test will be conducted to evaluate the accuracy of markings applied to classified documents contained in the following containers …

Schedule: When the activity will be conducted. In some instances a good sampling of data may need to include off shifts (evenings/weekends).

Evaluation Criteria: Each item is appropriately marked in accordance with U.S. Department of Energy (DOE) directives and local site procedures. Include document titles, dates, and approval authority.

SAMPLE SELF-ASSESSMENT PLAN TEMPLATE

Title:

Topical Area: *Based on DOE F 470.8*
Subtopical Area(s):

Facility Name/Code:
Facility Description:

Assessment Team Lead: *Name and organization, area assigned*
Assessment Team Members:
Observer(s):

Assessment Schedule:
Performance Date(s): **In-brief:** **Out-brief:**
Draft Report Date: **Final Report Date:**

Purpose:

Describe why the assessment is being performed (e.g., requirement, management concern, new or modified operations, high-risk program).

Scope:

Describe work system(s)/process(es)/activity(ies), products/output results, or performance goals/measures to be assessed, and identify organization(s) and/or facility(ies) to be included in assessment. If applicable, identify high-risk activity(ies) associated with this scope that could result in significant increased risk to security assets if noncompliant.

If applicable, identify and explain specifically excluded system/process/activity elements, products/output results, performance goals/measures, or organization(s) and/or facilities that would typically be included in the identified scope.

Status of Previous Findings/Corrective Action Plans:

Include status of open findings/corrective actions.

Trending Data:

Review of trending data must be accomplished prior to start of the self-assessment. Opportunities for improvement (OFIs), findings, and security incidents need to be analyzed. This will assist in determining what interviews, performance tests/observations, or random sampling shall be completed during the self-assessment. List the documents that will be reviewed for trending data.

Essential Elements:

Identify equipment, procedures, personnel components, etc. of an S&S system/program whose failure would impact the success of the program and/or reduce the effectiveness to an unacceptable level.

Performance Test(s)/Work Observations/Random Sampling:

Identify planned performance tests, work observations, and/or facility/area walk-downs to be performed. Note: Random sampling will be performed by the assessment team member. Performance testing is the evaluation of task or function execution by individuals, systems, structures, or components against specified qualification standard(s) that must be met for the tested item to be authorized to perform the task or function (e.g., driving test, sensor detection rate, alarm response time). Observance of work activities, processes, or systems is performed to verify actual performance against applicable procedures and/or requirements.

Include list of individuals to be interviewed.

Requirements Documents:

List all requirement documents that will be reviewed. Institutional and organizational requirements must be reviewed if established. Suggested document types are listed below:

- *Federal regulations (Code of Federal Regulations [CFRs], Federal Acquisition Regulations)*
- *Departmental requirements (DOE directives, National Nuclear Security Administration [NNSA] Administration Policies)*
- *Institutional requirements (Site Security Plans [SSPs], Material Control and Accountability [MC&A] Plans)*
- *Organization procedures*

Deviations:

List all deviations current at any time during the past year whether active or inactive at the time of this assessment. Include deviation number, title, date of request, and date of approval/cancellation.

Data Call:

List all requested documents that are produced by or a result of the applicable requirements and that provide evidence of compliance and/or performance. Suggested documents can include any or all of the following:

- *Prior self-assessments and surveys (prior year only)*
- *Open findings*
- *Security incident(s) for the past 12 months*
- *Training materials/plans/rosters*
- *S&S plans, procedures, organization charts, contract documentation*
- *Authorization documents (e.g., approved plans, memoranda, deviations)*

Training:

Note: All personnel involved with carrying out a self-assessment should have taken (include course requirements). Identify site-specific training assessment team members and observers who are required to complete training prior to this assessment.

Safety and Security Considerations:

Identify safety and security issues that team members and observers must be cognizant of during the assessment (e.g., escorting, cell phone/blackberry restrictions, traffic conditions, site terrain). Also, include any required safety equipment (e.g., hardhat, steel-toe shoes, dosimeter) that may be required.

Report Preparation/Format:

Provide team members with applicable worksheets and report formats.

Approvals: *(Obtained after the scoping/preplanning meeting)*

DOCUMENTS FOR POSSIBLE REVIEW

The following is a list of documentation that should be considered for review. 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 scope of each topical area, as outlined in the assessment plan. Documents requested in one topical area may be applicable to another topical area; therefore, to reduce operational impacts, duplicate requests should be kept to a minimum.

PROGRAM MANAGEMENT AND SUPPORT

General

- Applicable memoranda of understanding (MOU) or memoranda of agreement (MOA)
- Approved and pending deviations
- Project execution and management plans for S&S-related projects
- Organizational charts for all elements, Federal and contractor (including significant S&S subcontractors) with S&S responsibilities. Where S&S topical and subtopical responsibilities are apportioned among organizations, provide an overall organization chart indicating the interrelationships of all topics/parties in the conduct of the S&S program.
- Copy of SSP and status
- Copy of most recent self-assessment, survey, and inspection reports
- Copy of findings and corrective action plan (CAP) tracking procedures
- Current status of all open and closed findings and CAPs since the last survey or self-assessment (including Office of Security and Cyber Evaluations, GAO, and IG) as well as all onsite and offsite facilities
- List of all subcontractors performing work (name of company, contract number, names of individuals with access authorizations)

Organization/Staffing

- Organization and function chart to include all S&S personnel (management, staff, and administrative). The list should reflect each person's S&S function(s), duties, and responsibilities (job title); level of access authorization; and entry on duty date.
- Documents depicting responsibilities and authorities of S&S management
- List of all current, approved job analyses (JAs) for S&S employees, their completion date, approval date, review date, and projected review and completion date for any JA changes
- Position descriptions for S&S management
- List of vacancies and length of vacancy

Training

- List of S&S training programs, lesson plan titles for each, and a task-to-training matrix for each
- All S&S personnel training records
- Position descriptions (knowledge, skills, and abilities)
- Training approval program assessment report (most recent)

Evaluation Data

- Survey reports, inspection reports, GAO and IG audit/appraisal reports, self-assessment reports conducted during the past 12 months, and the status of corrective actions for noted deficiencies
- Documentation of the integrated contractor assurance system required by DOE O 226.1, *Implementation of Department of Energy Oversight Policy*

- List of essential elements documented in the Performance Assurance Program (PAP) and the testing schedule for each

Incidents of Security Concern (IOSC) Data

- Documentation concerning all S&S-related reportable occurrences and all security infractions and violations for the past 12 months
- Listing of all S&S-related reportable incidents of concerns to include security infractions and violations issued during the past 24 months; actual inquiry reports should be made available
- Examples of inquiry appointment letters and training profiles

Contractor Information

- List of all active contracts, subcontracts, agreements, or other contractual arrangements involving work for DOE
- List of all active subcontracts and consulting agreements for conducting work for the contractor
- Copies of active Contract Security Classification Specification (CSCS) forms for all contracts, subcontracts, or agreements involving access to classified matter, significant quantities of special nuclear material (SNM), or granting of access
- Copy of procedures for establishing security interests and submitting CSCS forms
- List of all contracts or purchase agreements involving access to classified matter, significant quantities of SNM, or granting of access authorizations that have been executed in the past 12 months. including the statement of work
- List of all subcontractors and consultants conducting work for the contractor
- Copy of all contracts issued to the contractor that require access to classified matter to ensure appropriate DOE directives and security clauses have been incorporated
- Copy of all subcontracts and agreements issued by the contractor that require access to classified matter to ensure appropriate DOE directives and security clauses have been incorporated
- Contractor missions and function manuals or other reference material that describes the roles and responsibilities of current site organizations including deliverables and accountability within the S&S program

S&S Plans and Procedures – A list of all S&S-related plans (including drafts). This list should include title, approval date (submission date for drafts), area/location to which the plan is applicable, and authorized activities (e.g., storage, generation).

- VA reports
- Contingency plans
- Self-assessment program plans, procedures, schedule, reports, CAPs, and status updates for all open deficiencies
- IOSC procedure, including initial notification and inquiry reports
- Approved PAP plan
- Local operating instructions for the implementation of S&S programs
- Approved SSP
- Catalog listing of evidence files supporting the approved SSP and vulnerability assessment (VA)
- Most recently approved Security Incident Response Plan (SIRP) and tactical doctrine
- Copies of the most recent security condition (SECON) plan
- Current graded security protection (GSP) implementation plan and status
- Copies of all active deviations
- Emergency management plans

Foreign Ownership, Control or Influence/Facility Clearance (FOCI/FCL)

- Procedures for the implementation of FOCI requirements.
- Copies of the active Facility Data and Approval Record(s) (FDAR) for the contractor's facility(ies) registered in Safeguards and Security Information Management System (SSIMS)
- Completed Standard Form (SF) 328, *Certificate Pertaining to Foreign Interests*
- Key management personnel (KMP) list
- Dates of all applicable FOCI determinations
- Copy of active FDAR for all corporate tier parents
- Copy of parent exclusion resolution(s)
- Reports submitted documenting significant changes to FCL or documents executed to mitigate any FOCI
  - Significant changes that would modify an existing SF 328
  - Changes to a previously reported threshold/factor that has increased to a level requiring determination by the DOE Office of Health, Safety and Security/Defense Nuclear Security or a different FOCI mitigation method be used
  - Changes that necessitate a change to SF 318
  - Changes in ownership or control, including stock transfers that affect control of the company

PROTECTIVE FORCE

Management/Organization

- Organization/function charts
- Protective Force (PF) general, special, and post orders
- PF shift schedules and post assignments
- MOU with local law enforcement agencies and documentation of exercises conducted with those agencies
- Integration of crisis management personnel into procedures
- List for managers or POCs, with telephone numbers and locations, responsible for the following PF areas: management, training, duties (operations manager), equipment and facilities, and performance testing
- Inventory of PF equipment to include: vehicles, weapons, night vision goggles (NVG), radios, non-lethal weapons, breaching equipment, etc.
- VA and SSP development process protocol documents
- Process for developing adversary strategies/tactics
- Process for evaluating insider adversaries, both working alone and in collusion with the outsider
- Process for developing and evaluating upgrade/efficiency packages
- Presentation of chronological efforts and events leading up to the current/approved SSP (include VAs, validations, peer reviews, headquarters [HQ] visits, etc.)
- Data from PF performance testing that supports the most recent VA or PF performance assumptions made in the VA requested above, particularly any performance tests included in the calculation of the probability of neutralization
- List of Adversary Timeline Analysis System (ATLAS) or Analytic System and Software for Evaluating Safeguards and Security (ASSESS) files used to develop the VA and the associated evidence files for the following types of data:
  - Modeling inputs
  - PF response
  - Adversary capabilities
  - Blast effects

  - Sabotage data (if appropriate)
  - Timeline data
  - Neutralization data
  - Special weapons effectiveness
- Joint Conflict and Tactical Simulation (JCATS) and other PF simulations reports and capability to review sample scenarios
- Tabletop qualitative methods, copies of any meeting notes, and supported documentations for rating, if applicable

Facilities/Equipment

- Standard PF equipment issuance (Security Police Officer [SPO]-I, -II, -III, and Special Response Team [SRT])
- Ammunition inventories
- Comprehensive weapons inventory list to include serial numbers
- Weapons maintenance logs
- Follow-up/investigative reports for inventory shortages, property loss, property theft, or missing property for the last fiscal year
- Inventory of PF equipment to include: vehicles, NVG, radios, non-lethal weapons, breaching equipment, etc.

Training/Qualification

- List of PF personnel who are subject to weapons qualification within 90 days of the assessment start date
- Training approval plan certification/recertification letter from the National Training Center (NTC)
- Annual training plan
- Annual SRT certification by the Site Office
- PF training records
- Certification records (instructors [classroom and range], armorer, central alarm station [CAS]/secondary alarm station [SAS] operators, SRT members, part-time trainers)
- Current year training schedule
- SPO lesson plans
- 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 self-assessment
- CAS operator annual refresher training lesson plans
- Last force-on-force (FOF) test plan, risk assessment and performance test results
- Job task analyses (JTAs)
- Performance test program procedure, schedule, and documentation for the last 12 months
- Bank of test questions typically used for SPO knowledge tests
- Alarm response and assessment performance test (ARAPT) plan
- Engagement Simulation System (ESS) guidelines for conducting performance tests
- ARAPT/no-notice limited scope performance test (LSPT) reports from the last 12 months

Duties

- Compensatory measures currently in place (including pertinent documentation) and notification process
- Procedures (administrative, training, non-response-related operational requirements)
- Access/badge control
- Policies/procedures for issuing, replacing, and recovering passes/badges

- Inventories (since last S&S survey/self-assessment) of passes/badges made, issued, lost, recovered, returned, and destroyed
- PF fitness for duty inspection process
- Site map indicating PF fixed posts and patrol areas
- List of all posts and patrols, location of their corresponding orders
- Current PF procedures, general, special, and post orders, including fixed post and mobile patrol orders
- Current "on-shift" PF duty roster (spreadsheet format) to include: SPO level, rank (if applicable) and weapons used for the period: [insert date]
- Sample of supervisor and post logs

Plans

- Security Emergency Response Plan (SERP)
- SIRP
- Facility evacuation response plans
- Security contingency response plans
- Shipment security plans
- Shipment procedures
- In-transit emergency plan
- Shipment emergency response plan
- Target folders

Provide an informal briefing that includes

- Changes in program management since the last self-assessment
- Prior findings and status of corrective actions with supporting documentation
- Corrective action and causal analysis processes
- Overview of contract management structure
- VA process reflecting the implementation of DOE planning requirements; cover integration of planning, equipment selection and utilization, barrier placement, PF organization and training, and mechanisms that provide VA analysts with performance tested validation of VA assumptions and values
- PAP integration by the contractor, if applicable, including testing and maintenance results, PF LSPTs, training, ARAPTs, etc., to accomplish the self-assessment program objectives

PHYSICAL SECURITY

General

- Organization and function charts
- Physical security system (PSS) description(s) and location(s)
- Site plan drawing indicating security areas and target location(s), include all maintenance and communications facilities as well as locations of the CAS and SAS
- List all approved PSS deviations
- List of all PSS-related self-assessments, surveys, inspections, and external reviews completed during the past 12 months and associated CAPs
- List of all vaults and vault-type rooms, including up-to-date floor plans
- List of current compensatory measures

Access Controls

- Automated access control system records and procedures, including biometric access input as well as access credential issuances (e.g., keycards, tokens)
- Property control procedures
- Access control procedures
- Security container documentation and maintenance records
- Automated systems description and procedures
- Inspection procedures
- List of all badges and passes issued, stored, lost or stolen, reissued, and retrieved at the time of separation
- System description and diagram for all access control systems, include description of badging systems, procedures for badge fabrication, personnel enrollment, interface between badge systems with CAS/SAS, and a VA
- Description of the explosive detection program
- Lock and key control policies, procedures, accountability documentation, audits, and key and combination changing procedures

Intrusion Detection System (IDS)

- IDS maintenance and testing records and procedures
- Unscheduled alarm reports
- CAS/SAS procedures (interface description)
- Emergency response for CAS/SAS recovery
- Emergency power systems (uninterruptible power supply [UPS])
- Compensatory procedures for equipment outages
- Documentation detailing all changes in alarm systems (including computer software) since the last self-assessment, including the procedures to ensure changes are correctly implemented and no unauthorized changes have occurred
- List of all incoming alarms for the week of [date]
- System description and diagram for all alarm monitoring and control systems, including locations of major equipment (data gathering panels, activation panels, and communication panels) for interior and exterior systems, if applicable
- System description and diagram for all primary and auxiliary power systems associated with all PSS, including generators, automatic failover systems, UPS systems, etc.
- Procedures for testing auxiliary power systems and documentation of test results from the past 12 months
- Description of all types of line supervision and tamper alarms used and where they are located
- Procedures and test results of redundant CAS/SAS operations and failover features
- Configuration management policies and procedures for PSS hardware and software
- Alarm system operator training and testing documentation
- Alarm recording logs for [period]
- Copy of the PSS critical system elements (CSEs) and essential element lists
- Copy of PSS-related compensatory plans
- Procedures and program description for false alarm rate (FAR) and nuisance alarm rate (NAR) reviews, analyses, and corrective action development
- FAR and NAR data and analysis for all security system sensors for the past six months
- Lighting testing results for past 6 months
- Description of planned upgrades relating to PSS, including status of authorization and funding as well as the expected date the planned upgrades will be in service. Additionally, descriptions and

dates of implementation for all upgrades and modifications to alarm monitoring and video assessment systems, access control systems, and security-related voice communications systems, that have been completed in the last 5 years (hardware and software).

Barriers

- Barrier maintenance procedures and records
- Description and diagrams for all active or passive barrier systems used to direct or control the movement of personnel and vehicles through security area boundaries
- Procedures to identify potential barrier degradation

Testing and Maintenance

- Local performance testing plans and procedures
- Procedures for requesting maintenance for security systems
- Calibration and testing procedures and records (e.g., X-ray, metal detectors, IDS)
- Testing records for the last year for security systems and components, including the UPS (e.g., battery, emergency generator), and the frequency of testing
- Copies of test procedures, including frequency of testing for security systems components (e.g., alarm sensors, tamper capabilities, and auxiliary power systems) available for review
- Security systems preventive and corrective maintenance and testing program documentation and procedures with a list of maintenance activities associated with all PSS in the past 12 months
- Performance testing criteria for alarm monitoring and video assessment systems, access control systems, and security-related voice communications systems; note that this information should include automatic failover testing criteria to move from CAS operation to SAS operation
- List of all PSS-related performance testing activities completed during the past 12 months
- Acceptance testing procedures for installation of new or replaced security systems

Communications

- Manual
- Procedures
- Controls
- System description and one-line diagram for all security-related voice communications systems including backup systems to include:
  - Make and model of radio equipment in service
  - Signal coverage map of site
  - Features used to mitigate or detect jamming
  - Alternate communication modes
  - Locations of major transmission/control equipment such as mobile and fixed antennas
  - Base stations
  - Amplifiers
  - Repeaters
  - Power supplies
- VA
- Description of the emergency communications plan (may be within the tactical defense plan or PF response plan)

INFORMATION PROTECTION

Basic Requirements

- Organization and function charts

- Training records

Technical Surveillance Countermeasure (TSCM)

- TSCM survey reports
- Site inventory of accredited systems, showing property tag number, accrediting authority, and most recent accreditation date for each
- Formal assignments of TSCM operations manager (TSCMOM) and TSCM officer (TSCMO)
- TSCM activity support memoranda (if applicable)
- Local TSCM implementation guidance
- TSCMO service schedules, files, and corrective action reports
- TSCM team equipment maintenance and calibration files
- TSCM team training and certification records

Operations Security (OPSEC)

- OPSEC plans
- OPSEC procedures
- OPSEC program files
- Local threat statement
- Critical information
- Counter-Imagery Program Plan (if applicable)

Classification

- List of all classification personnel to include derivative classifiers (DCs) and DDs, classification officer (CO), and Unclassified Controlled Nuclear Information (UCNI) review officials; indicate each person's job title, DC or DD, and appointment authority
- Appointment letters (e.g., CO, DC, UCNI reviewing official [RO])
- Training records, reports, and lesson plans
- List of all HQ and locally approved classification guides and a list of individuals issued to
- Copy of the corrective actions implemented for any findings issued within the last 24 months
- Copy of CO position description and evaluations identifying critical skills; include other positions evaluated as being critical performers
- Statistics for the last 24 months of classification and declassification activities
- Sampling of all approved CSCS(s) that require generating classified and include the classification guidance required for performance on the contract
- Declassification initiatives completed or continuing during the last 24 months
- Procedures for reviewing requirements for classified working papers

Classified Matter Protection and Control (CMPC)

- CMPC procedures
- Appointment letters (e.g., custodians, control station personnel, alternate custodians/controls station personnel)
- Control station procedures
- Copy of the latest CMPC-related training materials, specifically CMPC-related custodian and refresher training/briefings
- Copies of all classified document inventories conducted in the last 12 months
- Sample copy of accountability log, destruction log, incoming and outgoing mail logs, or any other site-specific log used within the CMPC program
- List of individuals approved to hand-carry classified matter

- List of personnel authorized to receive matter addressed to the classified mailing address, prepare classified documents for transmittal, and access classified matter repositories
- List of classified holdings, including documents and matter
- List of control stations locations
- Procedures for appropriate marking, storage, and destruction of classified removable electronic media (CREM)
- Current organization chart with identified information protection, CMPC, and classification function identified
- List of security areas (temporary, limited areas [LAs], or higher, if any); include information for POCs and approved area activities and functions
- List of security containers (including vault-type rooms and vaults) and their location by building and room; containers that store accountable matter should be further identified by matter type
- Copy of the corrective actions implemented for any findings issued within the last 24 months

PERSONNEL SECURITY

Access Authorizations

- Local procedures for terminations, leaves of absence, reinstating clearances, clearance processing, and exit briefing process
- Contractor access authorization requests
- Reciprocal access authorization documentation
- Security infraction and violation records
- Central Personnel Clearance Index (CPCI) list of individuals overdue for reinvestigation
- List of individuals on leaves of absence and associated procedures for tracking
- List of inactive classified contracts for the past 5 years
- List of personnel with access authorizations and the associated contract
- List of all cleared employees who are or have been absent from work for more than 90 days (e.g., leave, assignment, extended travel); include name, position, clearance number, and dates of absence
- List of all new hires since [date]
- List of all employees terminated since [date]; include name, clearance number, and date of termination
- List of special term appointees, levels of clearance, and the last time classified was accessed
- Current list of all employees with access to Sensitive Compartmented Information (SCI) and Nuclear Weapons Data

Human Reliability Program (HRP)

- Drug testing/handling procedures
- Drug testing records
- HRP criteria, plans, and procedures
- Random test procedures
- Copy of the HRP implementation plan(s) and documentation of review and approval by the site manager
- List of positions identified for HRP certification and a description of the process for evaluating these positions for certification, including those positions applicable to 10 CFR 712, Category 4
- Alphabetized lists (last name first) of HRP employees for the period of January 1 through May 1, [year], separately by the following groups:
  – All HRP individuals that have been temporarily removed with the date of removal and reason (security, safety, medical, or change of position/employment)

  - All HRP individuals that have had their HRP certification revoked with the date and reason (security, safety, medical or changes of position/employment)
  - All individuals denied HRP certification by the site certifying official
  - All HRP individuals that have had any disciplinary action(s), including the reason, date the action was taken, and if the individual was temporarily removed from HRP because of the disciplinary action
  - All HRP individuals that have been involved in an accident or incident, including incidents of security reported as an occurrence to DOE
- Alphabetized list (last name first) of all non-HRP escorted individuals indicating the dates of entry for the period January 1 through May 1, [year], grouped for each escorted visitor with all date(s) (most recent first) of entry for each material access area (MAA), and the individual's employer; include the individual's authorized clearance level at the time of entry (Q or L)
- List of job titles for which JTAs have been developed for each organization and an example (blank form) for the JTA format used by each organization
- HRP files and HRP-associated medical and psychologist files
- Copies of HRP training and instructional materials (computer-based, classroom, etc.)
- Names and letters, if used, for designation of the following positions:
  - HRP certifying official
  - HRP management officials
  - Designated physician
  - Designated psychologist

Control of Classified Visits

- Request for visit or access approval (notification and approval of incoming and outgoing classified visits records)
- Visitor control logs
- Local visitor control procedures
- Classified visit program procedures
- List of individuals requesting a classified visit, name of host, and type of information and accessed

S&S Awareness

- Sample training curriculum, briefing materials
- Awareness tools (posters, newsletters)
- List of all security education briefings conducted since [date] by type of briefing (e.g., initial, comprehensive, refresher, and termination), name, and date of briefing

UNCLASSIFIED VISITS AND ASSIGNMENTS BY FOREIGN NATIONALS

- List of all site visits/assignments by foreign nationals (FNs) since [date], to include those FNs from terrorist-sponsored countries; include visitor's name, country of birth, country of citizenship, visit/work area(s) on site, beginning and ending date of visit/assignment
- Specific security plans for FNs visiting from sensitive countries
- Escort procedures
- Local procedures for requesting, processing, and approving visits and assignments
- Documentation authorizing approval for specific categories of visits and assignments
- Incident reports involving FNs
- Requests for FN visit
- Indices checks

- List of sensitive subjects
- List of sensitive countries
- Deviations pertinent to visits and assignments
- Personnel assignment agreements
- Specific security plans and IA-593s, as well as a record of indices checks and visitor registration logs applicable to such visits since [date]
- List of foreign visitors that required an export license
- Procedures for export control

NUCLEAR MATERIALS CONTROL AND ACCOUNTABILITY

- Approved MC&A pan with approval letter from the responsible federal element
- Search procedures
- Material surveillance procedures
- Portal monitor records and procedures
- Daily administrative check program and procedures
- Incident reporting process and procedures
- Internal control procedures
- Emergency response plans and facility procedures
- Emergency plans pertinent to the loss of control of SNM
- Shipper/receiver difference procedures and records
- Facility procedures
- Procedures for monitoring rollup and the most recent VA
- MC&A functional organization chart
- List of MC&A deviations with supporting documentation
- Training records, reports, and lesson plans
- Performance tests
- Categorization process documentation
- Database descriptions
- Material balance area (MBA) account structure
- Material transfer records
- Nuclear Material Management and Safeguards System (NMMSS) reports
- Material control indicator program
- Inventory difference program
- Materials containment documentation
- Material access program
- Authorization access lists
- List of tamper indicating devices (TIDs), custodians, applicators and/or verifiers, and TID procedures (if not included in MC&A procedures manual)
- Current list of all areas authorized for the use and storage of nuclear materials, including names of the custodians and alternates and a brief description of the area
- One set of nuclear material inventory listings for the site as of [date]
- List of all internal and external nuclear material transfer documents for the period [date] through [date]
- List of all measurement systems qualified for accountability purposes including precision and accuracy requirements for each measurement technique
- All accountability ledgers (manual and automated), documents, and procedures should be available

- Complete list of findings and corrective actions conducted during [period] (may be included with program management documentation; if so, please state)
- All facility-reported incidents involving MC&A, security, and operations for the past 2 years with backup documentation
- Internal Review and Assessment Plan (IRAP) and procedure, internal review and assessments completed since [date], and the current IRAP schedule for [year].
- Summary inventory list for MBAs showing total quantities for each material type (may be kept with accounting organization and will be reviewed during the assessment)
- Procedures for measuring holdup (if not included in the MC&A procedures manual)
- Summary information on holdup measurements conducted since [date]
- Statistical sampling plans and procedures used for physical inventory and confirmation and verification measurements (if not included in the MC&A procedures manual)
- Status of SNM considered unmeasured and/or not amenable to measurement sorted by MBA (if not included in the MC&A plan)
- Safeguards termination documentation on nuclear materials terminated [date]
- List of current measurement procedures for approved accountability systems (actual procedures may be requested)
- List of current measurement control procedures for approved accountability systems (actual procedures may be requested)
- List of replicate data used in the determination of measurement uncertainties for the last six inventories.
- Inventory procedures and schedules (if not included in the MC&A procedures manual).
- Sampling plans (if not included in the MC&A procedures manual) and the results of the verification/confirmation program for the previous two physical inventories
- VA demonstrating MC&A analyses for Category I SNM locations and other locations where rollup to Category II is credible (if not provided in above)
- List of defined MC&A CSEs, list of MC&A-approved performance test plans, and a summary of MC&A performance tests the site conducts as part of the performance testing program.
- List of any MC&A performance incentives or award fee items in the MC&A area
- Inventory differences, Limit of Error of the Inventory Difference (LEID), and identification of key measurement error contributors by material type by MBA for each inventory period for the last 18 months

Briefings

- General overview of site MC&A activities including a description of the current MC&A organizational structure (Federal and contractor, including names of individuals and funding mechanisms)
- Overview of MOU between the MC&A organization and other organizations for which the MC&A organization provides MC&A services
- List of MBAs and the category of each MBA
- Status of previous findings and OPIs and the status of CAPs
- Approval status of MC&A documents and a list of approved deviations
- Overview of MC&A accounting and measurement systems

It is very important that the briefing also include the results of recent assessments and key issues currently being addressed by the MC&A program. Copies of the briefing notes should be provided.

NOTIFICATION MEMO 1

SUBJECT: Safeguards and Security Self-Assessment

The [organization] will conduct a Safeguards and Security (S&S) Self-Assessment of [organization] during the period of [dates]. This will be a comprehensive self-assessment and will be conducted in accordance with DOE O 470.4B, *Safeguards and Security Program.* The assessment will examine the compliance and performance of S&S programs with DOE policy and SSPs 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 [team lead] not later than close of business [date]. In addition, please provide point of contact information for each topical area, including email addresses and phone numbers. The names of assessment team members will be forwarded to your organization under separate cover.

Self-assessment activities will begin with an in-briefing at [date, time, and 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 [team lead name, phone, and email].

Attachment

NOTIFICATION MEMO 2

Subject: Safeguards and Security Self-Assessment

This memorandum confirms informal discussions between [assessing office] and [organization to be assessed] regarding conduct of the upcoming Safeguards and Security (S&S) Self-Assessment. As agreed, the assessment will take place [dates], and will be focused on the requirements contained in applicable DOE and site implementing directives.

An informal preliminary meeting is scheduled for [date, time] with S&S management and selected site personnel. The self-assessment process, schedule, and focus will be discussed during this meeting.

To assist with planning efforts, an assessment questionnaire and data call is attached. Please provide the requested information to [team lead] by [date]. This material will be distributed to team members for review and familiarization prior to the assessment.

If there are any questions regarding this self-assessment, please contact [team lead] at [phone number, email]. Your assistance is appreciated.

Enclosures

SAMPLE ACCOMMODATION REQUEST

The following items may need to be available to the assessment team:

- One conference room or a two-office suite with tables and seating for 5 to 10 people
- Access to a classified conference room
- Four unclassified desktop computers loaded with Microsoft Word 7.0 and two unclassified printers
- Telephones with outside lines and a POC list
- Whiteboard and associated supplies
- U.S. General Services Administration (GSA)-approved security container (with appropriate markings and required forms)
- Office supplies (staplers, scissors, tape, classification stamps, etc.)

SAMPLE TRAINING/SAFETY CHECKLIST

Safety is paramount to any assessment activity. A checklist may be appropriate to ensure required training and paperwork is completed.

Training/Safety Checklist			
Team Member: Date Arriving Onsite: Topical Area: Area Access Required: Material Access Area Access Required:			
Training Required	Yes	No	Preferred Date/Time
Chamber Tests Classified Cyber General Employee Resource Conservation Restoration Act of 1976 (RCRA)			
Required Paperwork			
Dosimeter Accountability Tags Badging Other:			
Safety Equipment			
Shoes Glasses Mask			Size _________ 1/2 or Full Face
Approved By:			Date:
Topical Area Lead:			
Assessment Team Leader:			

2.0 CONDUCT TOOLS

IN THIS SECTION:

- Sample In-Briefing
- Worksheet
- Data Collection Form
- Sampling Methodology
- Developing and Conducting Performance Tests
- Performance Test Safety Plan
- Performance Test Plan
- No-Notice Performance Test: Best Practice

Tab 2

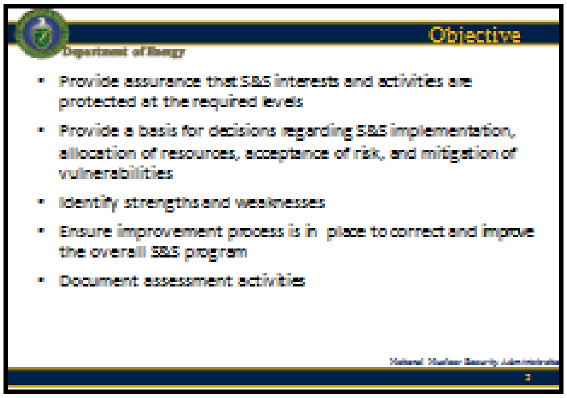
SAMPLE IN-BRIEFING

Self- Assessment

Facility Name

Dates

Conducting Organization



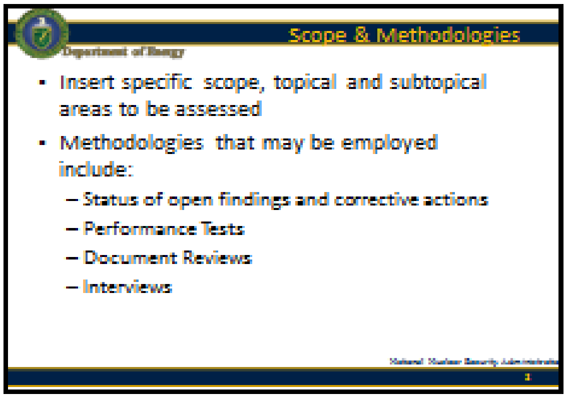
Objective

Department of Energy

- Provide assurance that S&S interests and activities are protected at the required levels
- Provide a basis for decisions regarding S&S implementation, allocation of resources, acceptance of risk, and mitigation of vulnerabilities
- Identify strengths and weaknesses
- Ensure improvement process is in place to correct and improve the overall S&S program
- Document assessment activities

National Nuclear Security Administration

2



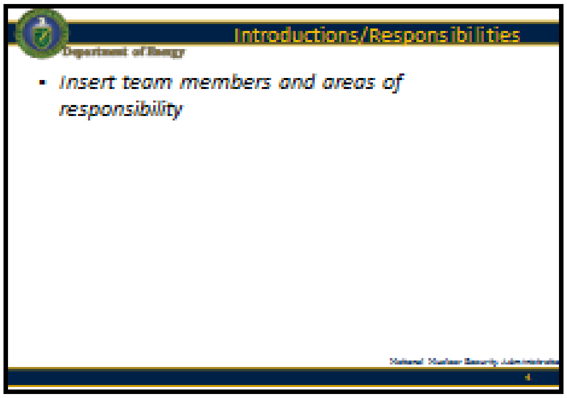
Scope & Methodologies

Department of Energy

- Insert specific scope, topical and subtopical areas to be assessed
- Methodologies that may be employed include:
  - Status of open findings and corrective actions
  - Performance Tests
  - Document Reviews
  - Interviews

National Nuclear Security Administration

3



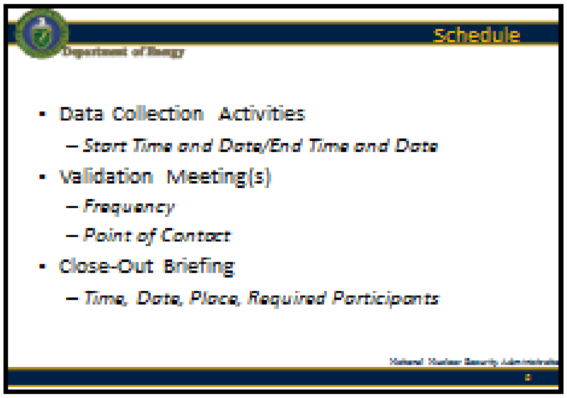
Introductions/Responsibilities

Department of Energy

- *Insert team members and areas of responsibility*

National Nuclear Security Administration

4



Schedule

Department of Energy

- Data Collection Activities
  - *Start Time and Date/End Time and Date*
- Validation Meeting(s)
  - *Frequency*
  - *Point of Contact*
- Close-Out Briefing
  - *Time, Date, Place, Required Participants*

National Nuclear Security Administration

5

SAMPLE WORKSHEET

This form may be used to capture data collection details (both positive and negative).

CLASSIFICATION

WORKSHEET
Date:
Responsible Organization:
Finding: OFI: Best Practice:
Concern: Compliance Performance Both:
Topical Area: Subtopical Area:
Description: *The finding description should be used to provide a clear understanding of what was observed or discovered; it is not adequate to reiterate the requirement. The description should clearly identify the pertinent facts, circumstances, and observations surrounding the finding or leading to the finding.* *Findings should be clear and focused on the root cause of the observed protection shortfall, rather than merely stating the occurrence of a protection element failure or weakness. A finding should be written in such a manner that it is actionable by the responsible agency, i.e., that action can be taken that will close the finding and that this action will correct the observed deficiency. A well-worded finding is readily closeable when the cause or source is corrected and impossible to close without correcting the cause or source.* *Necessary and pertinent information should be presented regarding the finding in order to clearly identify what was found, how the information was collected, and any other background information. The discussions should attempt to correlate the data collected and focus on the root cause of the deficiency. The nature of the data (observations, interviews, tests) should be described as well as any quantifying data that will put the results in perspective.*
Synopsis: *Each finding should be concisely described and have a separate, standalone classification level and category in a separate field. 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.*
Impact: *Clearly state the immediate or potential impact that exists because of the issue.*
DOE Directive:
Other (Plan Or Procedure Citation):
Assessor's Name/Phone:
POC Name/Phone:

CLASSIFICATION

FCOG

DATA COLLECTION FORM

This form is used to document self-assessment activities.

CLASSIFICATION

DATA COLLECTION FORM

Date:	
Team Member:	
Site:	
Topical Area:	Subtopical Area:

(U) Results:

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

(U) Impact:

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

(U) Need for Additional Information:

Briefly state the need to collect additional information and what data collection activity will be conducted to meet this need. If none, then state accordingly.

Supporting Documentation:

Title:
Date:
Interview Participants:

Interview Date:

CLASSIFICATION

STATISTICAL SAMPLING METHODOLOGY

The following statistical sampling methodology can be readily applied to most S&S elements:

$$n = 0.5 \ (\ 1-\beta^{1/D}) \ (2N-D+1)$$

Where: n = the sample size

β = confidence level

N = population size

D = minimum detectable defective

Example: If it was necessary to sample a key inventory with 400 keys (Lock and Key subtopical area), and the goal was to detect a minimum error rate of 10% in the key inventory with a 95% confidence level, the formula would be: $n = 0.5(1-.95^{1/.10}) \ (2*400-.10+1) = 160.18$. Based on this equation, a sample of 160 randomly selected keys would be necessary to achieve a 10% error rate with a 95% confidence level.

SAMPLING METHODOLOGY

The following sample methodology was contained in the 2009 DOE Office of Independent Oversight (now the Office of Security and Cyber Evaluations) document, *Classified Matter Protection and Control Inspectors Guide.*

Introduction

The Office of Independent Oversight conducts inspections to assess the effectiveness of DOE S&S programs. Confidence in these assessments is influenced by perceptions of consistency, thoroughness, and fairness in conducting the inspections. The use of scientifically valid methods for gathering and interpreting information strengthens the confidence in the results obtained.

In performing inspections of items or individuals (i.e., populations) at a facility, often it is necessary to determine what proportion possesses a certain characteristic. For example, it may be necessary to determine what proportion of classified documents is properly accounted for in a facility's inventory. In most cases, a 100% inspection of the population is impractical; however, pertinent information can be obtained by examining a portion, or sample, of the population and drawing inferences that extend to the entire population. Properly used, statistical sampling allows these inferences to be drawn accurately.

The Office of Independent Oversight has developed statistically valid, practical procedures for gathering information during inspections. The procedures specify methods and indicate the types of conclusions that can be drawn from the sample results. The procedures also specify the sizes of the samples to be selected and the techniques for randomly selecting the samples.

The remainder of this paper is organized as follows: Section 2.0 presents a general sampling methodology that is applicable to most topics; Section 3.0 covers a discussion of the Office of Independent Oversight's application of sampling methods to the review of classified document and material accountability; and Section 4 provides post-assessment tools. This paper focuses on sampling techniques, which is only one of the activities conducted by the Office of Independent Oversight to review a facility's information security program.

General Sampling Methodology Considerations

Although the Office of Independent Oversight's comprehensive inspections are very broad, there frequently are too many items in a given population to permit a 100% inspection because of limited time and other resource availability. The tasks that must be addressed in conducting statistical sampling are (1) defining the population, (2) determining a sample size and level of confidence, and (3) selecting random samples.

Defining the Population

In defining the population, a clear, complete, and accurate statement of the objectives of the statistical sampling is essential. The population is then defined in accordance with these objectives. Defining the population to be sampled is the first step in the sampling process.

It must be clear to the inspection team exactly which items belong to the population being sampled and, in some complex cases, it may be appropriate to reconsider the objectives to ensure that no ambiguities or gaps exist. If the population is well defined, identifying the items that comprise the population and specifying the data to be collected are usually straightforward. If difficulties are encountered in preparing a list of items or in defining data requirements, it is likely that those difficulties can be traced back to population definition.

Definition of the population forms the basis for sample selection. For example, if classified documents are being inspected for proper markings and the population is defined as all classified documents at a particular site, then a sample of classified documents would be selected for examination from this population. In selecting this sample, it would be inappropriate to confine the sample to only one or a few of the locations at the site where classified documents are held. Although confining the sampling would be convenient, it would not permit generalizations to be made about the population of classified documents as a whole. If a sample were confined to only one or a few locations, then the population is only the documents at those locations and generalizations would apply only to this restricted population and not to the defined population of all documents at the site.

Determining a Sample Size and Level of Confidence

The sample to be observed must be specified. This requires that the sample size be determined. In turn, sample size reflects the degree of precision that is desired in the results. Whenever inferences are made on the basis of a sample, some uncertainty must be accepted because only part of the population is being measured or observed. Thus, the amount of error that can be tolerated without compromising the quality of decisions or conclusions beyond acceptable limits should be kept to a minimum.

In determining sample sizes for a particular sample problem, confidence levels are associated with statements made about the outcome of the sampling procedure. For example, statistical inferences made at a 95% level of confidence are correct 95% of the time. Thus, if a random sample of 200 items is selected and zero defects are observed, it can be stated with 95% confidence that the true proportion of defectives in the population is at most 0.015 (1.5%). In this same case of a sample of 200 items and zero defects, it can also be stated with 80% confidence that the true proportion of defectives in the population is at most 0.008 (0.85). Thus, a lower level of confidence permits a more reliable statement to be made about the population proportion, but at the price of an increased chance of an incorrect statement—in this case, a 55 chance of being wrong versus a 205 chance of being wrong.

For facilities with large (more than 1,000) classified document inventories, the population size (i.e., the total number of documents in the inventory) is not a major determinant of sample size. In such cases, the inspectors should select as large a sample as possible given the time and resource constraints of the inspection. With large samples, the inspectors can develop more reliable estimates of the proportion of defective items.

Selecting Random Samples

Statistical inferences are drawn from observations of random samples selected from populations. The basic theory underlying statistical inferences requires that the samples be selected randomly to allow valid conclusions about the population as a whole. For example, if the surveyed population of sensitive documents contains a finite number of documents, a random sample is selected so that the probability of individual documents being chosen is the same as for any other sample of the same size.

Two specific steps involved in selecting a random sample are enumerating the population units and generating random numbers to match to the enumerated population. These steps are defined as follows:

- **Enumerating.** The individual items in the population being sampled are enumerated; i.e., they are arranged in any convenient (or natural) order and assigned unique sequential numbers. For relatively small populations (on the order of a few hundred or less), this can be done manually. For larger populations containing several hundreds or thousands of items, a computer system is preferable for preparing and executing a sample selection process efficiently.
- **Matching Random Numbers to the Population.** Any one of several widely available and well-documented computer programs can be used to select a random sample from a population. These programs produce a list of distinct random numbers within the range corresponding to the population size. These programs can be found on many computer systems; however, not all populations have computer programs/systems that can be adapted to the sampling process. Those facilities that maintain inventory records with computerized systems typically have such

programs in place for various administrative purposes and, with minor modifications, can produce random sampling tools useful for the SP-40 inspection process.

For large populations in which records are maintained on computer systems, a program can be prepared to generate the random numbers and then match these with the population computer file to produce a list of sample items. For example, if a population of classified documents to be surveyed is composed of 100,000 documents and the document accountability records are on a computer system, the following procedure is an acceptable means of selecting a sample:

- Number the records from 1 to 100,000; that is, create a computer file containing the individual records consecutively numbered.
- Use a computer program to generate 200 random numbers from the range 1 to 100,000 and match the numbers with the main file of records. The output of this simple routine is the list of 200 documents comprising the sample.

An important point when dealing with computer inventories is that it is not necessary to produce hardcopy listings of entire populations. Computer files containing the information in the proper format either already exist or can be prepared (by minor modifications in many cases) from existing programs. To avoid reducing the time available for inspection activities, computer programs that will carry out the sample selection process should be prepared or modified before the inspection. Also, the computer programming requirements should be identified during the planning stage of the inspection.

Some procedures used to select samples, although "random-like," cannot be considered to produce random samples for a valid statistical methodology. For example, starting at the top of a list of documents and selecting every 50th document until 200 are selected will not produce a statistically valid random sample. Such a procedure may yield a biased sample. A random sample is produced only by following well-defined and accepted procedures for generating random numbers to select members from a population. If these procedures are followed, the resulting sample is truly random; otherwise, it is not.

Determining Confidence Intervals

Table 1 provides sets of confidence intervals that can be used to estimate the percentages of accountable and unaccountable documents in an inventory system. These confidence intervals can be applied to the results of a "front check" document accountability performance test. Once the test has been concluded, Table 1 should be used to evaluate the results.

The table is used by locating the appropriate sample size block and then reading down the left side of the table to the appropriate "number of defects." The bracketed numbers at this point are the upper and lower confidence limits for statements that can be made about the document population. For example, if the sample size is 200 and two documents cannot be located, then one can state with 95% confidence that no more than 3.114% of the total accountable document inventory is unaccounted for. Or one can state with 95% confidence that at least 0.178% of the total accountable document inventory is unaccounted for. If the population in this example were 100,000 accountable documents, this means that one can be 95% confident that at least 178 accountable documents are unaccounted for in this system. Finally, one can also make the statement with 90% confidence that the number of unaccounted-for documents in this system is somewhere between 0.178% and 3.114%, which means that there are between 178 and 3,114 unaccounted-for accountable documents.

Note that the level of confidence for this last statement dropped from the 95% used in the previous two statements to 90%. This is because the statement that the number of unaccounted-for documents is between 178 and 3,114 is a stronger statement than the other two, which are essentially "either/or" statements. The price paid statistically for this stronger statement is a lower level of confidence.

Table 1. Ninety Percent Two-Sided Confidence Levels for the Proportion of Defects

Number of Defects	Sample Size			
	100	125	150	175
0	(.00000, .02951)	(.00000, .02368)	(.00000, .01977)	(.00000, .01697)
1	(.00051, .04656)	(.00041, .03739)	(.00034, .03123)	(.00029, .02682)
2	(.00357, .06162)	(.00285, .04951)	(.00237, .04138)	(.00203, .03554)
3	(.00823, .07571)	(.00657, .06086)	(.00547, .05088)	(.00469, .04371)
4	(.01378, .08920)	(.01100, .07173)	(.00916, .05998)	(.00784, .05154)
5	(.01991, .10225)	(.01589, .08226)	(.01322, .06881)	(.01132, .05913)
6	(.02645, .11499)	(.02111, .09254)	(.01756, .07742)	(.01503, .06654)
7	(.03331, .12746)	(.02657, .10261)	(.02210, .08586)	(.01892, .07382)
8	(.04043, .13972)	(.03224, .11251)	(.02681, .09417)	(.02295, .08097)
9	(.04776, .15180)	(.03807, .12228)	(.03165, .10236)	(.02709, .08803)
10	(.05526, .16372)	(.04404, .13192)	(.03661, .11046)	(.03133, .09500)
	200	225	250	275
0	(.00000, .01487)	(.00000, .01323)	(.00000, .01191)	(.00000, .01083)
1	(.00026, .02350)	(.00023, .02091)	(.00021, .01883)	(.00019, .01713)
2	(.00178, .03114)	(.00158, .02772)	(.00142, .02497)	(.00129, .02272)
3	(.00410, .03831)	(.00364, .03410)	(.00328, .03072)	(.00298, .02795)
4	(.00686, .04518)	(.00609, .04022)	(.00548, .03624)	(.00498, .03297)
5	(.00990, .05184)	(.00880, .04615)	(.00791, .04159)	(.00719, .03785)
6	(.01314, .05835)	(.01168, .05195)	(.01050, .04682)	(.00954, .04261)
7	(.01654, .06473)	(.01469, .05764)	(.01321, .05195)	(.01201, .04728)
8	(.02006, .07101)	(.01781, .06324)	(.01602, .05700)	(.01456, .05188)
9	(.02367, .07721)	(.02102, .06876)	(.01891, .06198)	(.01718, .05641)
10	(.02737, .08334)	(.02431, .07422)	(.02186, .06690)	(.01986, .06090)
	300	325	350	375
0	(.00000, .00994)	(.00000, .00918)	(.00000, .00852)	(.00000, .00796)
1	(.00017, .01571)	(.00016, .01451)	(.00015, .01348)	(.00014, .01259)
2	(.00119, .02084)	(.00109, .01924)	(.00102, .01788)	(.00095, .01669)
3	(.00273, .02564)	(.00252, .02368)	(.00234, .02200)	(.00218, .02055)
4	(.00457, .03025)	(.00421, .02794)	(.00391, .02596)	(.00365, .02424)
5	(.00659, .03472)	(.00608, .03207)	(.00565, .02980)	(.00527, .02783)
6	(.00874, .03909)	(.00807, .03611)	(.00749, .03355)	(.00699, .03133)
7	(.01100, .04338)	(.01015, .04007)	(.00942, .03724)	(.00879, .03477)
8	(.01334, .04760)	(.01231, .04398)	(.01142, .04086)	(.01066, .03816)
9	(.01574, .05177)	(.01452, .04783)	(.01348, .04444)	(.01258, .04151)
10	(.01819, .05588)	(.01679, .05163)	(.01558, .04798)	(.01454, .04481)

Number of Defects	Sample Size			
	400	425	450	475
0	(.00000, .00746)	(.00000, .00702)	(.00000, .00664)	(.00000, .00629)
1	(.00013, .01180)	(.00012, .01111)	(.00011, .01050)	(.00011, .00995)
2	(.00089, .01566)	(.00084, .01474)	(.00079, .01392)	(.00075, .01319)
3	(.00205, .01927)	(.00193, .01814)	(.00182, .01714)	(.00172, .01624)
4	(.00342, .02274)	(.00322, .02141)	(.00304, .02022)	(.00288, .01917)
5	(.00494, .02610)	(.00465, .02458)	(.00439, .02322)	(.00416, .02201)
6	(.00655, .02939)	(.00617, .02767)	(.00582, .02615)	(.00551, .02478)
7	(.00824, .03262)	(.00776, .03071)	(.00732, .02902)	(.00694, .02750)
8	(.00999, .03580)	(.00940, .03371)	(.00888, .03185)	(.00841, .03018)
9	(.01179, .03893)	(.01109, .03666)	(.01047, .03464)	(.00992, .03283)
10	(.01362, .04204)	(.01282, .03958)	(.01210, .03740)	(.01147, .03545)
	500			
0	(.00000, .00597)			
1	(.00010, .00945)			
2	(.00071, .01254)			
3	(.00164, .01543)			
4	(.00274, .01821)			
5	(.00395, .02091)			
6	(.00524, .02355)			
7	(.00659, .02613)			
8	(.00799, .02868)			
9	(.00942, .03120)			
10	(.01089, .03369)			

DEVELOPING AND CONDUCTING PERFORMANCE TESTS

The following guidance relating to the development and conduct of performance tests was pulled from the Office of Independent Oversight (now the Office of Security and Cyber Evaluations) document, *Protective Force Inspectors Guide*, October 2009. For a complete version, please contact the Office of Health, Safety and Security Office of Enforcement and Oversight.

Determining Test Objectives

Before serious planning can begin, the objective(s) of the test must be clearly defined and stated. This is necessary whether or not the type of test can meet more than one objective. For example, an entry control performance test could test the adequacy of entry control procedures, or it could test an SPO's ability to properly apply those procedures. Detailed planning must be aimed at satisfying clearly understood objectives. The objective may be to see whether all PF flashlights work, all rifles are properly battlesight zeroed, or whether protective personnel can properly perform certain specific skills or adequately execute specific procedures.

Determining Test Attributes

After determining the test objectives, the planner must select a testing protocol that provides maximum achievable realism, assures adequate safety, and satisfies the test objectives. This determination involves several components:

- How to Test – The type of performance test and specific testing techniques must be determined. Test objective, realism, safety, available resources, and all other applicable variables must be considered in determining an acceptable testing method. The planner has to determine what skill, duty, or function is to be tested, and then devise the best method of testing it. The best way to test is to make the subject actually demonstrate the skill, perform the duty, or operate the equipment under conditions that are as realistic as possible.
- Where to Test – Test location is important and, in some cases, has a significant impact on realism. Generally, the best location is where the event being tested would actually occur. For example, if the test is to determine the tactical skills of the PF in protecting the vital areas of a reactor, the test should be conducted at the reactor. An acceptable alternative might be a similar reactor that is offline or shutdown. A poor alternative would be a non-reactor building or facility that does not resemble a reactor. If testing entry control procedures, the tests should be conducted at actual entry portals, preferably at a representative sample of such portals.
- When to Test – The timing of the test also affects realism. When testing night firing skills, it is best to test at night. When testing day-shift personnel on felony vehicle stop procedures, it is best to test in daylight. When testing entry control procedures, it is best to conduct the bulk of the tests during normal working hours, including shift change, when most entries and exits occur. When testing an event that would normally take place at a crowded facility, the test should take place when the facility is crowded, not after hours when it is deserted except for protection personnel.
- How Many Tests to Conduct – The number of iterations of a particular performance test will depend on the nature of the test and the available resources. Detailed planning requires an early determination of the number of tests to be conducted; this is especially true of complex tests and tests involving large numbers of personnel or use of scarce facilities.

Scenario Development

Once preliminary decisions such as test objectives, location, and time have been made, planning of specific scenario events can begin. The scenario consists of those events that create the situation that will test the subject. The complexity of the scenario is directly related to the complexity of the test. For example, an LSPT might be conducted to determine whether flashlights work. The scenario would be as simple as to switch on the selected flashlights and see if they illuminate.

Scenario development requires the planner to devise and think through a logical series of events that will elicit realistic responses and accomplish the test objective. As scenarios become more complex, particularly those involving adversaries and tactical procedures, there will be a wide range of scenario event options. It is important to judiciously choose among the options to select events that are realistic, within the appropriate threat guidance, and logical (in the sense scenario event flow), and that also serve to fully satisfy the test objective. It is helpful to keep scenario events as simple as possible unless there is a specific requirement to include intricate or complicated events.

For large-scale ESS performance tests, Independent Oversight normally develops the scenarios based on the objectives, which will then be coordinated closely with the site trusted agents to ensure the test objectives can be exercised. The primary trusted agents from both the site and Independent Oversight will give written concurrence agreeing to the scenarios.

Simulation

There is some amount of simulation or artificiality in most performance tests. To preserve realism, it is best to keep simulation at a minimum. Performance tests involving live adversaries usually require the greatest amount of simulation, generally because of safety or test control requirements. The following are some typical simulations encountered in PF performance tests:

- Response Times – To keep PF players within the test area, it is frequently necessary to place players who would normally respond from outside the test area into a holding area and release them into test play according to a predetermined schedule. The best way to determine the release schedule is to conduct a no-notice response test and record the actual response time for each responder.
- Explosives – Typically, inert dummy explosives and related equipment are carried and deployed as actual explosives would be. A controller is required to verify that the explosives are properly set, at which time he/she simulates the effects of the explosives, which may include throwing a grenade simulator, opening a door or gate, and assessing casualties.
- Initial Player Positioning – At times, adversaries are prepositioned in the test area. For example, in containment performance tests, it is usual to place the adversaries inside the target building before the test. If this approach is taken, the PF players must be briefed on the simulated events (through alarm chain, eyewitness observations, etc.) by which the adversaries entered the building. Similarly, PF players are sometimes prepositioned in their response positions or in a holding area for scheduled release. These positions may have been determined based on previous observations of routine posts and patrol activities.
- Personnel and Time Limits – At most sites, over a period of time, more and more protective personnel and local law enforcement would be able to respond to a security incident. For test purposes it may be desirable to limit PF players to a manageable yet realistic number; for example, those personnel in a target area and those who could respond to the area within 15 minutes. Using this strategy, it is reasonable to also limit the running time of the test, so that the PF players do not have to continue long after they would have realistically received more resources.
- Target Material – If SNM or other sensitive devices are involved in scenario play, it is usually simulated using other materials or devices of similar size, weight, and configuration.
- Location – If the actual facility or building cannot be used, the test must be conducted at an alternative location. The layout and attributes of the test facility should be as similar as possible to the actual facility.

- Controller Presence/Actions – The mere presence of controllers is artificial, but necessary. At times, controllers must simulate scenario events, such as alarms, explosive effects, and breaching of barriers, or they may have to intervene to enforce safety rules or rules of engagement. Generally, controllers should intervene in test play only when necessary and otherwise avoid interfering.

Control Measures

Conducting an orderly and safe test requires planning and enforcement of various control measures. Some control measures are restrictive, so it is important to strike a balance between the need for realism and the need to control the test. Without being overly burdensome, sufficient control measures should be planned to ensure that the scenario can be executed properly and realistically, the test can be conducted safely, and the necessary degree of control can be exerted by the exercise coordinator during the entire test. Control measures generally apply to both sides and the desired condition is that the cumulative effect of all control measures be neutral. The following are some typical control measures:

- Boundaries – Establish the limits of the test area. Players are not allowed to leave the test area and armed protective personnel are not allowed to enter the test area except under controlled conditions.
- Off-Limits Areas – At times, certain areas (rooms, buildings, rooftops, and excavations) within the test area boundaries must be placed off limits, usually for safety or operational reasons. Radiation areas, construction areas, and rooms where armed protective personnel are sequestered are typically off limits. These areas are off limits to players on both sides and frequently off limits to controllers and other non-player participants. Locations of off-limits areas must be fully explained, and locked, marked, or otherwise physically identified to all participants. The number of off-limits areas should be kept to a minimum. As agreed to by safety and operational trusted agents, it is sometimes sufficient to caution participants about the hazards in an area rather than place the area off limits.
- Rules of Engagement – This is a set of rules by which players on both sides must abide during tests involving live adversaries. While there is a fairly standard set of rules, they may be amended as conditions require for each test. For more details on specific rules of engagement, see *Protective Force Protocols and Rules of Engagement*, March 12, 2007.
- Safety Rules – This is a set of safety-related rules by which all test participants must abide. There is a fairly comprehensive set of standard safety rules. These rules are normally modified to accommodate the scope and nature of the specific performance test and site-specific safety requirements.
- Controller Actions – Controllers are responsible for enforcing the rules of engagement, conduct, and the safety. They may also have specific preplanned or spontaneous responsibilities, such as opening doors, passing messages to alarm station operators, releasing responders from a holding area, or assessing casualties.
- Communications – In any test where not all participants are at the same restricted location, reliable communication is essential. The exercise coordinator must be able to communicate directly with all evaluators and either directly or indirectly with all controllers and players. Suitable methods of coordinating with the shadow force or summoning an ambulance, if necessary, must be established.
- Test Initiation and Termination – Conditions for starting and stopping the test must be established. Generally, a test is started when all participants are in place and all safety and other requirements are satisfied. Conditions and procedures for temporarily stopping the test must be established and briefed to all participants prior to the start of the exercise. Temporary delays

should be avoided if possible, but are occasionally caused by safety or security incidents or administrative holds to reposition players during an FOF exercise. Conditions for terminating the test are usually based on completion of the test scenario or reaching a predetermined time limit, but may also include the occurrence of a major safety or security event at the site, whether or not it involves test participants.

Logistics

Some logistical planning is necessary for even the simplest performance test; complex tests may require extensive and detailed logistical planning. While the trusted agents are responsible for accomplishing most of the logistical tasks, it is up to the exercise coordinator to ensure all logistical needs have been identified and that trusted agents deliver the required support. The following list includes some typical logistical planning considerations:

- Personnel – The total number and attributes of participants must be determined. This includes the number of PF personnel or other facility personnel and who they will be (that is, which individuals, shift, and SRT). It also includes the number of adversaries that will be needed and any special qualifications they require. The required number of controllers and evaluators must be determined and their sources decided. Each controller and evaluator must be assigned a position and specific test responsibilities. All participants must be notified of their selection and told when and where to report and what to bring with them. It may be necessary to provide a general notification to all personnel working in the vicinity of the test area.
- Facilities – All facilities necessary for test preparation and conduct must be identified and scheduled. These would include the test area, briefing rooms, weapon and equipment issue, recovery areas, and possibly adversary training areas.
- Equipment – All equipment that is to be used in the test must be identified, the source of each item must be identified, and responsibility must be assigned for providing each item. Normal equipment categories are as follows:
    - Props – Various props are needed for testing purposes. A prop could be almost anything, including false or real badges, simulated explosives, rubber knives, replica weapons, briefcases, furniture, or safes.
    - Weapons/Multiple Integrated Laser Engagement System (MILES)/Ammunition – Total numbers and types of weapons, ESS/MILES equipment, and blank ammunition must be determined. PF weapons and ammunition are generally limited to what they actually have available. Adversary weapons and ammunition are limited only by the threat guidance, what can reasonably be made available to them, and what they can transport. Any pyrotechnics to be used by controllers must also be identified.
    - Duty Equipment – The PF is limited to their normal duty equipment. The adversaries are unlimited, within reason and current threat guidance. Controllers will need radios, ESS/MILES controller guns, and perhaps flashlights and other items.
    - Vehicles – Types and numbers of test vehicles that will be used by players or be in the scenario play must be determined. Additionally, any vehicles needed for test control purposes must be identified.
    - Uniforms and Clothing – The PF players usually wear their normal uniforms. Adversary uniforms or clothing will depend on the scenario. Controllers, evaluators, and observers will be issued some form of distinctive apparel, such as a traffic vest, cap, etc. Weather conditions should be taken into account and cold weather or rain gear should be available, if needed.

- Special Equipment – Any special equipment to be used by the PF players should be identified and limited to such equipment as they normally have available to them. Special adversary equipment needs must generally be identified early, so that equipment can be located and obtained before it is needed.

- Transportation – As necessary, arrangements must be made to transport all test participants to briefing areas, the test area, and the site of their specific assignment. Return transportation needs must also be identified and provided.
- Food/Drink – If the test involves outdoor activity in extreme weather conditions, either hot or cold, plans should be made to provide hot or cold drinks at appropriate places and times. Depending on the time and duration of the test, it may be appropriate to provide box meals to all test participants.

Safety

Safety must be considered during all planning activities. Safety considerations will vary with the type of test activity, but may include general personal safety, weapons safety, vehicle safety, aircraft safety, and availability of medical, fire, and ambulance services.

Every inspection-related performance test that has any safety implications, including most PF performance tests, requires review by Independent Oversight and approval by DOE field element and/or site safety representatives. The safety representatives should be involved early and throughout the planning process so that potential safety problems can be solved without causing delay or cancellation of the test.

Standard safety plans and risk assessments exist for various types of performance tests, but the standard plans are frequently modified to accommodate the particular test and the site-specific conditions and requirements. Safety plans are developed by the site in accordance with local procedures.

Security

During any performance testing of PF personnel or equipment, the security of the site must be considered. When personnel or equipment are taken off post or out of service for testing, or when personnel on post are carrying ESS/MILES weapons instead of live weapons, compensatory measures are frequently needed to provide for the minimum security needs of the facility. Any test, even a simple one involving only one or two SPOs on post, may require compensatory measures if the test has the potential to divert the attention of on-duty personnel from their normal responsibilities.

For most performance testing, test subjects are either brought in from off duty for testing, or they are relieved from their posts during the testing period; in these situations, other on-duty personnel provide the needed security. For some tests, such as no-notice tests at entry control portals, any needed compensatory measures would have to be more subtle, to avoid compromising the test element of surprise. For larger-scale tactical tests where all normal security posts in the test area are manned by players equipped with ESS/MILES weapons, the common compensatory measure is to place armed shadow force personnel in strategic locations in or adjacent to the test area. Shadow force locations must be off-limits areas and all shadow force personnel must be under the positive control of a controller at all times.

The need for compensatory measures should be determined by the local operations office. Whether they are employed is a decision to be made by the trusted agent or his/her superiors. However, the test director/exercise coordinator does have an obligation to raise the question if he/she believes compensatory measures may be required. If compensatory measures are required, the test director/exercise coordinator has a definite interest in what they are and should be involved in their planning. As with any other planning consideration, the goal for these measures is to affect test realism and safety as little as possible. In this case, however, the final decision rests with the site, and the test director/exercise coordinator must rely on persuasion, if necessary, to influence a reasonable solution.

PERFORMANCE TEST SAFETY PLAN

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

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

Printed 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 LSPT'S HAS BEEN GRANTED BY A RESPONSIBLE 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 contraband and prohibited items from being introduced into LAs, exclusion areas, protected area (PAs), and MAAs. 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 cognizant security authority (CSA). Once the entry is initiated, the person attempting the entry will only proceed after being cleared to do so by the security officer (SO) 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 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 controller and obey all instructions given by PF personnel. The 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. 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

____ 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

____ 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

____ 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.

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

List other specific safety measures below:

1. All personnel attempting to gain entrance into one of the identified areas will be briefed on the LSPT objectives and how they should conduct themselves during the LSPT.
2. All contraband or prohibited items will be photographed prior to the initiation of the LSPT.
3. All personnel attempting to gain entry or exit with contraband items will be photographed prior to 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, CSA-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:

____ Applicable

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

____ Not applicable

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

Off-Limit Areas:

____ Applicable

____ 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 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 controllers and the person carrying the contraband or prohibited items will be filled in prior to conducting the LSPT.

PF Appendix Required:

____ Yes

____ No

DOE Safety Review:

List any pertinent safety procedures concerning this LSPT that are not addressed in this plan. Normally, the PF will not be notified in advance of the specifics of the LSPT being conducted. The shift captain will be notified upon termination of the LSPT.

APPROVALS:

____ Date _________________
Director, Cognizant Security Authority

____ Date _________________
Safety and Health Representative

SAMPLE PERFORMANCE TEST PLAN

Objective: This performance test is designed to

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

Scenario: A simulated SRD document will be left unattended in an area accessed by employees with L-level clearances. 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.

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 xxx. The document shall be placed in the designated location at approximately 7:30 am.
2. Upon notification of the unattended "classified" document, the CDCO will verify that the individual finding the document completed the following actions (answers will be based on applicable procedures):
   a) xxx
   b) xxx
   c) xxx
3. The Document Control Center shall also verify that PF completed the following actions (answers will be based on applicable procedures):
   a) xxx
   b) xxx
   c) xxx
4. In order to successfully complete the performance test, the following must occur:
   a) Classified Document Control Office is notified within three hours of placement.
   b) Individual locating the unattended document adheres to all protection and notification requirements.
   c) PF officer responding to the incident adheres to all protection and notification requirements.

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

- Only self-assessment 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 organization being assessed 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 indication to a casual observer that the document is not classified.

Resource Requirements: The following resources are needed to conduct this performance test.

- Simulated SRD document
- Identified location to place the document
- Three self-assessment team members to be assigned the following:

  a) Monitor the document
  b) Monitor the PF response
  c) Monitor the CDCO

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

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

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

Coordination and Approval Process: The following steps and documentation will be followed in the conduct of this exercise.

- This test plan will be approved by the self-assessment team lead prior to conduct of the performance test. Approval of this test plan will be documented by the team lead'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 assessment team members participating in the evaluation of this performance test.

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

- DOE O 471.6, Information Security Program
- Information Security Standard Operating Procedure #
- PF Standard Operating Procedure #

Team Lead: ______________________________ Date: _____________________________

NO-NOTICE PERFORMANCE TEST: BEST PRACTICE

Date: August 5, 2013

Site: Nevada Field Office (WSI Nevada)

SECLL Title: No-notice Performance Tests **SECLL Identifier:** SEC-WSI-NV-08-05-2013

Document Type: Best Practice

Lessons Learned Statement: Prior to developing any no-notice performance test, we met with our PF leadership, safety, VA lab, and performance testing. As a group, we discussed what objectives each wanted from the performance test. We agreed that the primary objective was to validate PF abilities to identify and locate an unauthorized individual(s) within a specific area of operation, with a secondary objective of validating the PF ability to respond to a low level threat (protester). Safety was the primary concern associated with this type of performance test. The group evaluated various pathways and determined the areas that present significant safety concerns. Each concern was addressed and mitigated with specific hazard controls.

Discussion: Performance test plans were developed with emphasis on pre-operations and actual conduct of the performance test. Each phase is described below.

A. Pre-conduct operations

1. Test administrator will meet with the site tactical commander prior to him/her assuming their shift, advise him/her of their trusted agent responsibilities, and brief him/her on the test time and guidelines of the performance test (recorded on briefing checklist).
2. Test participant(s) will carry nothing other than a cell phone while performing this performance test.
3. Test participant(s) will wear normal site attire; under no circumstance will he/she/they wear clothing that can be misconstrued as that worn by an adversary (e.g. dark or camouflaged).
4. The site tactical commander will confirm with the test administrator that he/she is in the CAS prior to arriving at the performance test start point.

B. Conduct

1. The site tactical commander will confirm with the test administrator (or designee) that he/she is in the CAS and ready to conduct the performance test.
2. Test participant(s) will enter the area of operation from a predetermined location.
3. Test participant(s) will proceed directly to the exterior Perimeter Intrusion Detection and Assessment System (PIDAS) fence.
4. At no time will the test participant(s) walk in the direction of or approach a tactical response team unit.
5. If the test participant(s) are challenged and an escalation of security phase is initiated, the statement will be announced over the PF radio net, ESS radio net, and facility public address system: ***"This a PF no-notice performance test. Only PF personnel are involved in the test. All others will continue with normal operations."***
6. If the test participant(s) reaches the exterior PIDAS fence unchallenged, he/she/they will continue to make noise and attempt to draw attention to their location.
7. If the test participant(s) remain unchallenged, he/she/they will enter the PIDAS, ensuring the gate is locked behind them and proceed directly to the interior PIDAS fence. Once at the interior PIDAS fence, he/she/they will tug on the taut wire with no more force than to set the alarm off.
8. The test participant(s) will back away from the interior PIDAS fence, ensuring his/her/their hands are clearly visible.

9. The test participant(s) will remain away from the interior PIDAS fence; at no time will any threatening gestures be made towards the PF.
10. **If the test participants are detected prior to reaching the PIDAS but are not located by the PF, the test participants will standup and don their reflective safety vest if a PF vehicle comes within 25 yards (75 feet) of their position.**
11. The test participant(s) will comply with all directions/orders given by the PF.
12. The site tactical commander will maintain control of the performance test and terminate it if at any time he/she feels it necessary. Termination of the performance will occur if a real-world security phase is initiated for other reasons.
13. The site tactical commander is the only individual authorized to terminate the performance test. The test participant(s) will carry a "Trusted Agent" identification card identifying him/her/them as a participant in a performance test.

Analysis: The first thing we discover is there is no way to conduct a complete no-notice performance test. There must be someone in the PF chain of command that can control the performance test and stop it should things get out of hand. We selected the site tactical commander to be that individual. Our first attempt at no-notice performance testing was somewhat disconcerting; however, you have to trust in the training that our SPOs receive. Most of our no-notice performance tests are directly tied to the low-level threat; however, we have expanded our no-notice performance testing program to included explosive detection and active shooter scenarios

Recommended Actions: None

Priority Descriptor: Routine

Topical Area: Program Management Operations

Sub Topical Area: PAP

Estimated Savings: N/A

Keywords: No-notice Performance Testing

Reviewing Official: WSI Nevada

Derivative Classifier: WSI Nevada

3.0 TOPICAL AREA TOOLS

IN THIS SECTION:

Tab 3

3.1 PROGRAM MANAGEMENT AND OPERATIONS

THIS SECTION WILL INCLUDE:

- Subtopical Areas
- Common Deficiencies

Subtopical areas will address:

- Current Directives
- Potential Documents for Review
- Potential Interview Candidates
- Lines of Inquiry
- Performance Tests

Tab 3.1

SUBTOPICAL AREAS

Protection Program Management

- Program Management and Administration
- Resources and Budgeting
- Personnel Development and Training

S&S Planning and Procedures

Management Control

- Surveys and Self-Assessment Programs
- PAP
- Resolution of Findings
- Incident Reporting and Management

Program-Wide Support

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

COMMON DEFICIENCIES

The following is a sample of common deficiencies identified by the Office of Independent Oversight (now the Office of Security and Cyber Evaluations) in the 2009 document, *Protection Program Management Inspectors Guide*. By reviewing the list of common deficiencies during the planning phase, assessors can be alert for similar deficiencies during data gathering activities.

- Lack of expertise to review plans
- Lack of planning and analysis expertise
- Lack of procedures for updating plans
- Lack of procedures for integrating plans
- Failure to integrate resource requirements
- Procedures inconsistent with plans
- Vague or ineffective survey or self-assessment guidance and plans
- Ineffectively implemented survey or self-assessment programs
- Inadequate self-assessments
- Inadequate CAPs
- Reactive organizational oversight

SUBTOPICAL AREA: PROGRAM MANAGEMENT AND SUPPORT

Sub-elements include:

- Program Management and Administration
- Resources and Budgeting
- Personnel Development and Training

CURRENT DIRECTIVES AND REFERENCES

The following references apply to Program Management and Support:

- DOE O 331.1C, *Employee Performance Management and Recognition Program*
- DOE O 360.1C, *Federal Employee Training*
- DOE O 226.1B, *Implementation of Department of Energy Oversight Policy*
- DOE O 470.4B, *Safeguards and Security Program*
- DOE P 470.1A, *Safeguards and Security Program*
- DOE-STD-1171-2009, *Safeguards and Security Functional Area Qualification Standard*
- DOE-STD-1123-2009, *Safeguards and Security General Technical Base Qualification Standard*

SAMPLE DOCUMENT LIST

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

- Organization diagrams depicting the management structure
- Documents depicting assigned roles, responsibilities, and authorities of S&S management
- Descriptions for S&S management positions
- Operating instructions for the implementation of S&S programs
- Supplemental directives implementing S&S programs
- Training records for personnel with S&S responsibilities
- Contract documentation (directives applicable to the organization being assessed)
- Budget documentation
- Training plans and procedures
- Overall training process and training record system (is there one program)
- Certification records for specialized jobs
- Copy of active deviations
- Last two years survey and self-assessment reports

The existence of other documents, which further delineate management of the S&S program, may be derived from review of these initial documents. Documents should be used as the basis for determining whether management supports the S&S program in a manner that demonstrates both compliance with the requirements and a commitment to performance that assures the adequate protection of national security assets.

SAMPLE INTERVIEW CANDIDATES

Interview candidates may include:

- S&S director/manager

- Individual S&S program managers
- Management assigned responsibility for developing and implementing this element of the S&S program
- Contracts and procurement management
- Budget/finance management
- Human resources management
- Security management assigned responsibility for developing and implementing the S&S programs
- Property management
- Training management
- Individuals responsible for S&S training activities (including PF)

SAMPLE LINES OF INQUIRY

Suggested lines of inquiry can be used to (1) assist in determining the scope of assessment activities, (2) assist in developing document call lists, and (3) guide the interview process. Lines of inquiry may include:

PROGRAM MANAGEMENT AND ADMINISTRATION

1. Who has overall responsibility for the S&S program? Review organizational chart, describe the management structure, where the security functions are located within the facility/company.
   - Has management established an effective and efficient organization structure?
   - Is the organization structure documented in writing?
   - Are lines of communication, accountability, and authority clear?
   - Have responsibilities been explicitly assigned to individuals?
   - Are reporting requirements for IOSC assigned?
   - Are there indications of frequent change in the organizational structure?
   - Have S&S programs been developed and maintained that incorporate the responsibilities and requirements contained in DOE O 470.4B?
   - Where are the following items documented?
     - Roles
     - Responsibilities
     - Delegations
     - Authorities
     - Planning and budget, including personnel resources
     - Program mission

2. What is the process used for reviewing, approving, and/or updating major S&S plans?
   - Is the SSP current and been approved? If so, when?
   - Is the approval chain for S&S plans, procedures, and implementation policy documented?
   - Are there supplemental plans (standard operating procedures [SOPs]) for implementing the S&S program?
     - Are the supplemental plans current and approved? If so, when?

3. Are there any current deviations/exemptions on file in SSIMS?
   - Are the deviations/equivalencies/exemptions supported by the GSP and a VA, or by a sufficient analysis to form the basis for an informed risk management decision?

Resources and Budgeting

1. 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?

2. Have S&S budgets been developed and allocated for assigned programs including budgets for the infrastructure that supports S&S missions?
   - How are future S&S resources and program budgets formulated?
   - How is the allocation of resources executed?
   - How are near-term and long-term resource requirements, needed to ensure the integrity of existing and planned S&S upgrades, incorporated into the budget process?

3. Is there adequate funding allocated to this S&S program?
   - Who is involved in the coordination of adopting new programs involving security?
   - Are new strategies, technologies, or systems being considered/evaluated in regard to overall effectiveness and economics of the program, including costs of implementation, impacts to operations, and need for modifications and/or construction?
   - Where are proposed capital equipment procurements and funding requirements that are not part of a line-item-construction project, general plant project, or support S&S programs and operations identified?
   - Do funding requirements for proposed capital equipment procurements include:
     - Alarm and assessment system components?
     - MC&A systems?
     - Access control system components?
     - Equipment necessary to complete the S&S mission?

Personnel Development and Training

1. Is there a formal training program in place?
   - Has funding been allocated for training?
   - Who maintains the organizations training records?
   - Is succession planning considered when training staff?
   - Are procedures applicable to S&S training documented in facility security plans or SSPs?
   - Does the S&S training program for each facility encompass all program elements performed by employees working at that location?
   - Are training courses produced using a systematic approach that includes at least analysis, design, development, implementation, and evaluation phases?
   - If training that meets analysis requirements is provided by external resources, such as commercial vendors or other government training agencies, are the training products procured from these resources evaluated at the site level for consistency with DOE policy and site needs?
   - Is an evaluation of training performed to ensure that instructional objectives are met and to determine overall effectiveness?
   - Are training plans that project training derived from a valid needs analysis for the forthcoming year developed annually?

2. Is the content of training (initial, refresher, and on the job) consistent with the knowledge and skills required to perform assigned S&S tasks and/or responsibilities as determined by valid and complete JAs?

   - Has there been an analysis of the job skills needed to fulfill each assigned responsibility? Has this been documented in individual job descriptions?
   - Are personnel adequately trained to perform their assigned duties?
   - Are knowledge- and/or performance-based testing used to measure the knowledge and/or skills acquired from training programs?
   - Are accurate and complete employee training records that contain dates of course attendance, course title, and scores/grades achieved (where applicable) maintained in accordance with DOE Administrative Records Schedule 1, Personnel Records?
   - In accordance with the National Industrial Security Program Operating Manual (NISPOM), have facility or site SOs completed training appropriate to their position and the security operations conducted at their assigned facilities? Note: *This training should be completed within one year of appointment to the position of facility security officer (FSO).*

SAFEGUARDS AND SECURITY PLANNING AND PROCEDURES

SUBTOPICAL AREA: S&S PLANNING AND PROCEDURES

Sub-elements include:

- None

CURRENT DIRECTIVES AND REFERENCES

The following references apply to S&S Planning and Procedures:

- Department of Defense (DOD) 5220.22-M, *National Industrial Security Program Operating Manual*
- DOE O 470.4B, *Safeguards and Security Program*
- DOE O 470.3B, *Graded Security Protection Policy*
- DOE O 150.1, *Continuity Programs*
- DOE P 470.1A, *Safeguards and Security Program*
- DOE-STD-1192-2010, *Vulnerability Assessment Standard*
- Executive Order (EO) 12977, *Interagency Security Committee*
- Homeland Security Presidential Directive (HSPD)-3, *Homeland Security Advisory System*
- HSPD-7, *Critical Infrastructure Identification, Prioritization, and Protection*
- Presidential Decision Directive (PDD) 39, *U.S. Policy on Counterterrorism*

SAMPLE DOCUMENT LIST

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

- SSP
- VAs/performance tests
- Approved or pending deviations
- SSIMS reports
- Emergency plans
- Contingency plans
- MC&A plans
- S&S training plan
- Survey, self-assessment, and inspection reports
- Data from evidence files
- Current compensatory measures

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

SAMPLE INTERVIEW CANDIDATES

Interview candidates may include:

- S&S director
- Individual S&S program manager(s) responsible for S&S-related activities and plans
- Senior management with line responsibility for S&S activities and plans

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

SAMPLE LINES OF INQUIRY

Suggested lines of inquiry can be used to (1) assist in determining the scope of assessment activities, (2) assist in developing document call lists, and (3) guide the interview process. Lines of inquiry may include:

S&S PLANNING AND PROCEDURES

1. Is there a formal, coordinated effort regarding the development, approval, and updates associated with S&S plans?
   - How is integration of major S&S plans ensured?
   - Is the Design Basis Threat (DBT) used for addressing threats? If not, is this approved in writing?
   - Is there a local procedure for developing the SSP?
   - 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?
   - Does the security plan reflect actual operating conditions at the covered location?
   - Does the security plan include a listing and prioritization of the assets and security interests at the facility or site, a description of how the protection program is managed, and a description of how national and DOE S&S requirements are met, including any deviations from requirements?
   - Does the security plan include implementation plans for meeting changes in national or DOE policies or other changes (such as the addition or removal of security interests) that may require an extended timeframe to implement because of financial or other resource considerations, including an implementation schedule and planned contingency measures in case the requirements cannot be met as scheduled?
   - Are any S&S plans currently being updated? If so, why?
   - Are the various protection systems adequately integrated?
   - What deviations are in place? When were they approved and by whom?
   - How do deviations impact protection strategy?
   - Are updates to security plans made when any of the following conditions apply:
     - Changes in baseline security requirements in national-level or DOE policy?
     - Changes in facility operators/contractors?
     - Changes in assets or security interests?
     - Changes in facilities included in an SSP?
     - Changes in the security posture of a facility or site?
     - Planned changes to the security program at the facility or site?
     - Changes in operations at a facility or site that require modifications to approved security measures?
   - Have the specific measures been identified that will most efficiently and effectively implement the required increases in readiness at each SECON level?
   - Does the response plan describe the specific actions to be taken for each SECON level and are SECON response plans part of the SSP?
   - Are implementation activities and schedules for performance assurance plans included in the SSP?

2. Have SSPs been developed and implemented for all facilities not requiring an SSP?
   - What is the protection strategy used at this facility?
   - Do key S&S plans match procedures actually used at a facility?
   - How does the facility comply with the contents of the SSP?

3. Who is responsible for maintaining SSP/VA data?
   - Are VA documents and validation results from performance tests reviewed during the update process or are data obtained from new sources?

4. How has management effectively established program direction?
   - How are changes in policy and/or procedures communicated to those with implementing responsibilities? How are these versions maintained?
   - How are evaluation results used by management to evaluate the effectiveness and viability of S&S plans?

MANAGEMENT CONTROL

SUBTOPICAL AREAS: MANAGEMENT CONTROL

Sub-elements include:

- Survey and Self-Assessment Programs
- PAP
- Resolution of Findings
- Incident Reporting and Management

CURRENT DIRECTIVES AND REFERENCES

The following references apply to Management Control:

- 10 CFR Part 1016, *Safeguarding of Restricted Data*
- 10 CFR Part 1045, *Nuclear Classification and Declassification*
- 10 CFR Part 824, *Procedural Rules for the Assessment of Civil Penalties for Classified Information Security Violations*
- 32 CFR Part 2001, *Classified National Security Information*
- 32 CFR Part 2001.48, *Reporting Loss of Classified Information*
- DOD 5220.22-M, *National Industrial Security Program Operating Manual*
- DOD Defense Security Service Industrial Security Letters
- DOE O 221.1A, *Reporting Fraud, Waste, and Abuse to the Office of Inspector General*
- DOE O 232.2, *Occurrence Reporting and Processing of Operations Information*
- DOE O 470.4B, *Safeguards and Security Program*
- DOE O 475.1, *Counterintelligence Program*
- DOE P 470.1A, *Safeguards and Security Program*
- EO 12829, *National Industrial Security Program*
- EO 13526, *Classified National Security Information*
- National Security Decision (NSD) 84, *Safeguarding National Security Information*
- 18 United States Code (USC) Section 923 (g)(6), *Licensing*
- 42 USC Sections 2271 to 2181, *Enforcement of Chapter*
- 42 USC Section 2282b (Section 234B, as amended)
- 42 USC Section 5801, 5877 and 307, *Energy Reorganization Act of 1974*
- 50 USC Section 402a, *Coordination of Counterintelligence Activities*
- 50 USC Section 2656, *Notice to congressional committees of certain security and counterintelligence failures within nuclear energy defense programs*

SAMPLE DOCUMENT LIST

Documentation to be reviewed may include the following:

- Self-assessment program plans (and schedules)
- IOSC implementing procedures
- Survey and self-assessment reports
- CAPs and tracking systems (information derived from)
- Site-specific self-assessment guide 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 and closed finding for past three to five years (review for recurring findings)
- Copy of the current and approved PAP plan
- List of essential elements documented in the PAP and testing schedule for each
- Performance assurance test procedures
- Performance assurance test reports and subsequent correction actions

SAMPLE INTERVIEW CANDIDATES

Interview candidates may include:

- S&S director(s)
- Individual S&S program managers
- Personnel responsible for VA testing and SSP development
- PF personnel
- IOSC inquiry officials

SAMPLE LINES OF INQUIRY

Suggested lines of inquiry can be used to (1) assist in determining the scope of assessment activities, (2) assist in developing document call lists, and (3) guide the interview process. Lines of inquiry may include:

Surveys and Self-Assessment Programs

1. Are self-assessment programs in place to determine the effectiveness of the S&S program? Are the programs documented?
   - Do self-assessment team members possess qualifications, experience, and training sufficient to review and inspect the topical/subtopical areas being assessed?
   - Are the self-assessment procedures approved by the appropriate CSA?
   - Are self-assessments planned, scheduled, and conducted in an integrated manner? If topical and subtopical area evaluations are performed separately, are results documented and integrated into a single (periodic) report that includes a composite rating?
   - When was the last self-assessment conducted? Did it include all applicable topical and subtopical elements?
   - What ratings were given?
   - Are ratings based on the effectiveness and adequacy of the program and do they reflect a balance of performance and compliance results as well as the impact of the deficiency(ies) and mitigating factors?

2. Are repeat topical area marginal ratings for consecutive survey or assessment periods assigned an unsatisfactory rating unless one of the following conditions applies:
   - The current assessment of the topical area results in a satisfactory rating?
   - The previous assessment that resulted in a marginal rating identified different deficiencies and reasons for the rating?

- The deficiencies and reasons that were the basis of the previous marginal rating were related to the completion of a line item construction project or upgrade program? In that case, acceptable interim measures must have been implemented, physically validated pending completion of the project and documented in the assessment report.

3. Are the results of surveys and self-assessments validated by document reviews, performance testing, interviews, analyses, and observations?

4. Are surveys and self-assessment reports distributed to the applicable senior managers and other personnel responsible for corrective actions and other personnel, as deemed appropriate?

    - How does the S&S survey or self-assessment provide assurance that departmental assets are being protected at appropriate levels?
    - Are findings that may have programmatic impact on vulnerability to national security, classified information or matter, nuclear materials, or departmental property immediately reported to the departmental element and contractor line management?

5. Have recent survey or self-assessment activities resulted in repeat findings?

6. Are self-assessments performed between the periodic surveys conducted by the DOE CSA?

7. Do self-assessments include all applicable facility S&S program elements and provide an integrated evaluation of all topical and subtopical areas to determine the overall status of the S&S program?

    - Is any decision not to use all subtopical areas documented in a local procedure?
    - Are the results of surveys and self-assessments factored into performance measures or award fees?

8. Do the survey and self-assessment programs provide compliance and performance-based documentation of the evaluation of the S&S program?

PERFORMANCE ASSURANCE PROGRAM

1. Is there a formal process for implementing a PAP?

    - How often is testing conducted?
    - Who reviews and approves the PAP plan?
    - Who determines what tests will be conducted and the criteria for evaluation? What is the basis for this determination?
    - Have all facilities with assets requiring a facility security clearance conducted performance assurance activities? Have these activities been tailored to the assets at the location and the elements that compose the total system in place at the location?
    - Has each test been documented in a test report that includes a narrative description of testing activities and an analysis of test results?
    - Are issues requiring corrective action documented and tracked until resolved?
    - When unsatisfactory results of a test indicate that national security and/or health and safety of facility/site employees or the public is jeopardized, are immediate compensatory measures taken until the issue is resolved and normal reporting procedures followed?
    - Is there a process that the facility or site must implement compensatory measures when an essential element is under repair or in an inoperative or ineffective state that ensures the protection of assets is maintained?

2. Are performance assurance plans reviewed and updated when essential elements are affected due to:
   - Changes in facility/site mission, programmatic activities, or S&S interests and/or assets?
   - Changes in the operation or physical configuration of a facility or site, such as a building addition; new work processes or systems; construction of fences, roads, buildings, etc.; demolition of buildings; or reconfigurations of fences, roads, etc.?
   - Completion of S&S upgrades or downgrades?
   - Changes in protection strategy, risk or vulnerability analysis, PF deployment, or other significant revisions to the applicable security plan?
   - Changes in S&S policies, including DOE O 470.3B, *Graded Security Protection Policy*?

3. Does performance testing include, at a minimum, the following:
   - Operability tests to confirm that a system element or total system is operating as expected?
   - Effectiveness tests to provide assurance that essential elements of the system are working as expected, separately or in coordination, to meet protection program objectives?

4. Have the following occurred at facilities/sites with Category I SNM; with identified credible radiological, biological, or chemical sabotage targets; or that have been identified as critical national security facilities/assets:
   - Within the last 12 months has a comprehensive facility or site threat scenario test been performed to demonstrate overall facility/site S&S system effectiveness?
   - Are the comprehensive threat scenarios consistent with DOE 0 470.3B, *Graded Security Protection Policy?*
   - For facilities/sites with denial protection strategies, are PF exercises performed quarterly with a rotational schedule for multiple facilities requiring denial protection strategies?

Resolution of Findings

1. Is there a corrective action tracking system in place? If so, does it cover the entire site/facility?
   - Are CAPs developed for all open survey and self-assessment findings?
   - Do CAPs explain how deficiencies will be addressed and include detailed milestones?
   - How are CAPs coordinated with management?
   - Are CAPs for surveys and self-assessments submitted within 30 working days of the date of the exit briefing?
   - Are the milestones for completing the corrective actions reviewed on a recurring basis?
   - Are quarterly reports of the status of corrective actions for each finding provided to the appropriate CSA?
   - Are the milestones for completing the corrective actions reviewed on a recurring basis?
   - Are milestone due dates being met?
   - What is the status of open findings? What is the status of the associated CAPs?
   - Is there a documented process in place that ensures all open S&S findings are reviewed during evaluations to validate the status of corrective actions and evaluate impact on the current operation of the facility's S&S program?

2. Is there a documented process in place to ensure the findings from periodic surveys, self-assessments, TSCM services, and DOE reviews are documented, monitored, and resolved in a timely manner?

3. Does the tracking system for findings include all periodic surveys, self-assessments, TSCM services, and DOE review findings?
   - Are all findings closed during the period reviewed for sustainability of the closing action?

- How is the effectiveness of corrective actions validated to prevent recurrence of the issues?
- Is there a process to ensure findings from all surveys are documented in an associated report and results of surveys reported in SSIMS?
- Are corrective actions and their current statuses reported in SSIMS until the associated finding is closed?

4. Is trending used in the resolution of findings to determine if systemic factors and systematic causal factors exist within the S&S program?

    - Have trending assessment activities based on findings been conducted to establish if findings represent an isolated issue or a systemic problem with a specific topical element or with the S&S program as a whole?
    - Are negative trends analyzed to ensure corrective actions address root causes and the need for continuous improvement?
    - What method of root cause analysis is used? What training has staff received? Who provides the training?

Incident Reporting and Management

1. Have any incidents of S&S concern occurred since the last survey/assessment? If so, how many?

    - Was a preliminary inquiry conducted, the initial categorization made, and the initial notifications made within five calendar days of when a potential incident was brought to the attention of management?
    - Do the IOSC procedures require that if there is still uncertainty at the five calendar day mark, with respect to incident categorization, the incident must be reported as a Category A pending completion of the inquiry process?
    - Are Category A incidents reported in SSIMS as required? Does the site have a local tracking system for Category B incidents or are they reported in SSIMS also?
    - Is each security incident assigned a unique local site tracking number?
    - Was the incident reported as soon as it was categorized?
    - Are any inquiries currently open?
    - Do IOSCs involving activities associated with sensitive programs follow the same initial reporting process (but may omit details because of programmatic controls)?
        - Is the subsequent reporting handled within the programmatic channels until the inquiry report has been closed within the sensitive program?
    - When individual responsibility cannot be established and the facts show that a responsible official allowed conditions to exist that led to an IOSC, is responsibility assigned to that official?
    - Have any inquiries established possible crimes or fraud, waste, and abuse?
    - If damage assessments were conducted, who appointed the damage assessment teams and approved the damage assessment reports?
    - Of those incidents, how many were known compromises and how many were potential compromises?
    - Upon closure, is the outcome of inquiries (regardless of category) for all security incidents involving individuals applying for or holding a DOE security clearance reported to the personnel security office with cognizance over the individual’s access eligibility?
    - Are Category A incidents closed via SSIMS?
    - Are Category B incidents closed using SSIMS or a locally approved system identified in the site IOSC program plan?
    - Does the incident notification and inquiry report contain supporting documentation of factors used to determine that the likelihood of compromise and/or potential for damage to national security is remote (e.g., failure to secure a document in a security container)?

- Is all supporting documentation retained with the final report?
- What kind of trending and analysis is performed on IOSCs? How are the results disseminated to management and staff?

2. Are all IOSCs categorized by significance level and type?

   - Are the DOE/NNSA cognizant security officer (CSO) and the contractor CSO notified of Category A incidents that meet a designated level of significance relative to the potential impact on the department and/or national security?
   - Are incidents constituting or determined to be a Category A Management Interest specified in the IOSC program plan?
   - Are incidents constituting or determined to be a Category B Management Interest specified in the IOSC program plan?
   - Are Category B incidents, which do not meet the Category A criteria, managed and resolved by the contractor CSO?
   - Is each IOSC, with the exception of incidents of Management Interest, categorized, have an initial report, an inquiry, and a closure report submitted?
   - Is information generated as part of this process protected according to its sensitivity and/or classification determination?

3. Does the facility maintain a central record of all inquiries into incidents of S&S concern and damage assessments? If not, in what manner are those records being maintained that facilitates their retrieval and use within the facility (e.g., for tracking and oversight purposes)?

   - How long are records maintained?
   - Are infraction reports maintained in individual personnel security files?
   - Is the inquiry process established in the site IOSC program plan?
   - Are the report content and closing procedures documented in the site IOSC program plan?
   - What training does staff receive prior to conducting inquiries?
   - What kind of IOSC awareness is provided?

4. Have staff members conducted inquiries into IOSC? Were these individuals appointed in writing?

   - Whenever possible, is the responsibility for an IOSC assigned to an individual rather than to a position or office?
   - Are inquiry officials appointed by the designated federal entity(ies)?
   - Do appointed inquiry officials have previous investigative experience or departmental inquiry official training?
   - Are inquiry officials knowledgeable of appropriate laws, E.O.s, departmental directives, and/or regulatory requirements?
   - Does the contractor CSO stop further inquiry actions and notify the designated federal designee(s) if an inquiry official determines or suspects that a foreign power or an agent of a foreign power is involved?
     - In such instances, does the inquiry official document the known circumstances surrounding the IOSC and submit all accumulated data to the federal designee(s)?
   - Do inquiry officials responsible for conducting the inquiry maintain all associated documentation including the following specific actions:
     - Collect all information and physical evidence associated with the security incident?
     - Control the physical evidence collected and maintain a chain of custody?
     - Identify associated persons and conduct interviews to obtain additional information regarding the incident?

- Reconstruct the security incident to the greatest extent possible using collected information and evidence.
- Include a chronological sequence of events in the reconstruction that describes the actions preceding and following the incident?
- Identify any collateral effect to other programs or security interests?
- Analyze and evaluate which systems/functions performed correctly or failed to perform as designed to provide the basis for determining the cause of the incident and subsequent corrective actions?

PROGRAM-WIDE SUPPORT

SUBTOPICAL AREAS: PROGRAM-WIDE SUPPORT

Sub-elements include:

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

CURRENT DIRECTIVES AND REFERENCES

The following references apply to Program-Wide Support:

- 10 CFR, Part 1016, *Safeguarding Restricted Data*
- 10 CFR Par 1045, *Nuclear Classification and Declassification*
- 32 CFR Part 2001, *Classified National Security Information*
- 32 CFR Part 2004, *National Industrial Security Program Directive No. 1*
- 48 CFR Chapter 9, *Department of Energy Acquisition Regulation* (DEAR)
  - DEAR Subpart 904.70, *Foreign Ownership, Control, or Influence over Contractors*
  - DEAR 952.204-2, *Security* [Security Clause]
  - DEAR 952.204-70, *Classification* [Classification Clause]
  - DEAR 952.204-73, *Foreign Ownership, Control, or Influence Over Contractor* (Representation)
  - DEAR 952.204.74, *Foreign Ownership, Control, or Influence Over Contractor* [FOCI Clause]
- DOD 5220.22, *National Industrial Security Program Operating Manual*
- DOE O 142.3A, *Unclassified Foreign Visits and Assignments Program*
- DOE O 231.1B, *Environment, Safety and Health Reporting*
- DOE O 470.4B, *Safeguards and Security Program*
- DOE O 475.2A, *Identifying Classified Information*
- DOE O 481.1C, *Work for Others (Non-Department of Energy Funded Work)*
- EO 10865, *Safeguarding Classified Information within Industry*
- EO 12829, *National Industrial Security Program*
- EO 12968, *Classified National Security Information*
- EO 13549, *Classified National Security Information Program for State, Local, Tribal, and Private Sector Entities*
- 10 USC Section 2536, *Award of Certain Contracts to Entities Controlled by a Foreign Government*
- 42 USC 2011-2296, et seq., *Atomic Energy Act of 1954*

SAMPLE DOCUMENT LIST

Documentation to be reviewed may include the following:

- Current contract 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 assessed (list of all contractors/subcontractors registered)
- Approved SSP

- Facility data sheets
- Copy of current award fee criteria and documentation (including performance measurement data) for the last two years
- Most recent FOCI determination(s)
- Approved CSCS from DOE F 470.1
- Signed FDAR from DOE F 470.2
- Deviations (pending and approved)
- Master facility registration, in SSIMS, 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. CPCI and contractor lists, including the list of current KMP, should be compared for discrepancies.
- Internal procedures (facility clearance, FOCI)
- Applicable MOUs or MOAs
- Completed FOCI questionnaire
- KMP list
- FOCI determination
- List of all employees of the company possessing or in the process of obtaining DOE access authorizations who are Representatives of Foreign Interests (RFI)
- List identifying any other organization conducting work at the facility and access authorizations requested for each of their respective organizations
- Copy of the contractor's records of all contracts and subcontracts involving access authorizations
- Copy of the contractor's procedures implementing FOCI
- 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 lender involved as well as the aggregate amount of the loan or credit agreement.
- Board of director's meetings minutes to determine if any actions taken by the board resulted, or will result, in changes that should be reported to DOE
- Copies of all Schedules 13D and 13G submitted to the Securities and Exchange Commission (SEC), if publicly traded
- Annual report and/or financial statement of the company
- Shareholders' agreements to determine if amount of stock is sufficient to elect representation to the board or an agreement exists whereby the shareholder(s) is permitted representation on the board, currently or at a future date
- Proxy statements (notice of annual meeting of stockholders) to determine (1) current beneficial owners of 5% or more of the company's securities; (2) changes to the company's directors; and (3) changes in location of its principal executive offices, state of incorporation, or the company's business, management, proposed mergers
- Annual report and SEC Form 10-K report to determine (1) changes in revenue/income derived from foreign interests, (2) loan or credit agreements entered into with foreign lenders or in which foreign lenders are participants, and (3) joint ventures/contracts with foreign interests
- Internal Revenue Service Form 5471, *Information Return of U.S. Persons with Respect to Certain Foreign Corporations*, to determine whether all foreign holdings were reported
- Articles of incorporation and by-laws or partnership agreement to determine if any changes have been made to the company's/partnership's business or management

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

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

SAMPLE INTERVIEW CANDIDATES

Interview candidates may include the following:

- Contracts and procurement managers
- S&S program managers
- S&S director
- FSO – POC for the company's FOCI representations and information on foreign citizens with access to classified information or SNM and on foreign visits and assignments
- Facility procurement and contracting officer – POC for records of all contracts and subcontracts
- Corporate secretary – POC 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 – POC for information on revenue/income derived from foreign interests and loan or credit agreements entered into with foreign lenders

Work for Others (Non-DOE-Funded Work)

An area of Registration of Activities that requires special attention is Work for Others (WFO). WFO is work for non-DOE entities by DOE/NNSA and/or their contractors, or use of DOE/NNSA facilities for work that is not directly funded by DOE/NNSA appropriations. WFO is covered in DOE O 481.1C, *Work for Others (Non-Department of Energy Funded Work)*.

WFO projects should be reviewed during periodic assessments. In addition to the program management aspects of WFO, the topical and subtopical guidance applicable to each project should be used when reviewing WFO projects.

SAMPLE LINES OF INQUIRY

Suggested lines of inquiry can be used to (1) assist in determining the scope of assessment activities, (2) assist in developing document call lists, and (3) guide the interview process. Lines of inquiry may include:

Facility Approval and Registration of Activities

1. Are facility clearances granted prior to allowing DOE S&S interests on the premises of the facility?
   - Has a FDAR, DOE F 470.2, been completed and approved?
   - Has a CSCS, DOE F 470.1, been completed for all activities?
   - Has a Nondisclosure Certificate been provided for each interlocking owner, officer, director, partner, regent, trustee, or executive personnel (KMP)?
   - Does the facility have an approved SSP?

- What is the status of SSP activities?
- Is the facility in compliance with contents of the SSP?
- Are there any deviations in place at the facility? Are they current?
- Is there a process in place to ensure that a self-employed individual or consultant who will retain classified information or matter at their place of business is processed for and granted an FCL that applies to the premises where the individual or consultant will store, handle, or process classified information or matter?
- When a new activity will exceed the current FCL, or if there is no FCL, have all actions required to upgrade the current level or obtain an FCL been completed prior to contract award?
- Is there a process to ensure that in a corporate tier parent-subsidiary relationship, the parent and each of its subsidiaries are separate legal entities and must be processed separately for an FCL?
- Because the parent controls the subsidiary, does the parent have an FCL at the same or higher level as that of the subsidiary or has a parent exclusion resolution(s) been adopted?
- When a registered security activity is terminated, have all access authorizations associated with the activity been terminated and all DOE property, classified information or matter, and/or nuclear and other hazardous material been appropriately reallocated, disposed of, destroyed, or returned to the appropriate DOE or cleared DOE contractor organization?

2. Is there a process to ensure all KMP who occupy positions with the authority to affect organization policies or practices in security activities conducted under the contract are processed for an access authorization equivalent to the level of the contract?

   - At a minimum, do KMP include the senior management official responsible for all aspects of contract performance and the designated FSO?
   - Is FSO access authorization equivalent with the facility clearance?
   - Is there a process to ensure when changes in an organization’s KMP occur and are reported, access authorizations are processed for new KMP immediately?
   - Are company officials (typically owners, officers, directors, partners, regents, trustees, and/or executive personnel [KMP]) with the ability to affect organization policies or practices in security activities conducted under the contract cleared to the level of the FCL or formally excluded from access as appropriate?
   - Is there a process in place to ensure that when officials are to be excluded from or cleared at a level not commensurate with the FCL, compliance with one or both of the exclusion actions listed below is mandatory before issuance of an FCL?
     - When formal exclusion action is required, the organization's governing body must affirm that specific KMP (designated by name) will not require, will not have, and can be effectively excluded from access to all classified information or matter, or nuclear or other hazardous material presenting a potential radiological, chemical, or biological sabotage threat, that is entrusted to or held by the organization.
     - Additionally, the governing body must affirm that the specific KMP (designated by name) do not occupy positions that would enable them to adversely affect the organization's policies or practices in the performance of classified contracts.

     AND/OR
     - When officials are to be cleared at a level below that of the FCL, the organization's governing body must affirm that such KMP (designated by name) will not require, will not have, and can be effectively denied access to higher level classified information (specified by level), and do not occupy positions that would enable them to adversely affect the organization's policies or practices in the performance of higher level classified contracts.

- Is there a process to ensure that exclusion actions are made a matter of record by the organization's executive body and that a copy of the resolution is provided to the DOE cognizant security office?

Foreign Ownership, Control, or Influence (FOCI)

1. Are the procedures applicable to the FOCI program documented in the facility or SSPs?

2. Has a FOCI determination been made on all contractors and subcontractors that require access authorizations?

   - Has the contractor and subcontractors been given a favorable FOCI determination?
   - Do the contractor and subcontractor provide notifications of any changes that may affect the FOCI determination?
   - Were there any changes in management, loan or credit agreements with foreign lenders, or formation of company(ies) in foreign countries?
   - Have the beneficial owners of 5% or more of the company's securities changed?
   - Have there been any changes to the company's directors?
   - Did the location of the company's principal executive offices change?
   - Have the articles of incorporation and by-laws or partnership agreement changed?
   - When were the representations and certification provided?
   - Are WFO programs being performed at the facility?

3. Does the certification report include:

   - Detailed description of the manner in which obligations are carried out under the agreement?
   - Changes to security procedures, implemented or proposed, and the reasons for the changes?
   - Detailed description of any acts of noncompliance, whether inadvertent or intentional, with a discussion of steps taken to prevent such acts from recurring?
   - Any changes or impending changes of KMP or key board members, including reasons for the changes?
   - Any changes or impending changes in the organizational structure or ownership, including any acquisitions, mergers, or divestitures?
   - Any other issues that could have a bearing on the effectiveness of the applicable agreement?

Security Management in Contracting

1. How many classified contracts have been awarded at this facility?

2. Are the required DEAR clauses listed in the contract (DEAR 952.204-2-Security Requirements, DEAR 952.204-70-Classification/Declassification, and DEAR 952-204-73-Facility Clearances (Solicitation) for Contracts)?

3. Have all applicable security requirements been incorporated into the contract? Are there any pending incorporation?

   - How are you informed of security requirements to be included in a contract?
   - What is the process for incorporating new directives into the site contract?
   - Have all applicable security clauses been incorporated into contracts as appropriate? What is the process for ensuring contracts are made aware of security considerations?

- How are new directives incorporated into daily implementation for site-related DOE organizations?
- Have the incorporation of any directives been unduly delayed?
- Are there any equivalencies/exceptions in place at the facility? Are they current? Are they registered in SSIMS?

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

   - Has a nondisclosure certificate been provided for each interlocking owner, officer, director, partner, regent, trustee, or executive personnel (KMP)?
   - Does the facility have an approved SSP? Is the facility in compliance with contents of the SSP?
   - 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 giving during past surveys and self-assessments?
     - Is there a trend?

SAMPLE WORKSHEETS AND PERFORMANCE TESTS

The following worksheets and sample performance tests may be used during the assessment process to capture data necessary to evaluate the status of the program management operations.

CONTRACT REVIEW FORM

CONTRACT REVIEW FORM	
Review Date:	
Company Name:	
Subcontractor (if applicable) To:	
Contract Number:	
Contract Vehicle Type:	
Subcontract Number (if applicable):	
Original Contract Terms:	
Start Date:	
End Date:	
Number of Contract Extensions:	
Extended By:	End Date:
	End Date:
	End Date:
	End Date:
	End Date:
FOCI Clause:	
Security Clause:	
Classification Clause:	
Comments:	

SSP Data Collection Form

SSP DATA COLLECTION QUESTIONS		NOTES	YES	NO
1.	Has the current SSP been approved by the Operations/Site Office?			
	If not, when was the last time it was approved?			
	What are the reasons for not having an approved SSP?			
2.	Is there formal evidence of an annual review?			
	If so, how is this documented?			
3.	Does the SSP identify all Category I/II facilities at the site?			
4.	Does the SSP discuss the potential for rollup to Category I/II quantities from facilities located outside a PA?			
5.	Does the SSP identify any non-SNM critical facilities?			
	Bio-research laboratories?			
	Critical computer facilities?			
	Large-dose radiation facilities			
	Facilities critical to weapons production/stewardship?			
	Other? (List)			
6.	Does the SSP accurately describe the site's mission as well as the mission of listed facilities?			
	If not, explain:			
7.	Does the/SSP accurately describe and reflect the status of the site's S&S program?			
	If not, explain:			
8.	Does the SSP include a list of equivalencies/exemptions from DOE requirements?			
	Has the list been updated to match current requirements?			
	Have appropriate VAs been conducted to support the equivalencies/exemptions request?			
	Comments:			

	SSP DATA COLLECTION QUESTIONS	NOTES	YES	NO
9.	Are there any "non-standard" assumptions?			
	If so, list and provide the rationale used to justify the assumption and whether the justification is adequate.			
10.	Does the SSP describe the current level of system effectiveness (risk) for each key facility target?			
	If not, explain:			
11.	Does the SSP describe the change in system effectiveness (risk) resulting from proposed upgrades?			
12.	Does the SSP list alternatives considered and justification for recommended upgrades?			
13.	Does the SSP provide a schedule/plan for accomplishing the recommended upgrades?			
14.	Is there a process to develop and approve the SSP?			
	Describe the process to develop and approve the SSP:			
	Comments:			

EQUIVALENCIES/EXEMPTIONS ASSESSMENT

Deviations	Yes	No
Are equivalencies/exemptions documented in the SSP?		
Are equivalencies/exemptions implemented prior to approval?		
Are equivalencies/exemptions approved at the appropriate level of authority?		
Do equivalencies/exemptions requests fully and accurately describe associated vulnerabilities?		
Are the results of VAs and tests documented in the equivalencies/exemptions request?		
Do compensatory measures appear adequate? If not, please suggest workable alternatives:		
Are compensatory measures monitored by the departmental element?		
How are the cumulative impacts evaluated?		
Are all equivalencies/exemptions appropriately registered in SSIMS?		
Comments:		

Equivalencies/Exemptions	Characterized Appropriately	Documented in SSP	Implemented Prior to Approval	Approval Level

Equivalencies/Exemptions	Accurate Description	VA Results Included	Adequate Compensatory	Monitor Compensatory

3.2 PROTECTIVE FORCE

PROTECTIVE FORCE

- Subtopical Areas
- Common Deficiencies

Subtopical areas will address:

- Current Directives
- Potential Documents for Review
- Potential Interview Candidates
- Lines of Inquiry
- Performance Tests

Tab 3.2

SUBTOPICAL AREAS

- Management
- Training
- Duties
- Facilities and Equipment

COMMON DEFICIENCIES

The following is a sample of common deficiencies identified by the Office of Independent Oversight (now the Office of Security and Cyber Evaluations) in the 2009 document, *Protective Force Inspectors Guide*. By reviewing the list of common deficiencies during the planning phase, assessors can be alert for similar deficiencies during data gathering activities.

- Inadequate operational supervision
- Inadequate tactical supervision
- Failure of field element to approve plans/orders
- Inadequate MOU
- Lack of root cause analysis of deficiencies
- Inadequate JTA
- Lesson plans inconsistent with tasks/needs
- Lack of interface between operations and training
- Lack of performance testing
- Unreliable radio communications
- Lack of post-maintenance weapon check procedures
- Storage and issue of extra/special equipment
- Ineffective personnel identification skills
- Searches not properly conducted
- Inadequate understanding/application of deadly force policy
- Deficient tactical weapons/communications/skills
- Lack of integration between PF/VA/PSS

MANAGEMENT

SUBTOPICAL AREAS: MANAGEMENT

Sub-elements include:

- None

CURRENT DIRECTIVES AND REFERENCES

The following references apply to Management:

- 10 CFR 707, *Workplace Substance Abuse Programs at DOE*
- 10 CFR 712, *Human Reliability Program*
- 10 CFR 1046, *Physical Protection of Security Interests*
- 10 CFR 1047, *Limited Arrest Authority and Use of Force by Protective Force Officers*
- 10 CFR 1049, *Limited Arrest Authority and Use of Force by Protective Force Officers of the Strategic Petroleum Reserve*
- DOE O 221.1A, *Reporting Fraud, Waste and Abuse to the Office of Inspector General*
- DOE O 221.1A, *Cooperation with the Office of Inspector General*
- DOE O 231.1A, *Environment, Safety and Health Reporting*
- DOE O 470.3B, *Graded Security Protection Policy*
- DOE O 470.4B, *Safeguards and Security Program*
- DOE O 473.3, *Protection Program Operations*
- EO 13111, *Using Technology To Improve Training Opportunities for Federal Government Employees*
- HSPD-7, *Critical Infrastructure Identification, Prioritization, and Protection*
- 42 USC 23 (see also: Public Law 83-703), *Atomic Energy Act of 1954* (42 U.S.C., Chapter 23, Sections 2011 to 2296)

SAMPLE DOCUMENT LIST

Documentation to be reviewed may include:

- SSP
- Approved or pending equivalencies/exemptions
- Staffing plans
- Budget documents
- Overtime allocations
- VA and performance test data
- HRP criteria and list of staff assigned to HRP positions
- Response plans
- Recent findings and associated CAPs
- General, post, and special orders
- MOUs with local law enforcement
- Open and closed findings for past 12 months
- CAPs
- IOSC, root causes, and CAPs

SAMPLE INTERVIEW CANDIDATES

Interview candidates may include the following:

- PF manager
- S&S director
- PF training coordinator
- Individuals responsible for VA data
- SRT lead
- HRP manager
- Inquiry officers

SAMPLE LINES OF INQUIRY

Suggested lines of inquiry can be used to (1) assist in determining the scope of assessment activities, (2) assist in developing document call lists, and (3) guide the interview process. Lines of inquiry may include:

1. Has a successful supervisory program been developed to include procedures for inspecting SPOs reporting for duty to determine job knowledge, fitness for duty, and adequacy of equipment?
   - What is the process for selection of supervisors? What qualifications are necessary?
   - Do PF managers have the necessary experience/skills to effectively manage all aspects of PF operations?
   - What is the supervision ratio? Is it adequate?
   - Does PF management measure the effectiveness/performance level of its SPOs and shift supervisors?
   - Do supervisors adequately inspect personnel on post/patrol to ensure that personnel are knowledgeable of the duties they are to perform, proficient in the use of duty equipment, that post/patrol equipment is functioning properly, and that orders/procedures at the post/patrol are current and complete?
   - Do supervisors measure the effectiveness/performance level of personnel on post/patrol?

2. Has PF management developed plans, orders, and procedures that provide specific direction to enable the PF to successfully perform routine and emergency duties as well as address potential security emergencies?
   - Are these plans, orders, and procedures reviewed annually to ensure that they are comprehensive and accurately aligned with the SSP and site operations?
   - Do plans, orders, and procedures adequately document PF use of force and rules of engagement policy?
   - Are plans, orders, and procedures available to field personnel?
   - Does the PF, as a significant element in the facility's protection system, have an appropriate amount of input into facility protection strategy and policy decisions and directions?
   - Do the PF strategies employed (through policies, procedures, budget, personnel allocations, training, weapons, and equipment) appropriately complement the facility's protection strategy and contribute adequately to the protection of the facility's security interests?
   - What is the process for developing, updated, and maintaining procedures?
   - How are changes in procedures communicated to the field?

3. Do PF personnel possess the general skills and knowledge needed to perform routine duties, including:

- Observation, assessment, and reporting
- Weapons employment and maintenance
- Individual tactics and self-defense
- Vehicle operation
- Communications skills (e.g., communications equipment operation and use of appropriate communications procedures)
- Portal control
- Alarm station operations
- Access control duties, including personnel identification, searches, and operation of available detection equipment
- Required first aid and fire protection, including the ability to operate appropriate equipment?

4. Is there a complete and accurate record of post visits, inspections, and incidents bearing on security maintained?

   - Are investigations of anomalies noted in recording visits and is reporting thorough and timely?

5. Do personnel administration policies and procedures contain required elements, including pre-employment screening, job descriptions, position classifications, promotion policy, appropriate security clearances for SPOs, work scheduling policy, and overtime policy?

   - Does management have a method to monitor/assess levels of morale and discipline?
   - Is there a mechanism for corporate oversight of the PF disciplinary program?
   - Does PF management trend disciplinary actions and grievances to determine if there are any patterns of racism, profiling, sexual harassment, or preferential treatment?
   - What is the role of the bargaining unit (if applicable) regarding the disciplinary policy and grievance process?
   - Does PF management ensure that personnel meet established qualification requirements?
   - At tactical response force (TRF) sites, do all new hires meet the SPO-II requirements?
   - Do SPOs possess L or Q clearances?
   - Are records accurately maintained, including event logs; medical, physical fitness, and firearms qualifications; firearms cards; and SPO, SRT, etc., certification records?

6. What are the criteria for participation in HRP?

   - Are armorers with unescorted access to HRP PF firearms enrolled in HRP?
   - How many PF personnel are in the HRP?

7. Has management allocated the necessary resources (personnel and equipment) for the PF to be successful in achieving its assigned mission?

   - Does the PF have sufficient personnel resources available to ensure an adequate response in the amount of time and with the number of personnel required to contain, deny, and/or neutralize an adversary as defined in the approved SSPs?
   - How much of the staffing budget is allocated to overtime?
   - What is the current PF strength (armed and unarmed)?
   - How does interface/integration with other S&S organizations occur?
   - Are adequate numbers of supervisors assigned for each shift to the extent required to ensure proper and adequate performance of duties?
   - Is the PF organized in a manner that fosters effective mission performance (tactically cohesive units at Category I/II sites)?

8. Has management identified and established PF mission requirements?

   - Do PF personnel possess knowledge of relevant laws, policies, and orders, including those pertaining to the use of deadly force?
   - Can PF personnel effectively execute a SERP and respond in a tactically effective manner to satisfactorily address a major adversary threat?

9. Do PF managers have an open and frequently used line of communication with appropriate DOE field elements and facility S&S managers and staff?

10. Are PF self-assessment and corrective action programs adequately implemented?

11. Are the location and manning of posts based on GSP, VAs, SSPs, local threat statements, and DOE directives?

    - For Category I facilities, are tactical resources concentrated around the target?
    - At Category I sites, is there an SRT?
    - Is the SRT available at all times and dedicated to re-entry, recapture, pursuit, and recovery operations?
    - Are MOUs with federal, state, military, and local law enforcement agencies and other documents delineating agreements and outside assistance current and exercised to determine their effectiveness? How often are they reviewed and updated?

12. Do personnel on the job meet all pertinent certification requirements?

    - Are PF personnel able to effectively and efficiently operate all equipment assigned to them for the performance of their duties?
    - Do the appropriate personnel have the necessary skills and knowledge to perform special duties that may be required on a site-specific basis (including dog handling, flight operations, explosive entry, and sniper operations)?

SUBTOPICAL AREAS: TRAINING

Sub-elements include:

- None

Current Directives and References

The following references apply to Training:

- 5 CFR 410, *Training*
- 10 CFR 712, *Human Reliability Program*
- 10 CFR 851, *Worker Safety and Health Program*
- 10 CFR 1046, *Physical Protection of Security Interests*
- 10 CFR 1047, *Limited Arrest Authority and Use of Force by Protective Force Officers*
- 10 CFR 1049, *Limited Arrest Authority and Use of Force by Protective Force Officers of the Strategic Petroleum Reserve*
- DOE O 470.4B, *Safeguards and Security Program*
- DOE O 473.3, *Protection Program Operations*

Sample Document List

Documentation to be reviewed may include:

- Annual PF training plan
- Staffing plans
- 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 assessment and a list of PF personnel who are medically certified to participate in the physical fitness program)
- Training materials (rosters, curriculum, tests, task to training matrix, training needs analysis)
- Site-specific risk analysis for lesson plans
- List of PF 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)
- Basic SPO Training Program
- IOSC, root causes, and CAPs

Sample Interview Candidates

Interview candidates may include:

- PF manager
- S&S director
- PF training coordinator

- Individuals responsible for VA data
- Instructors

Sample Lines of Inquiry

Suggested lines of inquiry can be used to (1) assist in determining the scope of assessment activities, (2) assist in developing document call lists, and (3) guide the interview process. Lines of inquiry may include:

1. Does the training plan provide a clear roadmap for accomplishing the organization's training?
   - What are the strengths and weaknesses of the training program?
   - Is the training mission oriented to meet the sites protection strategy?
   - How well does the training program prepare the PF for mission accomplishment (how well trained is the PF)?
   - Are the results of training/testing monitored by both operations and training program managers?
   - Are sufficient resources (qualified personnel and sufficient equipment) allocated to training to ensure program effectiveness?
   - What types of training facilities are used?
   - Does the training manager integrate feedback information into the training curriculum?
   - Do the lesson plans currently in use support training goals?
   - Are PF training facilities sufficient to conduct realistic training and qualification programs safely?

2. Is there an established training program in place?
   - Is it based on a valid and complete set of tasks and competencies documented in JA or mission essential tasks lists (METLs)?
   - Does it have established training objectives that take into account the learning characteristics and competencies of trainees?
   - Is it designed to ensure that training activities enable trainees to achieve the level of competency required to adequately perform routine and emergency duties?
   - Has training been scheduled and conducted so as to meet the identified needs and goals?
   - Are PF Training Approval Program certifications current?
   - Are test results shared among performance test operations and training personnel for incorporation into the identification of performance enhancement needs?
   - Is there an established process for administering site-specific response plan training?

3. Are major performance tests (e.g., FOF) being conducted in the numbers and frequencies prescribed by current DOE policy?
   - Does the performance test program effectively integrate all forms of testing (no-notice alarm response and assessment exercises, individual and team LSPTs, and major ESS enhanced FOF exercises)?
   - Are the results of performance tests reported to PF training and VA/risk assessment personnel?
   - Who conducts the LSPT's? Is there a schedule?
   - Do the major tests incorporate/reflect testing against current GSP parameters and are scenarios tested restricted to worst-case pathways as established by VA modeling or does the testing have the flexibility to accommodate other adversarial initiatives that might better stress the system?
   - Is the PF evaluated during FOF exercises in individual and team tactical skills, application of force, weapon skills, the ability to communicate, and the ability to conduct operations in a chemical environment?

- Are response plans (including those for fresh pursuit, recapture, and recovery) fully tested during FOF exercises?

4. If canine patrols are deployed at the site, are they able to effectively identify explosive threats?

   - Do PF canine patrols receive training in accordance with limits and recommendations established by the U.S. Police Canine Association (16 hours per month or 4 hours per week)?
   - Are site canine explosive detection performance testing and training procedures adequate to mitigate the unauthorized introduction of explosive materials?
   - Does the site employ an operational test/training methodology that requires canine teams to identify explosive odors in the actual environment where these tasks are likely to be performed?
   - Has the PF developed adequate procedures for handling and storing explosive testing sources and training aids?
   - Are explosive testing sources and training aids stored in a manner that precludes cross contamination of test source odors? Specifically, are trinitrotoluene (TNT), dynamite, and ammonium nitrate fuel oil (ANFO) stored in separate/isolated storage bunkers/containers?

5. Are JTAs site-specific? Are instructors trained and certified through an approved program or process?

   - How many instructors have been certified through the NTC?
   - Are instructors evaluated for competency at least every 36 months?
   - Is instructor refresher training administered as required?
   - Do all firearms/intermediate force instructors complete annual refresher training?
   - Do PF instructors attend at least one professional development course every three years? Are supervisors provided initial and annual refresher training in tactical leadership and how to perform their supervisory duties?
   - Have JTAs been completed for all identified positions? Have all essential components been included?

6. Has training been developed and implemented for personnel performing such functions as CAS operators, crisis negotiators, canine handlers, controller/evaluators, and law enforcement specialists?

   - Do SRT personnel receive adequate training regarding mechanical and explosive breaching, consistent with the tactics, techniques, and procedures?
   - Has the PF SRT Program been certified/recertified annually as required?
   - Are CAS operator and SPO-II refresher training and SPO-III maintenance training administered as required?

7. Have all SPOs demonstrated proficiency every six months with all assigned firearms?

   - How many personnel have failed to pass fitness qualifications during the review period?
   - How many personnel have failed their firearms qualifications during the review period?
   - What type of remedial training is required for failing?

8. Do PF personnel receive adequate training regarding the GSP and potential adversary characteristics, tactics, motives, and actions required of first responders to weapons of mass destruction (WMD) incidents?

   - Are tactical exercises against GSP comparable adversary combatants (FOF) conducted at least quarterly with each shift participating at least annually?
   - Are tactical exercises involving each PF shift and each SRT shift on fixed sites conducted at least twice monthly for sites implementing the DOE Tactical Doctrine and monthly for other facilities?
   - At Tactical Doctrine sites, are WMD FOFs conducted every 24 months?

- Are SPOs trained in tactical operations and small unit tactics, and tested on the use of all assigned tactical equipment?
- Do SRT members train semiannually (at least every six months) in decisional shooting, close quarter battle, live fire shoot house operations, tactical obstacle course, night operations, team tactical movement, and force options (e.g., open air, mobile, emergency, and stronghold assaults)?

DUTIES

SUBTOPICAL AREAS: DUTIES

Sub-elements include:

- None

CURRENT DIRECTIVES AND REFERENCES

The following references apply to Duties:

- American National Standards Institute (ANSI)/American Society of Safety Engineers (ASSE) Z87.1-2003, *Occupational and Educational Personal Eye and Face Protection Devices*
- 10 CFR 1046, *Physical Protection of Security Interests*
- 10 CFR 1047, *Limited Arrest Authority and Use of Force by Protective Force Officers*
- 10 CFR 851, *Working Safety and Health Program*
- 29 CFR 1910, *Occupational Safety and Health Standards*
- DOE O 470.3B, *Graded Security Protection Policy*
- DOE O 470.4B, *Safeguards and Security Program*
- DOE O 473.3, *Protection Program Operations*
- National Institute of Justice (NIJ) Standard 0101.06, *Ballistic Resistance of Personal Body Armor*

SAMPLE DOCUMENT LIST

Documentation to be reviewed may include the following:

- SSP
- Approved JTAs
- Staffing plans
- Overtime allocations
- List of standard equipment issued
- PF schedules and post assignments
- MOU/MOA affecting duties and response
- General, post, and special orders
- Shipment security plans and procedures
- Emergency response plans
- List of critical targets
- SRT rosters
- SIRP
- Recent findings and associated CAPs
- Security lock and key control procedures
- Tactical defense plans
- VAs
- Results of performance testing and validation

SAMPLE INTERVIEW CANDIDATES

Interview candidates may include the following:

- PF manager

- S&S director
- PF training coordinator
- Individuals responsible for VA data
- PF operations manager
- SRT personnel
- SOs/SPOs
- 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 LINES OF INQUIRY

Suggested lines of inquiry can be used to (1) assist in determining the scope of assessment activities, (2) assist in developing document call lists, and (3) guide the interview process. Lines of inquiry may include:

1. What are the critical targets associated with this facility? How are they recognized?
   - What training is provided relative to identification of critical targets? Who has received this training and what are the criteria?

2. Do the communication systems used operate as designed and as intended?
   - How are communication channels determined to be effective (both internal to the PF organization and external to its counterparts)?

3. Does the performance testing program meet departmental requirements?
   - Have the SIRPs been designed to prevent the current GSP threats? Have they been tested, approved, and validated as being sufficient?
   - When was the last FOF exercise conducted?

4. How are changes in operations (e.g., material movements, compensatory measures, increase threat levels) communicated?
   - How are compensatory measures determined? Relayed to the PF?
   - How are changes to policies and procedures transmitted? Who is responsible for ensuring post orders are approved and current?
   - What role does the EOC play during shipments?

5. Are duties based on an approved JA and JTA?
   - Do the duties meet the requirements of the GSP threat levels?

FACILITIES AND EQUIPMENT

SUBTOPICAL AREAS: FACILITIES AND EQUIPMENT

Sub-elements include:

- None

CURRENT DIRECTIVES AND REFERENCES

The following references apply to Facilities and Equipment:

- 10 CFR 851, *Worker Safety and Health Program*
- 10 CFR 1046, *Physical Protection of Security Interests*
- 10 CFR 1047, *Limited Arrest Authority and Use of Force by Protective Force Officers*
- DOE O 473.3, *Physical Protection Operations*
- DOE O 470.4B, *Safeguards and Security Program*
- DOE O 460.1C, *Packaging and Transportation Safety*
- DOE-STD-1212-2012, *DOE Explosive Safety*

SAMPLE DOCUMENT LIST

Documentation to be reviewed may include the following:

- SSP
- Deviations
- Staffing plans
- Budget documents
- Overtime allocations
- List of standard equipment issued and instructions for use
- PF schedules and post assignments
- MOU/MOA affecting duties and response
- General, post, and, special orders
- PF weapons and ammunition inventories
- Equipment maintenance logs (including weapons)
- Recent findings and associated CAPs
- SIRP
- Range operating procedures
- Armorer training records and certifications

SAMPLE INTERVIEW CANDIDATES

Interview candidates may include the following:

- PF manager
- S&S director
- PF training coordinator
- Individuals responsible for VA data
- PF operations manager
- SRT personnel
- Armorers

SAMPLE LINES OF INQUIRY

Suggested lines of inquiry can be used to (1) assist in determining the scope of assessment activities, (2) assist in developing document call lists, and (3) guide the interview process. Lines of inquiry may include:

1. 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 protection strategy at this facility?
2. What are the critical targets associated with this facility?
   - How are they recognized?
   - Where are they located?
3. Have CSEs been identified, approved, and communicated? Integrated between VA, PF, and PSS groups?
   - Have compensatory measures for CSEs been identified, approved, and communicated?
   - What CSEs are currently under compensatory measures (timeframe, approval)?
     - Who approved the CSE compensatory measures?
     - What testing is/was performed?
     - How long has the CSE been out of service?
     - What is the timeline for completion of the CSE?
     - Has the cumulative impact of compensatory measures been assessed?
   - Is the response to alarms and/or system failures documented?
   - How are SPOs notified in case of system failure?
4. Are fixed posts and tactical fighting positions at key locations (i.e., near likely avenues of approach with optimal fields of observation) and in a manner that provides mutually supporting and/or overlapping fields of fire with adjacent posts and patrols?
   - Do fixed posts that DOE policy requires to be hardened meet the appropriate construction and materials requirements?
   - Are sufficient fixed posts and hardened fighting positions available in appropriate locations?
5. Is there an approved acceptance and validation testing program in place that encompasses security-related components and subsystems?
   - How is the acceptance and validation testing program implemented?
   - Are compensatory measures implemented immediately when any part of the critical system is out of service?
   - How are SPOs notified in case of system failure?
6. How is the assessment of alarms conducted?
   - Are assessment actions clearly delineated in post orders?
   - Are the PF trained to conduct assessment actions? If so, how often is the training conducted?
7. What actions are taken when an alarm point, sensor, or camera malfunctions or fails to operate correctly?
   - Are corrective actions clearly delineated in post orders?
   - Are the PF trained to conduct corrective actions?

- How often is corrective action training conducted?
- Are corrective actions covered by on-shift drills?
- Are corrective actions independently tested by the performance assurance/ performance testing section?
- Are the results of performance tests reported to PF training and VA personnel?

8. PF equipment (special equipment, supplies, transportation, communications, inventory requirements):

   - Is the PF equipped to effectively, efficiently, and safely perform routine and emergency duties?
   - Are all armed PF personnel issued equipment that provides an intermediate force capability (e.g., side-handle or collapsible baton, or chemical agents)?
   - Are protective masks available for SPO I, II, and III personnel, and federal agents (i.e., carried by personnel or stationed in such a manner to be quickly donned in support of response requirements without impact to response times)?
   - Are corrective eyeglass lenses worn by PF personnel made of Z87.1 American National Standards Institute safety glass?
   - Are personnel who are required to wear corrective lenses issued an extra pair to carry while on duty?
     - Are personnel who are required to wear corrective lenses also issued protective mask inserts?
   - What is the reliability of communications equipment, particularly of radios?
   - Is the maintenance and testing of communications equipment adequate?
   - Does the PF have sufficient updated specialized equipment such as x-ray machines, chemical/ biological detectors, explosive detection, and metal detectors?

9. Are individually and post-issued equipment stored and/or carried readily available in a manner that supports timely and effective response?

   - Is secure storage available for individually assigned equipment belonging to off-duty personnel (e.g., lockers)?
   - Are there adequate stocks of expendable supplies and equipment on hand to support the PF mission?
   - Has the PF established protocols and procedures that facilitate control and accountability of surplus equipment items?

10. Does the PF have sufficient appropriate vehicles to perform its patrol and response missions?

    - Are PF vehicles distinctively marked and equipped with necessary emergency equipment (e.g., external warning lights, sirens, radios, and spotlights)?
    - Are vehicles used in pursuit/recovery operations capable of communicating with supporting law enforcement agencies?
    - Are PF vehicles maintained in serviceable condition, with preventive maintenance performed at intervals that meet or exceed the manufacturer recommendations?
    - If armored vehicles are deployed at the site, do they offer assurance of continued operation and a safe level of protection to occupants under small arms fire, up to and including North Atlantic Treaty Organization 7.62 millimeter full-metal jacket?

11. Does the PF have adequate and sufficient special equipment and radios to perform its mission?

    - Can SPOs properly operate all equipment available for their use?
    - Can personnel properly operate assigned vehicles, including appropriate equipment on the vehicles?
    - Does the PF have sufficient suppressive fire weapons and weapons that facilitate neutralization of armored threats?

- Does the PF have adequate quantities of appropriate types of ammunition (armor penetrating, high explosive, high explosive/dual purpose, etc.) to defeat the threat?

12. Has the site established appropriate inventory and accountability protocols for the PF armory/ weapons?

    - Does protocol require the inventory (by number count) of all issued weapons at the beginning of each shift, of all weapons in storage (by number count) weekly, and all PF weapons (by type, manufacturer, and serial number) monthly?
    - If a weapon is missing, does protocol require an immediate investigation and reporting to site management and the cognizant DOE office?
    - Are all unissued or post issued firearms battlesight zero tested and verified semiannually? A review of firearms maintenance records will be conducted.
    - Has the site established appropriate procedures for the repair and serviceability of weapons by qualified, Q-cleared/HRP certified armorers?
    - Has the site established an adequate surplus (10%) of each type of firearm deployed?

13. How does the PF mitigate introduction of explosives to security areas?

    - If electronic explosives detection equipment is used, does it function effectively and are operators skilled in employment of such equipment?
    - If canine patrols are deployed at the site, are they able to effectively identify explosive threats?
        - Are canine patrol shift durations and working conditions established in a manner that fosters effective performance of duties?
        - Are kennel procedures, facilities, and resources adequate to facilitate a safe and healthy work environment?
        - Do PF canine patrols receive training in accordance with limits and recommendations established by the U.S. Police Canine Association (16 hours per month or 4 hours per week)?
        - Are site canine explosive detection performance testing and training procedures adequate to mitigate the unauthorized introduction of explosive materials?
        - Does the site employ an operational test/training methodology that requires canine teams to identify explosive odors in the actual environment where these tasks are likely to be performed?
        - Has the PF developed adequate procedures for handling and storing explosive testing sources and training aids?
        - Are explosive testing sources and training aids stored in a manner that precludes cross-contamination of test source odors? Specifically, are TNT, dynamite, and ANFO stored in separate/isolated storage bunkers or containers?
        - Are testing sources and training aids routinely replaced with fresh sources?
        - Are explosives test sources stored in approved repositories for the appropriate class of pyrotechnics/explosives?

14. Does the PF SRT at Category I/II sites have sufficient appropriate mechanical and/or explosive breaching resources to support recapture/recovery operations?

    - Is breaching equipment deployed in a manner that facilitates timely response?
    - Does each tactical entry specialist participate in quarterly mechanical breaching training?
    - Absence of specialized functional capabilities, such as mechanical or explosive breaching, or precision rifleman/forward observer teams must be justified. The site/facility must demonstrate alternative methods that can be used to meet these functional capabilities and/or demonstrate that absence of these capabilities does not affect the SRT ability to successfully execute recapture/ recovery.

SAMPLE WORKSHEETS AND PERFORMANCE TESTS

The following worksheets and sample performance tests may be used during assessment activities to evaluate the status of the PF topical area.

SECURITY VEHICLE INSPECTION CHECK SHEET

Date:	Assessment Team Member:	
Vehicle Number:		
Vehicle Year:	Make:	Model:
Mileage:		
General Vehicle Condition:		
Primary Use:		
Routine Patrol:	Shift Commander:	Security Staff:
Shift Change:	Emergency Use:	Armorer:
Training:	Other:	
Equipment Assigned to Vehicle:		
Emergency:		
Weapons:		
Comments:		

PORTAL/PATROL INSPECTION CHECK SHEET

Date: ______________________________ Assessor: _______________________________________

Portal Number: _____________________ Patrol Number: __________________________________

Post Order: Available ________________ Current: (Y / N)

Duress Alarm: (Y / N)

Portal Condition: ____

____

Number of SPOs: ___________________ Number of SOs: _________________________________

General Appearance: ____

Equipment:

Duty bag _____ Baton ________ Miranda Card ________
Flashlight _____ Rain Coat _____ Hand Cuffs __________
Arming Authority Card _______

Safety Glasses? (Y / N) Extra pair required? (Y / N) Extra pair carried? (Y / N)
Vision correction required? (Y / N) Vision inserts in use? (Y / N)
Gas Mask ___________________ Mask correctly fitted? (Y / N)

Weapons: ____

____

Ammunition: ____

Auxiliary Weapons: ____

Auxiliary Ammunition: ____

Accessibility of Auxiliary Weapons:

Communications Equipment: Radio ________
Telephone ____
Other ________

Comments: ____

CRITICAL ASSET IDENTIFICATION PERFORMANCE TEST

Objective: To evaluate critical asset identification capabilities of individual PF personnel.

Scenario: PF personnel are required to identify photographs of authentic critical assets, which are intermingled among numerous other photographs of spurious nuclear weapons components, nuclear devices, SNM, or other material resembling critical assets stored at the respective site. The test should not be limited to identification, but should also require personnel to identify likely storage locations and indicators for unauthorized movements/shipments of critical assets.

Evaluation Criteria:

1. Are PF personnel able to quickly identify critical assets?
2. Are PF personnel familiar with likely storage locations of critical assets?
3. Are PF personnel able to identify indicators of unauthorized movements/shipments of critical assets (e.g., lack of specified paperwork or dispatch to a particular type of alarm)?

Safety Plan: A safety plan will be completed for this performance test.

Commentary: This test is relatively simple to organize and administer. The primary difficulty encountered is displaying the photographs in a manner that does not indicate which photographs are false. This difficulty is compounded by the fact that many photographs of critical assets may be classified. One method of circumventing this obstacle is to place all photographs in identical document protectors and attach opaque tape over portions of the document protector where classification markings are visible. This performance test may be employed as part of a larger “shift readiness” performance test, which typically includes numerous, easily administered performance tests where a representative sample of the PF is selected for participation.

DURESS RESPONSE TEST

Objective: To determine whether the CAS operator is able to perform required response functions and whether the PF can conduct an effective response, using sound individual and team tactics.

Scenario: The assessment team initiates a no-notice duress test by having an on-duty SPO activate his duress instrument because he feels faint and is about to pass out. Receipt of the duress alarm, reporting, and dispatch of PFs are monitored at the CAS. Actions of the responding forces are evaluated at the scene.

Evaluation Criteria:

1. Is the CAS being properly monitored?
2. Is dispatch of security patrols prompt?
3. Are PF communications effective?
4. Are proper individual and team tactics demonstrated?

Safety Plan: A safety plan will be completed for this performance test.

Commentary: Properly conducted, even a small-scale, limited-resource duress response test can yield data on a wide range of areas such as command and control; alarm station operation; individual tactics; team tactics; communications; and observation, assessment, and reporting. The use of an on-duty SPO obviates the need for additional role players, yet gives responders something concrete to assess (for example, do they observe the SPO slumped at his post, do they attempt to raise him on the radio, what conclusions do they draw). Depending on response procedures at the site and additional scenario inputs, the test can also drive a broader range of tactical actions.

It is vital to stress that both the initial duress alarm and all subsequent communications be accompanied by appropriate notification that these are exercise-related activities. It is also necessary to ensure that appropriate response exercise safety procedures be carefully reviewed for each oncoming shift during the period in which test exercises are to be conducted.

ENTRY/EXIT SEARCH OF HAND-CARRIED PARCELS TEST

Objective: To evaluate the SPO's ability to conduct an effective search of hand-carried parcels while processing pedestrian access.

Scenario: The assessment team places items of contraband, simulated classified information, and metal objects configured to represent SNM or instruments of sabotage in briefcases, lunch pails, and other hand-carried containers. These are carried by badged employees attempting to enter or exit appropriate security areas. The inspection team observes the parcel search actions of the SPO during this attempt.

Evaluation Criteria:

1. Does the SPO understand the procedures governing search of hand-carried parcels?
2. Does the SPO make proper use of available search equipment (X-ray or metal detectors) as specified in post orders?
3. Is the SPO capable of conducting an effective search of a hand-carried parcel?
4. Does the SPO understand the correct actions to be taken and notification to be made when discovering:
    a. Contraband
    b. Classified information
    c. SNM
    d. Weapons or explosives

Safety Plan: A safety plan will be completed for this performance test.

Commentary: Most of the considerations discussed under identification of personnel tests also apply to the personnel search tests. In addition, great care must be exercised to ensure that when the simulated prohibited item used might represent an immediate threat to the PF personnel on post (e.g., a weapon or explosive device), that the test itself is halted *as soon as the item is detected*. Once the SPO has been informed that a test has taken place, he/she may be allowed to continue with the notification portions of the test.

USE OF FORCE, APPREHENSION, AND SEARCH

Objective: To evaluate the ability of SPOs to apply DOE policy on the use of force in practical site-specific scenarios; additionally, to evaluate the application of self-defense, subject control, and arrest techniques.

Scenario: A representative sample of SPOs is selected for this test. These personnel receive a detailed briefing that stresses adherence to safety procedures and the limitations governing the application of physical force during these tests. In particular, the briefing stresses the special safety prohibitions that govern scenarios in which the baton might be drawn. A non-firing exercise handgun is substituted for the SPO’s service weapon during the performance test.

SPOs encounter a variety of situations in an office building requiring them to take action and apply some degree of force, up to and possibly including deadly force, to resolve the situation.

The scenarios may include an altercation among employees, theft of classified documents, burglary, intoxicated or psychologically disturbed employee, and/or suicidal employee. The scenarios are played by composite adversary team (CAT) members. SPOs are required to demonstrate a range of self-defense, subject control, and arrest techniques. SPOs may also be required to draw a baton or a non-firing exercise handgun, substituted for their service weapon.

Evaluation Criteria:

1. Does the SPO apply only the amount of force necessary and in compliance with DOE policy to resolve the situation while protecting his/her life and the lives of others?
2. Does the SPO identify and preserve items of evidence?
3. Does the SPO demonstrate proper techniques for approaching, handling, and controlling hostile and non-hostile subjects?
4. Does the SPO use proper self-defense techniques?
5. Does the SPO use proper arrest and search techniques?

Safety Plan: A safety plan will be completed for this performance test. This plan will incorporate special controls upon the application of physical force in contact situations.

Commentary: This test may be repeated with variations to assess many different responses. The variations are introduced by having role players respond in different ways during the scenarios. Great care must be given in coaching the role players to perform in ways that will elicit the desired responses. Great care must also be taken to ensure that role players do not offer levels of resistance that could lead to uncontrolled grappling, with its attendant risk of injury; therefore, role players will become passive during actual physical contact, allowing themselves to be controlled and handcuffed. This “passive role” must be written into the test plan and safety plan, and role players must be fully briefed on the limitations on level of resistance. This issue must also be addressed thoroughly in briefing PF participants prior to initiating the scenarios. Again, it should be emphasized that the focus of these drills is on the selection of the right techniques and levels of force. Tests of the SPO’s actual ability to fully apply restraint techniques must be conducted only in an appropriate training environment, with proper safety equipment and a qualified sparring partner (typically, the site’s own self-defense instructor).

In addition to providing data in this area, these exercises present useful information on areas including individual and team tactics, and observation, assessment, and reporting. This latter area can be served by having each participating SPO complete a PF standard incident report at the scenario site. Comparing this report with the actual events observed by controllers during the scenario yields data concerning the SPO’s ability in this area.

Command and Control Tabletop Exercise

Objective: To evaluate the notional command and control capabilities of PF supervisors and other first responders to direct assets and implement site plans for a given security incident.

Scenario: Tabletop participants selected for testing usually include a representative sampling of shift supervisory personnel, CAS operators, and other key first responders who may be working on any one given shift. Testing is conducted in a notional tabletop forum, where participants are arranged around a sand table mockup of site facilities and/or detailed facility maps. An inspector begins by providing participants with a detailed scenario briefing for a chemical attack, recapture/recovery of SNM, emergency evacuation, or similar incident. The briefing should be configured to include types of alarms that have been communicated by the CAS and other pertinent environmental descriptors that require an escalating level of response. As the scenario unfolds, participants are shown various photographs or provided with key elements of information that would involve specific response actions noted in site incident response plans.

Participants should be permitted reasonable amounts of time to use appropriate plans, procedures, and documentation while articulating response actions, issuing orders, making notifications, simulating the deployment of an entire PF shift, and requesting information and intelligence, as appropriate. Facility maps or a sand table mockup should be used to illustrate each participant's response actions.

Evaluation Criteria:

1. Are participants able to quickly articulate required/appropriate response actions?
2. Are participants familiar with associated plans, procedures, and MOA?
3. Are participants able to collectively execute response plans and/or formulate appropriate solutions?

Safety Plan: A safety plan need not be completed for this performance test.

Commentary: This test may be repeated with scenario variations to test many different responses. Reviewing a variety of response procedures and VAs, and identifying specific actions required for a given incident will assist in developing challenging scenarios. Great care should be given to inconspicuously prompt participants to act upon the desired scenario inject. A comparison of test results with the actual events observed by controllers during the FOF exercise yields valuable data concerning the overall command and control capabilities of the PF.

3.3 PHYSICAL PROTECTION

PHYSICAL PROTECTION

- Subtopical Areas
- Common Deficiencies

Subtopical areas will address:

- Current Directives
- Potential Documents for Review
- Potential Interview Candidates
- Lines of Inquiry
- Performance Tests

SUBTOPICAL AREAS

- Access Controls
- Intrusion Detection and Assessment Systems
- Barriers and Delay Mechanisms
- Testing and Maintenance
- Communications

COMMON DEFICIENCIES

The following is a sample of common deficiencies identified by the Office of Independent Oversight (now the Office of Security and Cyber Evaluations) in the 2009 document, *Physical Security Systems Inspectors Guide*. By reviewing the list of common deficiencies during the planning phase, assessors can be alert for similar deficiencies during data gathering activities.

- False and nuisance alarms
- Improper installation, calibration, or alignment
- Tamper protection for power sources
- Inadequate testing and maintenance program
- Failure to properly assess and respond
- Inadequate monitoring
- Improper badge accountability procedures
- Improper storage of unissued badges and passes
- Incomplete handling of lost badges
- Failure to update photos
- Ineffective barrier location
- Fence maintenance
- Access to active denial system controls
- Inadequate lock and key accountability and control
- Insufficient number of radio frequencies
- In adequate testing and maintenance procedures
- Compensatory measures not providing equivalent protection
- Inadequate preventative maintenance program
- Inadequate tamper protection for auxiliary power sources
- Responsibilities not specifically assigned
- Inadequate training
- Inadequate CAPs
- No root cause analysis of deficiencies
- Inadequate interface/integration with other protection elements
- Lack of integration between PF, VA, PSS

SUBTOPICAL AREAS: ACCESS CONTROL

Sub-elements include:

- None

CURRENT DIRECTIVES AND REFERENCES

The following references apply to Access Control:

- American Society for Testing and Materials (ASTM) C993-92 (2012), *Standard Guide for In-Plant Performance Evaluation of Automatic Pedestrian SNM Monitors*
- ASTM C1112-99, *Standard Guide for Application of Radiation Monitors to the Control and Physical Security of Special Nuclear Material*
- ASTM C1189-11, *Standard Guide to Procedures for Calibrating Automatic Pedestrian SNM Monitors*
- 32 CFR 2001, *Classified National Security Information*
- DOD 5220.22-M, *National Industrial Security Program Operating Manual*
- DOE O 470.4B, *Safeguards and Security Program*
- DOE O 473.3, *Protection Program Operations*
- DOE O 470.3B, *Graded Security Protection Policy*
- EO12968, *Access to Classified Information*
- NIJ Standard 0601.02, W*alk-Through Metal Detectors for Use in Concealed Weapon and Contraband Detection*
- National Fire Protection Association (NFPA) 101, 2012 edition, *Life Safety Code*
- Underwriters Laboratory (UL) 752, Edition 11, *Standard for Bullet-Resisting Equipment*
- 5 USC 552a, *Records Maintained on Individuals*
- 42 USC 2278a, *Trespass on Commission Installations*

SAMPLE DOCUMENT LIST

A personnel identification system should identify those personnel who are authorized to enter or leave security areas and should indicate, as necessary, limitations on their movements or access to classified matter within such areas. Documentation relating to access controls may be reviewed, including:

- 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 credential 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, procedures, records
- Documents identifying security areas and S&S interests
- Termination/transfer procedures and notifications
- Building plans and PA 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)
- Recent findings and associated CAPs
- IOSC, root causes, and CAPs

SAMPLE INTERVIEW CANDIDATES

Interview candidates may include the following:

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

SAMPLE LINES OF INQUIRY

Suggested lines of inquiry can be used to (1) assist in determining the scope of assessment activities, (2) assist in developing document call lists, and (3) guide the interview process. Lines of inquiry may include:

1. What types of access control systems are used at the facility (e.g., receptionists, badge readers)?
    - If more than one method of access control is used at a security area (e.g., badge check and card reader), how do the systems complement each other and which is considered the primary means?
    - What alternative identification verification procedures are available?
    - Is an authorized access list maintained?
    - Who conducts performance tests on the systems and how are the records kept?
    - What happens in the event of an unsuccessful test or system failure?
    - Is a layered approach to protection employed?
    - Are physical barriers used to preclude external visual access to classified matter?
    - Is access to facilities controlled as detailed in facility security plans?
    - Are personnel monitoring access control systems properly trained?
    - Are post orders relating to badge checks current and consistent with site policies?

2. What policies are in place to ensure timely termination of access through retrieval of keys and access credentials upon termination or transfer?
    - How are various functions notified of terminations and transfers?
    - How are records secured, maintained, and retrieved?
    - Is there a list of lost badges at the post (including lost badges of other organizations that are accepted by the facility)?
    - Is there a documented process for ensuring access is terminated as appropriate (e.g., HRP status changes, clearances terminated, employees terminated)?

3. Are there well-defined search system policies and calibration specifications for personnel and vehicle searches?
   - What are the procedures for vehicle control, including volume of traffic and the authorization process for private, government-owned, vendor, emergency, and SPO vehicles?
   - What are the methods and procedures for conducting exit searches at each security area?

4. Have auxiliary power sources been provided to all critical systems?
   - What are the testing and maintenance procedures for ensuring auxiliary power is available?

5. What policies/procedures are in place to ensure compliance with badge requirements?
   - How is the site badging system equipment secured after hours?
   - 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 storage/protection measures meet the requirements of the DOE directive?
   - Do the site procedures address the recovery of badges after employee termination?
   - Are lost badges being handled according to appropriate procedures?

INTRUSION DETECTION AND ASSESSMENT SYSTEMS

SUBTOPICAL AREAS: INTRUSION DETECTION AND ASSESSMENT SYSTEMS

Sub-elements include:

- None

CURRENT DIRECTIVES

The following references apply to Intrusion Detection and Assessment Systems (IDAS):

- DOE O 470.4B, *Safeguards and Security Program*
- DOE O 473.3, *Protection Program Operations*
- UL 681, *Edition 13, Standard for Installation and Classification of Burglar and Holdup Alarm Systems*
- UL 1076, *Proprietary Burglar Alarm Units and Systems*
- UL 1610, *Standard for Central-Station Burglar-Alarm Units*

SAMPLE DOCUMENT LIST

Documentation to be reviewed may include the following:

- SSP
- PSS 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 (UPS) certification and maintenance logs
- Compensatory procedures for equipment outages
- LSPT results
- System certification
- Approved/pending equivalencies/exceptions
- Recent findings and associated CAPs

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

SAMPLE INTERVIEW CANDIDATES

Interview candidates may include the following:

- S&S staff responsible for security systems
- SPO/SO
- 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 LINES OF INQUIRY

Suggested lines of inquiry can be used to (1) assist in determining the scope of assessment activities, (2) assist in developing document call lists, and (3) guide the interview process. Lines of inquiry may include:

1. How well is the PSS program functioning?
   - What areas of the system could be improved and what steps have been taken toward the improvements?
   - Are any line-item construction projects associated with the PSS? If so, when were they last reviewed and who conducted the review?
   - Is there a documented testing and maintenance plan?
   - Are CAS and SAS fully redundant?

2. Are all necessary security-related components supplied auxiliary power?
   - Are auxiliary power systems adequately protected?
   - What is the source of offsite electric power, including number of feeds?
   - Are indications received in CAS/SAS (alarm station) when normal or auxiliary power fails?
   - Are auxiliary power systems adequately tested (for example, are generators turned on, brought up to speed, and the load switched on or does the test only simulate power loss)?
   - Do site systems have power backups, tamper protection devices, etc.?
   - Are there appropriate anti-tampering devices on primary and backup power sources for intrusion detection equipment?

3. Does the site have policies and procedures for the installation, alignment, and calibration of intrusion detectors?
   - Is equipment calibrated according to documented specifications?

4. Does the site have procedures to assess intrusion, tamper, and line supervision alarms?
   - Is the alarm monitoring system operator adequately trained to identify potential threats and clearly transfer information to responding personnel?
   - Is access to the IDS terminals physically controlled?

5. Does the site have procedures for responding to alarms, including a defined response time and response procedures? If so, do they include multiple alarms that occur simultaneously?
   - What are the definition of false alarms and nuisance alarms for the facility and how they are assessed?
   - Does the site have procedures for recording/logging alarms?
   - Are FARs/NARs consistent with facility definitions?
   - Are there a minimum of false or nuisance alarms that can be verified by documentation?
   - Are response times consistent with those documented in security plans and VAs?
     - Is the response to alarms and/or system failures documented?
     - How are SPOs notified in case of system failure?

6. Does performance testing of interior alarms reveal any non-functioning or poorly functioning sensor?

7. Is the IDS effective in sensing intrusion into detection zones?
   - Does the site IDS distinguish between intrusion, tamper, and supervisory alarms?
   - Does the site use a closed-circuit television (CCTV) system with video capture capability for primary assessment of alarms?
   - Can alarms be reliably assessed with the cameras as they are installed and configured?
   - Do any obstructions interfere with assessment?
     - Is lighting adequate for assessment?
     - Does the video capture system support assessment?
     - Is it susceptible to deception by alarm stacking?

8. Does the PIDAS have an effective testing and maintenance program?
   - Are complementary sensors used for the PIDAS (different sensor types that cannot be defeated by the same means, rather than multiple layers of the same sensor)?
   - What is the condition of the PIDAS? Is the bed free of obstructions?
     - Do crossover points have blind spots?
     - Are sectors susceptible to bridging?
     - What methods are used to detect intrusion at each security area?

9. Have CSEs been identified, approved, and communicated? Integrated between VA, PF, and PSS groups?
   - What is the basis for the items on the CSE list? Is the list current?

10. Are there documented procedures to implement compensatory measures?
    - If so, do the compensatory measures provide equal to or greater coverage of the system or component they are replacing?
    - Have the accumulative impacts of compensatory measures been evaluated?
    - Has the risk-accepting authority approved compensatory measures?
    - What is the process for implementing compensatory measures should a CSE fail?
    - What CSEs are currently under compensatory measures (timeframe, approval)?
      - Who approved?
      - What testing is/was performed?
      - How long has it been out and what is the timeline for completion?

BARRIERS AND DELAY MECHANISMS

SUBTOPICAL AREAS: BARRIERS AND DELAY MECHANISMS

Sub-elements include:

- None

CURRENT DIRECTIVES AND REFERENCES

The following references apply to Barriers and Delay Mechanisms:

- DOD 5220.22-M, *National Industrial Security Program Operating Manual*
- DOE O 470.4B, *Safeguards and Security Program*
- DOE M 473.3, *Protection Program Operations*
- NFPA 101, 2012 Edition, *Life Safety Code*

SAMPLE DOCUMENT LIST

Documentation to be reviewed may include the following:

- SSP/VA data
- Performance assurance test plans, procedures, and results
- Post orders
- Critical target lists and locations
- PSS 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 (UPS system)
- Compensatory procedures for equipment outages
- Lock and key control procedures and inventory results
- Automated access control system testing and maintenance records

SAMPLE INTERVIEW CANDIDATES

Interview candidates may include the following:

- S&S staff responsible for security systems
- SPO/SOs
- Engineers (involved with security systems)
- Alarms maintenance/installation and testing personnel
- CAS/SAS management/operators
- VA staff
- Emergency management planners

SAMPLE LINES OF INQUIRY

Suggested lines of inquiry can be used to (1) assist in determining the scope of assessment activities, (2) assist in developing document call lists, and (3) guide the interview process. Lines of inquiry may include:

1. How is the program functioning?
   - Are approved equivalencies/exceptions 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?
   - 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?
   - Are response times consistent with those documented in security plans and VAs?
     - Are the barriers designed to provide for adequate delay time to allow for appropriate response?
   - Are the barriers at the site commensurate with the risk?

2. Does the site have procedures to patrol and inspect security area perimeter barriers to verify integrity and detect unauthorized objects or conditions?
   - Are fence lines and other barrier-type systems periodically inspected for condition and repaired as necessary? Who performs the inspection and at what frequency?

3. 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 the barriers at SNM areas, vaults, and MAA perimeters sufficient to ensure SNM cannot be removed?
   - Do the security containers meet all required DOE and other standards?

4. Does the site have a documented lock and key program?
   - Does the program have a documented inventory system with a defined inventory frequency?
   - How often are key inventories conducted? How are discrepancies resolved and what are the reporting requirements?
   - Are lock and key control requirements applied in a graded fashion, including storage, issuing, marking, use, and destruction of locks and keys as well as reporting of lost keys?
   - Has a database been established to provide accountability information for security locks and keys as well as padlocks, including the location of all of those items?

5. Has the GSP or Interagency Security Committee (ISC) policy been used in developing appropriate protection strategies?
   - Is the protection granted commensurate with the security interest value and importance?

TESTING AND MAINTENANCE

SUBTOPICAL AREAS: TESTING AND MAINTENANCE

Sub-elements include:

- None

CURRENT DIRECTIVES REFERENCES

The following references apply to Testing and Maintenance:

- ASTM F792-08, *Standard Practice for Evaluating the Imaging Performance of Security X-Ray Systems*
- DOD 5220.22-M, *National Industrial Security Program Operating Manual*
- DOE M 473.3, *Physical Protection Operations*
- DOE M 470.4B, *Safeguards and Security Program*
- ISC Standard, *Physical Security Criteria for Federal Facilities*
- NIJ Standard 0601.02, *Law Enforcement and Corrections Standards and Testing Program*

SAMPLE DOCUMENT LIST

Documentation to be reviewed may include the following:

- Performance assurance test plans, procedures, and results
- Post orders
- PSS description(s) and location(s)
- Maintenance and testing records and procedures
- FAR/NAR
- Calibration procedures and records
- CAS/SAS procedures
- Emergency power systems (UPS system)
- Compensatory procedures for equipment outages
- Inspection procedures
- Recent findings and associated CAPs

SAMPLE INTERVIEW CANDIDATES

Interview candidates may include the following:

- S&S staff responsible for security systems
- SPOs/SOs
- Engineers (involved with security systems)
- Alarms maintenance/installation and testing personnel
- CAS/SAS management and operators
- Other personnel responsible for monitoring/clearing alarm indications
- PF Managers
- Emergency management planners

SAMPLE LINES OF INQUIRY

Suggested lines of inquiry can be used to (1) assist in determining the scope of assessment activities, (2) assist in developing document call lists, and (3) guide the interview process. Lines of inquiry may include:

1. Is an approved verification and validation testing program in place that encompasses security-related components and subsystems?
   - How is information coordinated between the organization responsible for testing and maintenance and the user organization?
   - Are plans for installation of new or replacement security-related equipment thoroughly evaluated by subject matter experts before the installation process is initiated?
   - How is the testing program implemented?
   - How are the testing records maintained and/or retrieved?
   - Are there documented testing procedures?
   - Is the testing proceduralized and how are personnel trained to the procedures?
   - Are compensatory measures implemented immediately when any part of the critical system is out of service?
   - Does the site analyze maintenance results to identify trends and prioritize maintenance activities?
     - Do maintenance records from the prior year identify failure trends?
     - Is any trend analysis of maintenance requests being conducted for security equipment and systems?

2. Who performs the periodic testing (technicians, custodians, or security personnel)?
   - Are maintenance personnel qualified by the equipment vendor to perform repairs?
   - Are procedures in place to verify or inspect work performed by offsite vendors?
     - What mechanisms are in place to ensure appropriate access authorizations are held if required?

3. Does management ensure all areas of systems anomalies or non-compliance are corrected in a timely and efficient manner?
   - How are repairs initiated when a system element fails?
   - Is the response to alarms and/or system failures documented?
   - What is required to place the system back in service after maintenance and/or repair?
   - Are procedures in place to verify system integrity after software modifications are completed?

4. Is the maintenance and testing program documented, including frequency and content of specific preventive maintenance and of testing activities?
   - Is maintenance and testing for the CCTV system adequate?
   - Are there records of maintenance? If so, what are the minimum, maximum, and mean time of corrective maintenance of CCTV system for the past two years?
   - Are procedures adequate for maintenance and calibration of security-related equipment?

5. Is the site FAR/NAR consistent with established requirements and are excessive rates properly conveyed to management for resolution?

6. What is the process for implementing compensatory measures if a system fails?
   - Is there a backlog of maintenance activities for CSEs or other security related equipment?

COMMUNICATIONS

SUBTOPICAL AREAS: COMMUNICATIONS

Sub-elements include:

- None

CURRENT DIRECTIVES AND REFERENCES

The following references apply to Communications:

- ANSI/Telecommunications Industry Association (TIA)/Electronic Industries Alliance (EIA)-102, *Project 25 Circuit Data Specification*
- 18 USC 2511, *Interception and Disclosure of Wire, Oral, Or Electronic Communications Prohibited*
- 32 CFR 2001, *Classified National Security Information*
- 47 CFR, 90.548, *Interoperability Technical Standards*
- DOE M 205.1-3, *Telecommunications Security Manual*
- DOE O 473.3, *Physical Protection Operations*
- DOE O 470.4B, *Safeguards and Security Program*
- ISC, *Physical Security Criteria for Federal Facilities*

SAMPLE DOCUMENT LIST

Documentation to be reviewed may include the following:

- Performance tests of communication equipment
- PF post orders
- PF general orders
- VA/SSP data
- Description of communication equipment, its location, and test documentation
- Types of communication issued to PF
- Shipment procedures
- Recent findings and CAPs

SAMPLE INTERVIEW CANDIDATES

Interview candidates may include the following:

- PF members
- S&S staff responsible for communication systems
- Alarms maintenance/installation and testing personnel
- CAS/SAS personnel
- SRT members
- Emergency management planners

SAMPLE LINES OF INQUIRY

Suggested lines of inquiry can be used to (1) assist in determining the scope of assessment activities, (2) assist in developing document call lists, and (3) guide the interview process. Lines of inquiry may include

1. Are communications adequate for routine and emergency conditions?
   - When was the last time the communication systems was upgraded and why?
   - Are PF radios equipped with an encryption capability?
   - Are alternate means of communication available and what are they?
   - Is there an anti-jamming capability and/or jamming detection?
   - If the site uses an encrypted radio frequency signal for communication, is the encryption key appropriately protected and routinely changed?
   - What compensatory actions are taken when ratio communication is unavailable?
2. Does the site have proper authorizations to record radio and telephone traffic?
   - Are security radios continuously recorded over all channels?
3. Are radio battery power and sensitivity adequate?
4. 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?
   - Are communications tested on all frequencies and at key locations?
   - Are procedures in place for switching to different frequencies during specified tactical conditions?
5. Are there radio duress alarms and how often are they tested?
   - Does the site have procedures for communicating duress when a duress switch cannot be activated?
   - Can duress alarms be quickly and inconspicuously activated?
6. How are PF radios issued and controlled?
   - Can a single radio be identified and disabled by the CAS/SAS operator?
7. How are repeater towers protected?
8. Are security system transmission lines and data protected from tampering and substitution?

SAMPLE WORKSHEETS AND PERFORMANCE TESTS

The following worksheets and sample performance tests may be used during the assessment to evaluate the status of the Physical Protection topical area.

ACCESS CONTROL

Objective: The objective of this test is to determine whether an individual could access a security area with either an old badge or with no badge.

Scenario: The assessment team member, with a site representative, attempts to enter a security area where access is controlled by either a SO or receptionist. The team member has an old badge or conceals his/her badge before attempting entry.

Conditions: Normal operating conditions.

Evaluation Criteria: The SO or receptionist shall challenge the team member and deny access until a positive identification is made.

Intrusion Detection and Assessment System: Security Lighting

Objective: The objective of this test is to determine if adequate security lighting has been provided at all security areas, for the assessment of alarms, detection of unauthorized personnel attempting access, and to properly check credentials.

Scenario:

Procedures:

1. The test is conducted approximately one hour after sunset.
2. The site representative provides a calibrated light meter that displays light levels in foot-candles.
3. Light-level readings are taken within the PIDAS zone along the centerline of the zone, along the outer fence, and along the inner fence. Along each line of measurement, readings will be taken at 25-foot intervals between the light fixtures.
4. Light-level readings are taken around PF posts out to 30 feet from the post. Additional readings are taken out to 150 feet from the post.

Conditions:

The test is conducted during non-operational hours when the security lighting is activated. All light fixtures should be functioning properly.

Evaluation Criteria:

1. Lighting must be at least 2 foot-candles within 30 feet of entry control points for personnel to check credentials.
2. Lighting must be at least 0.2 foot-candles within 150 feet of PF post for unaided assessment of alarms.
3. Lighting for PIDAS zones must be at least 0.2 foot-candles to allow the PF to assess alarms using CCTV.
4. All lighting must meet the requirements outlined in DOE directives.

Intrusion Detection and Assessment System: Balanced Magnetic Switch Sensors

Objective: The objective of this test is to determine if door-mounted balanced magnetic switches (BMS) can be moved more than one inch (measured from the leading edge of the door to door frame) without indicating an alarm condition.

Scenario:

1. The assessment team member selects which BMS to test.
2. The assessment team member and site representative proceed to the selected alarm location(s) equipped with a PF radio.
3. The CAS is notified to announce when the alarm is received. When the alarm has been received the test is complete for that sensor.
4. The assessment team member observes as the site representative attempts to open an alarmed door a distance greater than one inch without causing an alarm.

5. The assessment team member ensures that the BMS is moved slow enough to allow the CAS to detect and announce the alarm.

Conditions: This test will be conducted during operational or non-operational hours depending on location of test and impact on operations.

Evaluation Criteria:

1. Ensure an alarm signal is received by the CAS.
2. The BMS must sound an alarm prior to being opened greater than one inch.
3. Ensure that the CAS receives the alarm and that it has an individual address and is not part of a loop of alarms.
4. Ensure maintenance records reflect proper maintenance.
5. Ensure that a record of previous tests exists and that the tests were performed in accordance with established procedures and timeframes.

Exterior Perimeter Sensors

Objective: The objective of these performance tests is to determine the effectiveness of exterior perimeter sensors.

System Tested:

<u>System</u>: IDS

<u>Function</u>: Perimeter intrusion detection

<u>Component</u>: Exterior sensors, transmission lines, alarm processing equipment, interfaces with CCTV and CAS operation, and testing and maintenance of perimeter sensors

Scenario: Assessors should select one or more zones of a perimeter system for testing based on sensor configuration, terrain, location of buildings and portals, and operating history. A quick tour around the perimeter is helpful in identifying zones and potential deficiencies. Items of interest may include ditches, humps, dips, other terrain variations, obstacles or obstructions, sewer lines, pipes or tunnels that pass under the zone, piping or utility lines that pass over the zone, barriers that could be used as a platform to jump over sensors or to avoid observation, excessive vegetation, and standing water. Particular attention should be paid to identification of potential gaps in sensor coverage.

The number of sensors and zones selected for testing depends on the time available, importance of the system in the overall protection program, and variation in the individual zones. The following guidelines are intended to assist the inspector in the selection of sensors and zones for testing:

- At least two zones should be tested. If the zones employ different sensor configurations, or if the sensor configuration at portals is significantly different, the inspectors should consider selecting at least one of each type.
- At least one of each type of sensor should be tested, if possible. This should include sensors on building roofs and in tunnels under the perimeter.
- If the first few performance tests do not indicate problems and there is no evidence of exploitable deficiencies, the assessors should not generally devote extensive time to testing numerous zones and sensors. However, if deficiencies are apparent, the assessors should collect sufficient data to determine if a deficiency is an isolated instance or evidence of a systemic problem.
- Tests should be conducted for selected zones in which terrain features or questionable installation practices are likely to degrade detection capability.

It is useful for assessors to observe security alarm technicians or SPOs conducting routine operational or sensitivity tests. Assessors should determine if the tests, calibrations, and maintenance procedures are consistent with DOE orders and the SSP, and if they are an effective means of testing the systems. Two goals are accomplished by having the facility's security technicians conduct the routine test prior to testing by the inspectors. First, the facility tests are indicators of the effectiveness of the test and maintenance program and procedures. Second, the facility tests should verify that the sensors are calibrated according to facility specifications, thus the assessors will be testing a system that is operating as the facility intends. This may be important in identifying the root cause of any deficiency.

The assessors may conduct walk, crawl, run, jump, climb, and step tests, as appropriate, to determine whether an adversary could cross the perimeter without detection and whether the individual sensors are properly calibrated.

Assessors should monitor the alarm annunciation in the CAS and SAS to determine whether the alarms are functioning properly. The assessors may also observe the operation of interfacing systems, such as the automatic CCTV display and video recorders.

Evaluation: If the detection system is effective, the sensors will detect intrusion and the alarms will annunciate accordingly.

Fence Disturbance Sensors

General Characteristics: Sensing wires/cables attached to or woven through fence, sonic capacitance, or piezoelectric technologies.

Intruder Detection Capabilities: Cutting, climbing, or other vibration/deflection of sensor wire or fence.

Vulnerabilities: Tunneling, trenching, bridging.

Concerns:

- Fence disturbance sensors are susceptible to defeat by tunneling, bridging, or jumping, if no physical contact with the sensing wires occurs.
- Depending on the sensitivity setting, fence disturbance sensors may be susceptible to high FARs. Common causes of false alarms include high winds, animals, and other sources of fence vibration. It is important that fences, gates, outriggers, and barbed wire be mechanically sound and well maintained to prevent excessive fence vibration.
- In some sensor designs, the sensing wires are least sensitive near the terminal connections and corners.
- The sensor wire or sensors must contact the fence for reliable, nuisance alarm-free performance. It is important that the sensors and/or cabling be attached per manufacturer specifications.

Types of Tests:

- Unaided Climb Test: An individual (preferably a small individual) climbs the fence at various locations to verify that detection occurs. Attempts should be made near fence posts, especially corners/posts.
- Ladder Climb Test: A ladder is placed against the fence. An individual climbs the ladder to the point of sensor activation.
- Cutting Attack: No actual cutting of the sensor wires or fence fabric should be performed.
- Jump Tests: These tests cannot normally be conducted if a fence disturbance sensor is properly installed, due to the height of the detection zone (8 feet or more). However, adjacent structures used

as platforms may permit an individual to jump over the fence/sensor wire, if personal safety can be ensured.

Test Guidelines:

- All of the unaided climb tests should be conducted on several fence posts in at least two typical zones.
- Zones that are substantially different (gates or different sensor configuration) should also be considered for testing.
- Areas that appear vulnerable to jumping should be tested to determine whether vulnerability exists. Safety concerns should be addressed.
- If an individual sensor can be defeated, that same sensor should be tested again to determine whether the deficiency can be repeated. Several tests of the same sensor may be required to determine whether an adversary can reliably exploit the sensor deficiency.
- If an individual zone can be defeated, other zones should be tested using the same methods to determine the extent of the problem. The assessors should conduct several (three to five) more tests in different zones. If most of these tests indicate that the sensors can be reliably defeated, it is likely that there is a systemic problem. If no other sensors are defeated, one may conclude that an isolated deficiency was identified. If the results are inconclusive, additional testing should be considered. Rarely would an assessor test more than 10 to 15 zones using the same methods.
- If the adversary has sufficient knowledge, time, and equipment, bridging or tunneling techniques can defeat all fence disturbance sensors. Such tests should only be conducted if a zone is particularly vulnerable (for example, due to barrier placement), or if patrol frequencies and direct visual observation (CCTV or from guard posts) are considered inadequate to provide reasonable assurance that such attempts are detected.

Checklist: Fence Disturbance Sensors **Exterior Perimeter Intrusion-Detection System**
Interview Items
Installation location:
Operational test frequency:
Operational test method:
Sensitivity test frequency:
Sensitivity test method:
Acceptance criteria for sensitivity test:
False alarm history/records:
Make/model:
Measures to prevent erosion:
Tamper switches (transmitter, receiver, junction boxes):
Tour/Visual Inspection Items
Vegetation present?
Zone length OK?
Complements other sensors?
Overlap sufficient?

Data Collection Sheet
Fence Disturbance Sensors
Exterior PIDAS Test Method

	Zone Tested	Unaided Climb	Ladder Climb	Cutting	Jump
1					
2					
3					
4					
5					
6					
7					
8					
9					
10					
11					
12					
13					
14					
15					

Comments:

INTERIOR SENSORS

Objective: Test the effectiveness of interior sensors in detecting adversary intrusion.

System Tested:

System: IDS

Functional Element: Interior intrusion detection

Component(s): Interior sensors, transmission lines, alarm processing equipment, interfaces with CCTV and CAS operation, testing and maintenance of interior sensors

Scenario: The assessors should select several interior locations (MAAs, vaults, vital areas, or vault-type rooms) for testing based on a number of factors: sensor types, construction type, materials, configuration of the interior area, and operating history of the various sensors. At least one of each type of room or vault configuration and sensor should be tested.

The assessors should review building layouts and architectural drawings. They should also briefly tour the facility to familiarize themselves with typical protection system configurations and to identify potential weaknesses. The relationship between sensor application and the types of structural barriers in use should be noted. The detection capabilities of individual sensor types may vary depending on the types of barriers used and the ability of these barriers to resist or delay penetration. Also, since some sensors respond to physical attacks on the barrier material, it is important that the detection technology employed (e.g., acoustic, vibration, strain, or capacitance technologies) be suited to the barrier material used.

In general, sensors will be of three generic types: motion (or area), barrier penetration, and proximity. Each of these types is subject to various physical and environmental limitations that must be considered when assessing suitability and operating performance. Limitations involve electromagnetic, radiological, acoustical, seismic, thermal, and optical effects as well as the physical limitations imposed by equipment placement, room arrangement, and building materials used in walls, ceilings, floors, windows, doors, and penetrations (for example, ductwork and cable chases).

If possible, the assessors should observe alarm technicians or SPOs during conduct of routine operational and sensitivity tests of selected sensors. The assessors should base their selection of the sensors to be tested on the number, type, configuration, and operational history of those sensors. During this portion of the test, inspectors should observe calibration and maintenance procedures to determine whether they are consistent with DOE orders and approved SSPs. In addition, observation of these tests may indicate the effectiveness of the test and maintenance program. Observations of facility-conducted tests are helpful in identifying the root causes of many noted deficiencies.

The assessors should conduct standard walk and tamper-indicating tests (provided no physical damage to the sensor will result) for each motion detection (area type) sensor tested. Barrier sensors (magnetic switches, glass sensors, and capacitance devices) and proximity sensors may require other tests as applicable and as identified in manufacturer’s instructions. The purpose of these tests is to determine whether each sensor type is functioning, whether it can detect attempted tampering, and whether it can detect its design basis target (intruder) or activity (for example, attempted barrier penetration using force or attack tools).

Within a single area there may be several types of sensors that have different detection goals. For example, some barriers may have a penetration detection sensor, a volumetric area sensor for the interior, and a proximity or capacitance sensor to protect the actual item.

The assessors should monitor the alarm annunciation in the alarm stations and observe the operation of any interfacing systems, such as CCTV displays and video recorders, to determine proper functioning.

The number of areas and sensor types to be tested depends on the available time, importance of the system in the overall protection program, and operating history. The following guidelines are intended to assist the assessor in selecting areas and sensors for testing:

- At least five protected interior areas (rooms/vaults/MMAs) should be tested. Priority should be given to those areas containing the most critical assets.
- At least one of each type of sensor should be tested, if possible, including motion sensors, penetration sensors, and proximity sensors, if used.
- If several tests of the same type of sensor are satisfactory, extensive testing of that sensor in different areas is not necessary. However, if deficiencies are apparent, sufficient testing should be conducted to determine whether there is a systemic weakness.
- Tests should be conducted for selected areas where environmental concerns (noise, electromagnetic interference, temperature, and humidity changes) or physical obstructions are likely to degrade sensor performance.

Evaluation: If a detection system is to be effective, the sensors must detect intrusion, the alarm condition must be correctly assessed, and PF must be available for a timely response.

Assessing Sensor Performance:

The primary objective in evaluating interior intrusion-detection sensors is to determine whether they effectively detect penetration, intrusion, or proximity to protected devices or equipment. Other factors to consider are:

- Do BMS sensors initiate an alarm when exposed to an external magnetic field or when the switch is moved one inch from the magnet housing?
- Does the sensor layout allow adversaries to circumvent any sensor(s) because of alignment, obstructions, or environmental interference?
- Are there any temporary entry points or penetrations to barriers that could allow undetected intrusion?

Interpreting Results: The following guidelines are provided to assist the assessor in interpreting evaluation results.

- Many interior sensor systems employ redundant or layered protection schemes that rely on a combination of barrier, volumetric, and point protection systems. If any one of these is found to be deficient during testing, this finding should be evaluated in the context of the site-specific protection program objectives and the effectiveness of other complementary systems.
- In some cases, facility tests may indicate sensors are properly calibrated but inspector tests may indicate that the sensors can be defeated or cannot reliably detect intrusion. In such cases, the inspector can reasonably conclude that there are deficiencies in the test and calibration procedures or in the quality assurance program, or both.
- When facility tests and calibrations and the tests conducted by inspectors indicate that sensors are performing according to specifications, the limitations of the test procedures used must still be considered. All modes of defeat and all physical and environmental factors may not have been considered when conducting the tests.
- Sensor performance that does not appear to be in accordance with specifications may simply indicate sensor drift or an alignment problem; however, a systemic deficiency in sensor design, application, or maintenance might also be indicated. If the facility tests indicate that sensors are out of

calibration, inspectors should consider instructing the facility's technicians to test a representative sample of sensors to determine the extent of the problem.

Special Considerations:

Some sensors are sensitive to the size of the intruder. The assessor should request the facility to provide a small person to conduct walk tests. If special equipment is necessary, it should be provided. Often, interior sensors may be located at ceiling height or in relatively inaccessible places (for example, in ductwork or cable chases). Ladders or other aids may be needed.

Related testing or activities, such as those for barriers, card access control systems, CCTVs, or line supervision or tamper indication, are typically conducted concurrently with sensor tests in order to minimize data-collection activities.

Perimeter CCTV Testing and Long Range Camera/Tracking Systems

System Description: Fixed and pan-tilt-zoom (PTZ) cameras, usually with low-light capability; mounted on pole, tower, or wall; coaxial, fiber optic, cable, or microwave transmission; associated switching, display, and recording equipment.

Capabilities: Perimeter surveillance and intrusion assessment with ability to discriminate human intruders from animals or other causes of false or nuisance alarms from the perimeter IDS.

Vulnerabilities: Extreme weather (ice, snow, fog, rain, wind), inadequate security lighting, improper alignment or overlap, and visual obstructions or shadows caused by structures or uneven terrain.

Concerns:

- Cameras and associated supporting systems (switches, monitors, and recorders) are complex devices requiring extensive maintenance and calibration. Certain components (especially camera image tubes) are subject to predictable failure due to age, which may be a system-wide occurrence.
- CCTV capability may be seriously degraded by weather extremes (ice, fog, snow, rain, wind-blown dust). Where extremes are prevalent, environmental housings (blowers, heaters, wipers) should be present and in good working condition.
- If CCTV towers, poles, or wall mounts are not rigid, the cameras are subject to wind-induced vibration that can cause loss of video assessment capability.
- For outdoor application, cameras should have a broad dynamic range to allow for effective operation during daylight and darkness. Light-limiting and auto-iris capabilities should be provided to compensate for varying background light levels and to minimize "bloom" from bright light sources (perimeter lighting, vehicle headlights).
- Visual obstructions (buildings, vegetation, towers, fences, structures, or terrain irregularities) can block camera fields of view, creating the potential for intruders to hide or cross the isolation zone without being observed. The shadows from such obstructions can also interfere with effective observation.
- Camera image tube and video monitor burn-in can result from constant focus on a high-contrast background (extreme light-to-dark ratio), which degrades camera and video monitor performance.
- If camera placement or alignment is improper, there may be holes in the CCTV coverage that permit an unobserved intruder to cross the isolation zone. Additionally, if the camera field of view is too long for the camera lens, an intruder at the extreme end of the field of view may not be adequately observed. (Note: Industry requires that the postulated adversary occupy at least five vertical scan lines when standing at the far end of the camera's field of view.)

- If cameras are located outside of PA boundaries (to provide better coverage with IDS zones), they may be more vulnerable to tampering.
- Automatic camera call-up on the alarm monitor at the CAS/SAS, upon activation of an IDS sensor (if employed), should be sufficiently rapid to observe the intruder before he/she crosses the isolation zone and reaches the inner perimeter fence. Alternatively, the video-recording system (digital or laser disk) should be capable of recording and playing back the camera scene showing the intruder crossing the isolation zone.
- PTZ cameras should have limit switches to preclude their facing directly into bright light sources. Also, if they are called up by IDS activation, they should be programmed to automatically position themselves to view the area from which the alarm was received.

Types of Tests:

Functional Test: The CAS/SAS calls up each camera scene to verify that cameras are operating and that a clear image is received. If multiple monitors are used for continuous display (for example, 9-inch sequenced monitors), assessors should verify their function and sequencing (if employed). Check all PTZ functions for proper operation. Also check video-recording systems.

Field-of-View Test: A person positioned at the far end of the camera field of view slowly walks across the isolation zone. This test should verify that the inner perimeter fence line is within the view of each camera that observes the isolation zone. In conjunction with the perimeter IDS test, assessors should conduct field-of view tests if the far point of the camera view appears to be excessively long (that is, a clear image of an intruder cannot be seen at the far end of the camera's view).

Obstruction Test: A person runs and hides behind an obstruction or in a shadowed area. This test should be conducted when an identified obstruction or shadow may preclude effective observation.

Speed of Response Test: At a narrow point in the isolation zone, a person runs through the IDS sensor zone to the inner perimeter fence line. This test is used to verify that automatic camera call-up and/or video recording is sufficiently rapid to allow observation of the intruder before he can leave the isolation zone and the camera's field of view.

Test Guidelines:

- All tests should be conducted during daylight and at night to ensure lighting is adequate and cameras can function properly in low-light conditions. Additionally, the functional test should be conducted at sunrise or sunset to verify that positioning the camera directly toward the sun does not degrade camera functions.
- At a minimum, testing of at least two camera zones should be conducted.
- Obstruction tests should be conducted whenever functional tests indicate the assessment capability in a camera zone is significantly degraded by an obstruction.
- If a significant number of camera zones (more than 10 percent) exhibit degraded picture quality, maintenance records should be reviewed to determine whether useful camera life limits might have been reached due to not replacing camera image tubes.

INTERIOR CCTV TESTING

System Description: Fixed and PTZ cameras; wall or ceiling bracket-mounted; coaxial cable or fiber optic transmission; associated switching, display, and recording equipment.

Capabilities: Interior surveillance and intrusion assessment with ability to differentiate between humans and animals or other causes of false or nuisance alarms generated by the interior IDS.

Vulnerabilities: Inadequate lighting, improper alignment or overlap, and visual obstructions.

Concerns:

- Cameras and associated supporting systems (switches, monitors, and recorders) are complex devices requiring extensive maintenance and calibration. Certain components (especially camera image tubes) are subject to predictable failure as they age. Failure because of aging may be a system-wide occurrence if several cameras were installed at the same time.
- Visual obstructions can block camera fields of view, creating the potential for intruders to hide or cross the camera zone without being observed.
- Camera image tube and video monitor burn-in can result from constant focus on a high-contrast background (extreme light to dark ratio), which degrades camera and video monitor performance.
- If camera placement or alignment is improper, there may be holes in CCTV coverage that could permit unobserved intruder access. Additionally, if the camera's field of view is too long for the camera lens, an intruder at the extreme end of the view may not be adequately observed. (Note: Industry requires the postulated adversary to occupy at least five vertical scan lines when standing at the far end of the camera's field of view.)
- Automatic camera call-up on the alarm monitor at the CAS/SAS upon activation of an IDS sensor (if employed) should be rapid enough (no more than 2 seconds) to observe the intruder before he/she crosses the camera's field of view. Alternatively, the video recording system (digital or laser disk) should be capable of recording and playing back the camera scene showing the intruder crossing the camera zone.
- PTZ cameras should have limit switches so they will not face directly into bright light sources. Also, if PTZ cameras are automatically called up by IDS activation, they should be programmed to automatically position themselves to view the area from which the alarm was received.

Types of Tests:

Functional Test: The CAS/SAS calls up each camera scene to verify that all cameras are operating and that a clear image is received. If multiple monitors are used for continuous display, their function and sequencing (if employed) should be verified. Any PTZ functions should also be checked for proper operation, as should video-recording systems.

Field-of-View Test: A person positioned at the far end of the camera field of view walks slowly across that view. In general, this test should verify that critical access portals are within the camera's field of view. In conjunction with the interior IDS test, field-of-view testing should be conducted if the far point of the camera's view appears to be excessively long (that is, a discernible image of an intruder cannot be obtained at the far end of the camera's field of view).

Obstruction Test: A person hides behind an obstruction or in a darkened area. This test should be conducted whenever an obstruction and/or lighting conditions could preclude effective observation.

Speed of Response Test: A person activates an interior sensor and then attempts to rapidly exit the area covered by the camera. This tests the speed of camera response when automatic call-up of a camera upon IDS activation is employed.

Test Guidelines:

- All tests should be conducted under day, night, and overcast conditions to ensure that the cameras can function in all light conditions, as applicable.
- At a minimum, test at least two camera zones, if possible.

- Conduct obstruction tests whenever functional testing indicates that the assessment capability in a camera zone is significantly degraded by an obstruction.
- If a significant number of camera zones (more than ten percent) exhibit degraded picture quality, maintenance records should be reviewed to determine whether useful camera life limits have been exceeded because camera image tubes have not been replaced.

ALARM PROCESSING AND DISPLAY EQUIPMENT

General Characteristics: CAS/SAS alarm consoles, alarm annunciators and displays, system status indicators, CCTV monitors and recorders, personnel and vehicle access controls, lighting and emergency power controls, and various support equipment.

Capabilities: Security system monitoring, control, assessment, and historical recording, as appropriate; redundant command and control capabilities at CAS and SAS.

Vulnerabilities: Poor human-machine interface, excessive numbers or differing types of displays, inadequate redundancy between CAS and SAS.

Concerns:

- High numbers of nuisance/false alarms may degrade operator response to genuine alarm conditions.
- Failures of the system to adequately identify alarm type and specific location may degrade response. This is usually most evident in systems that do not clearly differentiate between tamper-indication or line-supervision alarms, or when multiple sensors are monitored by a single circuit (for example, alarms in series).
- In older systems, which do not use a computer-based integrated alarm processing system, a variety of different alarm panels and status indicators may be employed. This can cause inefficiency and confusion in assessing and acknowledging alarms because the operator must respond to several standalone annunciators.
- In older computer-based systems, problems may arise from the computer’s lack of speed or from inadequate alarm prioritization. In those cases, the system is unable to expeditiously and effectively sort significant quantities of simultaneous, or near simultaneous, alarm information and the system becomes bogged down resulting in slower alarm processing, storing alarm information without prioritization, or (in the worst case) a system crash. If such conditions were to occur, the ability of the operator to provide timely detection/assessment information to the PF would be severely degraded, as would the PF ability to rapidly respond.
- For computer-based systems, problems may also arise as new or additional sensors or access control devices are added over time. Each time the system configuration changes, software programming changes are required in the system. Unless software modifications and system configuration are carefully controlled, program errors may be generated.

Types of Tests:

Function Test: Assessors should perform a functional test of each type of alarm annunciator, status indicator, or control device in conjunction with each subsystem test (for example, CCTV, intrusion-detection system, access control, emergency power test). The purpose is to verify proper system function and to determine whether alarm annunciation, acknowledgement, and command/control are clear and straightforward. Promptness of alarm display following field device activation should be checked concurrently.

Historical Record Test: Evaluate any historical records maintained by the system (for example, alarm logs, access control transaction histories, and video recordings) for completeness and accuracy. FARs and NARs may also be assessed by reviewing these records.

SAS Test: Test a representative number of alarm annunciations and command/control functions at the SAS to determine that the SAS provides adequate backup to the CAS. As part of this testing, inspectors should verify that the SAS is capable of knowing about any command actions taken by the CAS that change alarm points or access control devices from the secure mode to the access mode or that enable or disable security devices.

Test Guidelines:

- Conduct testing of alarm processing and display in conjunction with other system tests.
- Test CCTV displays and recording capabilities during both daylight and darkness.
- At a minimum, test at least one of each type of alarm annunciation, recording device, and command/control function.
- Conduct a separate LSPT of the SAS to verify its adequacy as a backup to the CAS.

CCTV Identification System

System Description: CCTV systems are used to verify the identity of personnel entering a security area. Such systems allow a remotely stationed SPO to conduct a badge check by simultaneously viewing images of a person and his/her badge. Alternatively, the SPO may compare a person’s image to a stored video image.

Components of CCTV ID Systems: Camera, transmission lines, monitor, remote door lock activator, electric door lock.

Concerns:

- In most cases, CCTV identification systems do not include provisions for searching personnel and are not suitable for portals where searches are required.
- If SPOs do not pay adequate attention to verifying identity, unauthorized personnel may be allowed entry.
- Remote CCTV identification systems are vulnerable to persons disguising their faces or using false or stolen credentials. As such, they are not suitable for high-security purposes (for example, MAAs or PAs); however, CCTV identification may be adequate for compartmentalizing areas within a security area.
- Uneven lighting, shutdown, glare, or degraded equipment may drastically reduce the capability to effectively compare images.
- If the CCTV identification system (or related controls) does not include provisions for preventing “tailgating” or “piggy-backing” (two or more persons entering an area using only one credential), the facility may be vulnerable to insiders deliberately allowing access, or employees unwittingly allowing access, to unauthorized persons. Measures to deter tailgating include having SPOs monitor the area or using mantraps (interlocked doors or turnstiles designed to ensure that only one person passes through at a time).
- Cameras and related systems and monitors require periodic maintenance to ensure reliable operation.
- Systems without uninterruptible or auxiliary power will not operate in the event of a power failure. Facilities with systems that fail in the non-secure mode (for example, electric locks that fail in the

open position) may be vulnerable to unauthorized access during periods when power is unavailable because of natural events, accidents, or deliberate sabotage.

Types of Tests:

Electric Door Lock Tests: One test involves verifying that the door lock engages immediately after the door closes so that a person following immediately behind cannot open the door before the door lock engages. The assessors should examine the door and electric lock system to determine whether it can be defeated by techniques such as blocking the lock operation or cutting power to magnetic locks.

Door Alarm Interface Tests: These tests are conducted to determine whether the door alarm is operational and integrated with the remote control. One test is to hold the door open for an extended period (30 seconds or more) to determine whether an alarm condition is initiated. This test is usually applicable only at unattended doors.

Visual Inspection of CCTV Monitor: The inspectors enter the CAS, SAS, or other location where a CCTV identification monitor is located and observe image quality. If any CCTV identification portals are outdoors, observation of monitors under day and night conditions is recommended.

Test Guidelines:

- The most frequent problem with CCTV is improperly maintained equipment. The assessors should visually check the quality of the images on the monitors at the CAS, SAS, and other control locations.
- Tests of electric door locks or door alarm interfaces should be conducted at portals that are used for high-security applications and are not protected by other means (for example, SPOs stationed at the post who can monitor the entrance).
- Tests involving unauthorized personnel or persons using improper credentials may be designed to test the alertness of the SPOs who monitor the CCTV identification system; however, such tests must be conducted without the knowledge of the SPO and require detailed safety plans.

SNM Detector—Walk-Through Testing

Typical Uses:

- Detect SNM at MAA personnel egress points.
- Detect SNM at PA personnel egress points.

Concerns:

- Personnel are typically in the detection zone of a portal monitor for only a short time and detection capability is sensitive to the rate of speed at which they pass through the detectors. The detectors are typically calibrated and tested with a test source carried by a person who walks through the detector at a normal rate of speed. If the speed of exiting personnel is not adequately controlled (that is, if personnel are not prevented from running or throwing items through the detectors), the detection capability can be substantially reduced.
- Detectors, wiring, and electronics may be susceptible to tampering if not adequately protected by methods such as buried lines, locked control panels, or tamper alarms.

Types of Tests:

Operability Tests: A person walks through the detection zone with a goal quantity of SNM or the standard test source according to the normal procedures at that post (which may include requirements for a short pause before proceeding). These tests are conducted to verify proper operability of the detector. Such testing should be conducted with the source placed near the left edge, center, and right edge of the detection zone and at different elevations (for example, shoe level, waist level, and head level).

Sensitivity Tests: Such testing generally involves observing a security technician as he/she conducts the acceptance test that would normally be conducted after a calibration. This may involve a series of walk-throughs designed to demonstrate that the detector has an acceptable detection probability. Sensitivity tests are conducted to determine whether the detector is correctly calibrated.

High-Background Tests: Generally, the facility's or manufacturer's test procedures are followed. Testing typically involves slowly moving a radiation source toward the detector (without setting off the occupancy sensor) while monitoring the detector count rate in order to verify the high-background alarm occurs at the specified threshold value. High-background tests are conducted to verify that high-background alarms operate as designed.

Low-Background Tests: Generally, the facility's or manufacturer's test procedures are followed. Testing typically involves disabling or shielding the detectors to reduce the count rate. The inspectors monitor the count rate to verify the alarm occurs at the specified threshold. Low-background tests are conducted to verify low-background alarms operate as designed.

Occupancy Sensor Tests: Generally, the facility's or manufacturer's test procedures are followed and typically involve entering the detection zone and verifying the alarm. Detectors use a variety of occupancy sensors to detect the presence of personnel and to initiate the monitoring measurement. The most commonly used sensors include photoelectric, ultrasonic, microwave, infrared, and pressure sensitive. Occupancy sensors are tested to verify sensor operability.

SNM Detection Capability Tests: Inspectors may elect to conduct additional testing of detection sensitivity, focusing on the capability of the detectors to detect SNM removal. Such testing may involve using SNM in the form and quantity found in the security area and testing the detection capability with the SNM concealed at various locations on the body or in packages. The inspectors should use their knowledge of SNM detectors, occupancy detectors, and search procedures to conduct tests that will challenge the system. For example, inspectors can attempt to pass material through the walk-through monitor while avoiding the occupancy sensor. Another example is a "kick test," which involves placing the SNM at shoe level and swinging the foot through the detector as fast as possible when walking through (minimizing the time in the detection zone). Testing should be conducted with a quantity of SNM that is equal to or greater than the goal quantity.

Shielded SNM Tests: Assessors may elect to conduct testing of the detector's capability to detect shielded SNM. Such tests involve shielding SNM with lead or other shielding material. Assessors can then determine the amount of shielding that is necessary to prevent detection of a significant quantity of SNM (for example, a Category I quantity). It is recognized that any quantity of SNM can be shielded and detection prevented if a sufficient amount of shielding is used. Shielding tests can be used to determine how much shielding would be necessary. Such information can be used to determine whether the other search procedures (for example, visual observation as the person passes through the portal) are a credible means of detection, and can also be used as a baseline for performance tests of SPO search procedures. For example, if shielding tests indicate that a 20-pound lead container will prevent detection of a Category I quantity of SNM, then the assessors might conduct testing of the SPO's visual search procedures involving a lead container in a toolbox.

Test Guidelines:

- Typically, the assessors conduct operability tests, sensitivity tests, high-background tests, low background tests, and occupancy sensor tests at a few key portals (typically two or three). If the facility has a large number of portals and those portals use several different types of detectors or substantially different search procedures, then the inspectors may choose to test one of each major type of detector.

- SNM detection capability tests and shielded SNM tests should be conducted at a typical portal if an appropriate SNM source and shielding is available. Frequently, such tests require extensive security precautions, particularly if Category II or greater quantities of SNM are involved. The assessor`s may, instead, elect to review the results of similar tests or analyses conducted by the facility to determine the capability to detect SNM in shielded or unshielded configurations.
- If any deficiencies are noted in the installation or operation of detectors, or in the implementation of search procedures, the assessors should conduct testing to exploit those deficiencies in order to determine their significance/extent. For example, if the assessors note that a walk-through detector is not adequately monitored by SPOs, then the assessors could design and conduct tests to determine whether a person could successfully throw a significant quantity of SNM through the detector in an attempt to avoid detection. Additional tests could be conducted to determine how large a quantity could be diverted by that method. Tests that are designed to indicate whether the SPO notes any unusual behavior (for example, throwing items through the detector) might be considered.
- If an individual detector can be defeated, that same detector should be tested again to determine whether such defeat is repeatable. Several tests of the same detector may be required to determine whether an adversary can exploit a deficiency.
- If an individual detector can be defeated by one or more methods (for example, walk-through, pass around), the similar detectors at other portals should be tested by the same method in order to determine the extent of the problem. If possible, assessors should conduct several (three to five) more tests at different portals. If most of these tests indicate the detector can be reliably defeated, there is sufficient evidence that a systemic problem exists. If no other detectors are defeated, then one may conclude that an isolated deficiency was identified. If the results are inconclusive, the inspector should consider testing more detectors. Rarely would an assessor test more than five detectors by the same method.
- If the adversary has sufficient knowledge, time, and equipment, all SNM detectors can be defeated by using sufficient quantities of shielding. Testing should generally be conducted only if a portal is particularly vulnerable (for example, due to lack of metal detection capability) or if direct visual observation CCTV or SPOs at posts are considered inadequate to provide reasonable assurance that such attempts can be detected.

3.4 INFORMATION SECURITY

INFORMATION SECURITY

- Subtopical Areas
- Common Deficiencies

Subtopical areas will address:

- Current Directives
- Potential Documents for Review
- Potential Interview Candidates
- Lines of Inquiry
- Performance Tests

Tab 3.4

SUBTOPICAL AREAS

- Basic Requirements
- TSCM
- OPSEC
- Classification Guidance
- CMPC

COMMON DEFICIENCIES

The following is a sample of common deficiencies identified by the Office of Independent Oversight (now the Office of Security and Cyber Evaluations) in the 2009 document, *Information Security Inspectors Guide*. By reviewing the list of common deficiencies during the planning phase, assessors can be alert for similar deficiencies during data gathering activities.

- Responsibilities not specifically assigned
- Inadequate training for classified matter custodians and key personnel
- Inconsistency in procedures and practices
- Inadequate CAPs
- No root cause analysis of deficiencies
- Inadequate inquiry and reporting
- No documented program of disciplinary action for infractions
- Lack of basic program elements (OPSEC Program)
- Lack of relevant OPSEC assessments and reviews
- Documents not reviewed for classification
- Draft documents not properly marked
- Incorrect or missing markings
- Improper declassification or change of classification level
- Failure to continuously control classified documents
- Documents not in accountability
- Inadequate reporting of unaccounted for documents
- Transmittal accountability receipts not returned
- Improper wrapping
- Improper transmittal methods
- Improper use of degaussing equipment
- Lock combinations not changed as required
- Repository checks not performed consistently

BASIC REQUIREMENTS

SUBTOPICAL AREAS: BASIC REQUIREMENTS

Sub-elements include:

- None

CURRENT DIRECTIVES AND REFERENCES

The following references apply to Basic Requirements:

- 10 CFR 1016, *Safeguarding of Restricted Data*
- 10 CFR 1044, *Security Requirements for Protected Disclosures Under Section 3164 of the National Defense Authorization Act for Fiscal Year 2000*
- 32 CFR 2001, *Classified National Security Information*
- Committee on National Security Systems (CNSS) Directive No. 502, *National Directive On Security of National Security Systems*
- DOD 5220.22-M, *National Industrial Security Program Operating Manual*
- DOE O 470.4B, *Safeguards and Security Program*
- DOE O 471.6, *Information Security*
- DOE O 473.3, *Protection Program Operations*
- DOE O 472.2, *Personnel Security*
- DOE O 475.2A, *Identifying Classified Information*
- EO 12968, *Access to Classified Information*
- EO 13526, *Classified National Security Information*
- EO 13549, *Classified National Security Information Program for State, Local, Tribal, and Private Sector Entities*
- NSD 52, *National Policy for the Security of National Security Telecommunications and Information Systems*
- NSD 84, *Safeguarding National Security Information*

SAMPLE DOCUMENT LIST

The following documents may be reviewed during the assessment:

- Training records for personnel with information security responsibilities
- Information security procedures
- Classification guidance
- Local site-specific policy
- SSP
- Specific S&S plans
- Unclassified controlled information procedures
- Recent findings and associated CAPs
- Recent IOSC, root cause analysis, and CAPs

SAMPLE INTERVIEW CANDIDATES

Interview candidates may include the following:

- CO

- CMPC program manager, custodians, and control station operators
- S&S director
- Users of classified matter and unclassified controlled information
- Cyber security management and staff
- Operation Security (OPSEC) program manager
- TSCMOM
- Inquiry officer(s) handling IOSC.

SAMPLE LINES OF INQUIRY

Suggested lines of inquiry can be used to (1) assist in determining the scope of assessment activities, (2) assist in developing document call lists, and (3) guide the interview process. Lines of inquiry may include:

1. How is information security guidance disseminated to the facility personnel?
   - Are approved information security guidance and procedures disseminated in a timely manner to appropriate staff?

2. How is classification guidance disseminated to the DCs involved in classified projects?
   - Is approved classification guidance provided to DCs in a timely manner?
   - Are staff working on classified projects made aware of requirements for having documents reviewed by their DCs?

3. What findings were given 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?
   - Are corrective actions effective in preventing the reoccurrence of the findings?

4. What incidents have been reported involving the protection of classified information and unclassified controlled information?
   - Is there a trend?
   - Is the root cause analysis effective in addressing the issue and developing an effective CAP?
   - Are corrective actions effective in preventing the reoccurrence of these types of incidents?

5. What kind of training is provided to generators, users, and control station operators?

6. How are information system requirements funneled into security education and awareness?

7. How is information security integrated into overarching S&S planning documents and other topical area plans?

8. Do SSP documents adequately address the information security program?

9. How is unclassified controlled information guidance disseminated to facility personnel?
   - Does the guidance appropriately address the generating, marking, and storage of unclassified controlled information?

- Is the protection of unclassified controlled information effectively addressed during surveys and self-assessments of the facility?

TECHNICAL SURVEILLANCE COUNTERMEASURES

SUBTOPICAL AREAS: TSCM

Sub-elements include:

- None

CURRENT DIRECTIVES AND REFERENCES

The following references apply to TSCM:

- 32 CFR 149, *Policy on Technical Surveillance Countermeasures*
- 32 CFR 2001, *Classified National Security Information*
- DOE O 470.4B, *Safeguards and Security Program*
- DOE O 473.3, *Protection Program Operations*
- DOE O 471.6, *Information Security*
- DOE O 475.1, *Counterintelligence Program*
- DOE-STD-1123-2009, *Safeguards and Security General Technical Base Qualification Standard*
- DOE-TD-1171-2009, *Safeguards and Security Functional Area Qualification Standard*
- DOE TSCM Annex (classified)
- EO 12333, *United States Intelligence Activities*
- Intelligence Community Directive (ICD) 702, *Technical Surveillance Countermeasures*

SAMPLE DOCUMENT LIST

Documentation to be reviewed may include the following:

- Formal assignments of 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 recertification records
- Local TSCM awareness education program
- Equivalencies/exceptions to DOE TSCM directives the facility may have pending and/or approved

SAMPLE INTERVIEW CANDIDATES

Interview candidates may include the following:

- DOE TSCMOM

- Contractor TSCMO(s)
- TSCM team manager and TSCM technicians

SAMPLE LINES OF INQUIRY

Suggested lines of inquiry can be used to (1) assist in determining the scope of assessment activities, (2) assist in developing document call lists, and (3) guide the interview process. Lines of inquiry may include:

1. Are local TSCM capabilities available and sufficient to detect, deter, and/or nullify technical penetrations and hazardous conditions? If not, is a signed MOU to provide for appropriate TSCM support with another DOE site approved and coordinated through the TSCM program manager?
   - What procedures are followed to request TSCM services or report TSCM concerns?
   - Are an appropriate number of contractor TSCMOs assigned to provide for effective management and coordination of local TSCM services?
   - Are complete and up-to-date TSCM reference documents and memoranda, including DOE TSCM Manual and classified TSCM Annex, available?
   - What reporting procedures of a TSCM penetration or hazard are in place? Are these procedures included in the site TSCM awareness briefing?

2. Has a TSCMO been appointed in writing?
   - Have TSCMOs received appropriate training concerning TSCM services and activities?

3. What kind of training has been provided to the TSCM team members?
   - Is there an annual recertification eligibility of TSCM technicians sent to TSCM program manager?
   - Does TSCM technician training include safety, administrative, and specialized technical course (e.g., telephony, OPSEC, counterintelligence (CI), information systems)?

4. Is there a TSCM awareness program?

5. Is there a list of all facilities that meet TSCM service criteria?
   - Are TSCM assets effectively used 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?
   - When was the last TSCM service performed?

OPERATIONS SECURITY

SUBTOPICAL AREAS: OPSEC

Sub-elements include:

- None

CURRENT DIRECTIVES AND REFERENCES

The following references apply to OPSEC:

- DOD 5220.22-R, *Industrial Security Regulation*
- DOE O 471.6, *Information Security*
- NSD 298, *National Operations Security Program*

SAMPLE DOCUMENT LIST

Specific OPSEC program documentation to be reviewed may include:

- Local OPSEC plan (reviewed and updated at least every 12 months)
- Local OPSEC awareness program files
- OPSEC reviews (of sensitive activities and facilities)
- Local threat statement
- Local critical information list
- Counter-Imagery Program Plan (if applicable)
- Results of internet website assessments

SAMPLE INTERVIEW CANDIDATES

Interview candidates may include the following:

- OPSEC POC
- CI program manager
- OPSEC working group chairperson
- S&S director/manager
- Program/project manager of selected sensitive activities

SAMPLE LINES OF INQUIRY

Suggested lines of inquiry can be used to (1) assist in determining the scope of assessment activities, (2) assist in developing document call lists, and (3) guide the interview process. Lines of inquiry may include:

1. Is an OPSEC program implemented to cover each program office, site, and facility to ensure the protection of classified and unclassified controlled information?
   - How are OPSEC concerns being disseminated to the staff of the facility?
   - Has a POC been established with overall OPSEC responsibilities for each site, facility, and program office?
   - Has an OPSEC assessment schedule been developed? When was the last assessment conducted?

2. Does the OPSEC POC participate in the development of local implementation training and/or briefings tailored to the job duties of the individual employees?

    - What OPSEC training has been provided to the POC?

3. 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 Special Access Program (SAP) information within their boundaries?

    - Are assessments of websites conducted? How are they done? Has a process been established to conduct these assessments?
    - Have CI and indicator lists been developed? Are they current?
    - Is there a review process for looking at website information prior to posting/making public? Who conducts the review and has criteria been established?

CLASSIFICATION GUIDANCE

SUBTOPICAL AREAS: CLASSIFICATION GUIDANCE

Sub-elements include:

- None

CURRENT DIRECTIVES AND REFERENCES

The following references apply to Classification Guidance

- 10 CFR 1045, *Nuclear Classification and Declassification*
- 32 CFR 2001, *Classified National Security Information*
- 32 CFR 2004, *National Industrial Security Program, Directive No. 1*
- DOE O 475.2A, *Identifying Classified Information*
- DOE O 471.6, *Information Security*
- EO 13526, *Classified National Security Information*
- Information Security Oversight Office (ISOO) Notice 2013-01, *Further Marking Guidance on Commingling North Atlantic Treaty Organization and Classified National Security Information*

SAMPLE DOCUMENT LIST:

The following documents may be reviewed during the assessment:

- Number of DCs and DDs
- Appointment letters
- Training records and materials
- Procedures
- Classification guidance
- Reviews, inspections, and appraisals by other organizations
- List of UCNI ROs

SAMPLE INTERVIEW CANDIDATES

Interview candidates may include the following:

- CO
- DCs and DDs
- Users of classified matter
- CMPC POCs and custodians
- UCNI ROs

SAMPLE LINES OF INQUIRY

Suggested lines of inquiry can be used to (1) assist in determining the scope of assessment activities, (2) assist in developing document call lists, and (3) guide the interview process. Lines of inquiry may include:

1. How is classification guidance disseminated?
   - How is classification guidance issued to DCs?

  - Is current classification guidance on hand for each of the facilities classified projects?

2. Does the facility have DCs appointed in writing?
    - Have all DCs been appointed in writing from the appropriate official?

3. Have DCs been appropriately trained?
    - How is DC training provided and at what frequency?

4. How do the site personnel know where to go to get information reviewed for classification?
    - Are reviews being conducted in a timely manner?

CLASSIFIED MATTER PROTECTION AND CONTROL

SUBTOPICAL AREAS: CMPC

Sub-elements include:

- Control of classified matter
- SAPs and intelligence information

CURRENT DIRECTIVES AND REFERENCES

The following references apply to CMPC:

- 10 CFR 1016, *Safeguarding of Restricted Data*
- 10 CFR 1044, *Security Requirement for Protected Disclosures under Section 3164 of the National Defense Authorization Act for Fiscal Year 2000*
- 32 CFR 2001, *Classified National Security Information*
- DOD 5220.22-M, *National Industrial Security Program Operating Manual*
- DOE O 470.4B, *Safeguards and Security Program*
- DOE O 471.6, *Information Security*
- DOE O 471.5, *Special Access Programs*
- DOE O 475.2A, *Identifying Classified Information*
- DOE O 481.1C, *Work for Others (Non-Department of Energy Funded Work)*
- EO 12968, *Access to Classified Information*
- EO 13526, *Classified National Security Information*
- NSD 84, *Safeguarding National Security 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)
- SSP
- Recent self-assessment, survey reports, security appraisals, and inspections
- 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
- CAPs for recent findings and IOSCs

SAMPLE INTERVIEW CANDIDATES

Interview candidates may include the following:

- CMPC POC
- 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 (SCIF) manager
- Cyber security management and staff

SAMPLE LINES OF INQUIRY

Suggested lines of inquiry can be used to (1) assist in determining the scope of assessment activities, (2) assist in developing document call lists, and (3) guide the interview process. Lines of inquiry may include the following.

Control of Classified Matter

1. What procedures are used to enforce limiting access, need-to-know, and handling classified documents outside storage locations?

2. What is the process for receipts not returned within the suspense period? How are follow-up actions documented?

3. How are fax transmissions documented for verbal receipts?

4. What are the hand-carry procedures?
   - How are staff identified and approved for hand-carry?
   - What kind of contingency plans are in place?

5. How is information from other government agencies handled?

6. What procedures are available for intrasite messengers or post office couriers to ensure they constantly attend and control classified matter?

7. What is the notification process for suspensions/revocations of access authorizations?

8. When was the last inventory conducted of accountable matter? What were the results?

9. Is classified email a common practice at this facility?

10. How are classified document facilities managed (is there overnight storage, how is classified waste handled)?

11. Are records maintained as required for accountable documents through the time they are physically destroyed?

12. Where are documents identified for destruction stored?
    - What protection measures are in place?

13. Do the control station procedures include requirements for handling drafts/working papers and having them reviewed for retention after six months?

SPECIAL ACCESS PROGRAMS AND INTELLIGENCE INFORMATION

1. Does the facility have SAPs?

2. Have the SAPs been properly registered with DOE- HQ using the FDAR process?

3. Do all persons with access to SAPs have proper clearance and briefings?
   - How is need-to-know for SAPs determined?

4. How is security managed for SAPs at this facility?
   - Are there specific security plans and operating procedures associated with SAPs?

5. How are intelligence-related efforts coordinated with the Office of Intelligence?

6. Has an individual been designated as being responsible for procurements involving field intelligence elements and/or SCI?

DC/DD/RO Questionnaire

Name: ____ Date: __________

Position: ______________________________________

The following are suggested questions that can be used to trigger discussions/other questions when interviewing individuals authorized to classify or declassify information.

1. What authorities do you have (circle all that apply)?

   DC DD RO

2. Do you have a letter authorizing your authority as a:

   DC Yes No (inspect copy)

   DD Yes No (inspect copy)

   RO Yes No (inspect copy)

3. What subject authorities have been granted to you by your CO?

   DC DD RO

   a. Are these subject authorities sufficient for information being reviewed?

   b. Are you comfortable with these authorities?

   c. Are there additional areas needed?

4. Is your training current?

   DC Yes No NA

   DD Yes No NA

   RO Yes No NA

5. What classification guides do you have in your possession (list guides including revisions and issue date)? Do you have a DOE-HQ-issued classification guide index?

   a.

   b.

   c.

   Are these guides current? Yes No Don’t know

6. Have you used or heard of the Classification Guides System?

   Yes No

   Discuss: ____

7. Do you have access to a classified computer system having disk reading and printing capabilities?

   Yes No

   Discuss response: ____________________

8. Have you met with the your CO or a representative from the Classification Office to discuss classification issues within the last month, three months, six months, a year?

   Yes No

   If Yes, obtain feedback – positive and negative

   If No, why not: ____________________

9. Do you feel comfortable contacting your CO?

   Comment: ____________________

10. Have you attended a CO's update/training meeting?

    Yes No

    If Yes, when: ____________________

    If No, why not: ____________________

11. When did you perform the last review for?

    Classification ____________

    Declassification __________

    UCNI __________________

12. Did you feel comfortable with making this review/decision?

    Yes No

    Comments: ____________________

13. Have you made or rejected reviews outside your authority?

    When: ____________________

    Why/Reason: ____________________

14. Have you portion marked a document?

    Yes No

15. Did you feel comfortable doing this portion marking task?

    Yes No

    Discuss: ____________________

16. Have you applied all required classification markings or remarked a declassified document?

    Yes No NA

    Discuss: ____________________

17. Does your individual performance appraisal/evaluation contain a statement about your being a DC, DD, and/or RO?

    Yes No

18. Does your management support your classification authority?

    Yes No

    Discuss: ____

19. Have you received information/training on the following:

    Official Use Only Yes No

    Export Control Information Yes No

    Discuss: ____

20. Overall Comments: ____

Document Generation Test Performance Test

Objective: To determine whether personnel responsible for generating classified documents are doing so in accordance with DOE requirements.

Scenario: The team member selects a sample of personnel who normally generate classified documents. These personnel are asked to generate simulated classified documents and are observed to determine whether they follow required procedures for tracking, controlling, obtaining classification review, marking, and accounting for (as applicable) these documents.

Document Marking Test Performance Test

Objective: To determine whether personnel responsible for marking classified documents are doing so in accordance with DOE requirements.

Scenario: To specifically verify the test participant's ability to mark classified documents, the team member gives the classified document handlers several simulated classified documents along with a complete description of the nature and contents of the documents, such as classification level, category, and authority. Each test participant is then asked to properly document and mark the documents.

Variation: Employ the same scenario as above, but substitute microfiche, viewgraphs, messages/cables, or other media for a typical paper document.

Intrasite Cross-Check Performance Test

Objective: To verify that documents sent within a site can be produced, or their disposition determined, at the receiving site organization.

Scenario: The team member uses an organization's document accountability records to identify classified documents that were recently transmitted to another organization within the same site. The team member then verifies that the receiving organization's accountability log reflects the receipt and that the organization can produce (1) the documents themselves, (2) their destruction forms, or (3) their transmittal slips.

Custodian Receipt Performance Test

Objective: To determine whether those receiving classified matter follow appropriate custodian receipt procedures.

Scenario: To verify appropriate custodian receipt procedures, a sample of document custodians who normally receive classified matter is selected for testing. Each test participant is sent a simulated Secret document through normal channels. The team member must then ascertain whether the recipient properly signs receipts for, checks, and enters the document into accountability.

Variations:

1. Send to a test participant a simulated Secret document that was incorrectly transmitted, incorrectly or incompletely marked, or is missing pages. Verify his/her response (e.g., to return the document, issue an infraction, or initiate other action).
2. Prepare a classified document to be sent off site through classified mail. The document prepared should indicate a classification level/category that the receiving facility is not authorized to accept.

Reproduction Performance Test

Objective: To determine whether classified documents are reproduced in accordance with DOE directives.

Scenario: The team member selects a sample of personnel for testing who normally reproduce classified documents. Test participants are asked to demonstrate their procedures for duplicating classified documents (genuine or simulated) to determine whether they comply with the requirements for using approved (and posted) locations/equipment, running the appropriate number of blanks after duplicating, treating those blanks as classified waste, controlling documents for reproduction if they are normally dropped off at a central reproduction station, and documenting/marking reproduced copies.

Variations:

1. Use the same scenario but instead of a typical paper document, use microfiche, viewgraphs, blueprints, or any other type of medium containing classified information.
2. Carry out the scenarios at the inspected site's print shop, photo lab, or other facility tasked with reproducing classified information.
3. Submit improperly or incompletely marked, simulated classified documents for reproduction and determine whether the discrepancies are noted.
4. Select a sample of personnel that do not regularly reproduce documents to see if they are familiar with their local site procedures regarding reproduction of classified documents.

Repository Check Performance Test

Objective: To determine whether repositories used to store classified documents are being routinely checked and ascertain whether appropriate actions are taken if a repository is left unsecured.

Scenario: Team members visit selected locations in which classified matter is stored and/or used. Team members arrange with someone having access to a repository to leave it open (simulated by using a sign or by substituting authentic classified documents with simulated ones). Actions by those responsible for security checking the repository are observed. Note: Scenario requires safety plan and PF coordination.

Document Accountability Performance Test Plan – Front Check

Objective: To evaluate the accuracy of the DOE San Diego Operations Office document accountability system and determine whether documents are protected, stored, and marked in accordance with DOE requirements.

System Description: The document accountability is maintained using a manual system of document receipts. Document control tickets may reflect more than a single document. Tickets are filed in the mail room, which also provides centralized dispatch and control. Individual custodians also maintain records of their holdings. Although individual custodians may have entered holdings in their personal computers, no computer enumeration of a master list of active holdings or system-generation of random samples is possible.

Sampling Technique: The San Diego Operations Office is unable to provide the total number of documents contained in active holdings. They estimate 2,400 control tickets are in use to reflect active holdings, but some tickets represent multiple copies of documents.

The Office of Independent Oversight selects a random sample of 200 documents by computer generating a list of random numbers reflecting document control tickets. Corresponding control tickets are then examined and documents reflected on the selected tickets are used as the inspection sample for the front check of the accountability system.

Scenario: Selected documents are reviewed at their storage locations or at a central location as appropriate. Each is checked to ensure it is the item described in the accountability records. Additionally, documentation, markings, dates, titles, and pages are checked to determine compliance with DOE requirements. Each repository is also inspected for compliance with DOE storage requirements.

Safety Plan: Not required.

Classified Transmittal Performance Test Plan

Objective: This test is conducted to determine whether classified matter is transferred to and from the U.S. Postal Service in accordance with requirements.

Scenario: Transfer procedures are reviewed by tracking certified and registered mail from its receipt at the U.S. Post Office until it reaches its final custodian. Observation includes receipt from postal personnel, transportation, delivery, entry into the appropriate accountability system, and custodian receipt procedures, as applicable.

Safety Plan: Not required.

Classified Document Destruction Performance Test Plan

Objective: To determine whether classified documents are destroyed in accordance with DOE directives.

Scenario: Team members observe personnel destroying classified matter using routine local procedures. Should destruction of classified not be planned during the assessment, site personnel are asked to describe procedures or perform actions on simulated classified matter.

Safety Plan: Not required.

Data Collection Sheet: Previously Identified Deficiencies

CLASSIFICATION

CLASSIFIED MATTER PROTECTION AND CONTROL

Previously Identified Deficiencies

Deficiency	Date Identified	Discovered by	Corrective Action	Est. Completion Date	Validated by

CLASSIFICATION

MAIL ROOM

Location: __________________ Operated by: __________________

What are the clearance levels (Q, L, Uncleared) of individuals operating the mail room or making the mail deliveries?

Accountability (Receipt and Transmittal, Pickup and Delivery):

Delivery Procedures from U.S. Post Office:

Delivery Procedures to U.S. Post Office:

Physical Protection between Post Office and Site:

Access Controls:

Storage (in Mail Room): Is accountable matter stored in the mailroom? Overnight?

How are classified mailing addresses verified in SSIMS? If kept as a record copy, how often is it updated?

Physical Protection during Internal Delivery: Inspect the mail delivery vehicle.

Other Comments:

Data Collection Sheet: Security Infraction Program

Location: ________________________ Responsible Organization: ______________________________

Program Procedures/Directives: Does the site use an internal tracking system?

DOE HQ Reporting: Does DOE and/or the contractor use SSIMS for reporting this information? If so, who is responsible for communicating closure to HQ?

Internal Reporting: Include how incident reporting is handled off hours.

Investigation: Include all matters involving foreign visitors or assignees

Appropriate Management Involvement?

Disciplinary Schedule?

Appropriate (Disciplinary) Action?

Trend Analysis?

Corrective/Preventive Actions:

Number of Inquiry Officials: Include a review of their training records and appointment letters.

Required Reports Submitted?

Other Comments:

3.5 PERSONNEL SECURITY

PERSONNEL SECURITY

- Subtopical Areas
- Common Deficiencies

Subtopical areas will address:

- Current Directives
- Potential Documents for Review
- Potential Interview Candidates
- Lines of Inquiry
- Performance Tests

SUBTOPICAL AREAS

- Access Authorization (Personnel Clearances)
- HRP
- Control of Classified Visits
- S&S Awareness

COMMON DEFICIENCIES

The following is a sample of common deficiencies identified by the Office of Independent Oversight (now the Office of Security and Cyber Evaluations) in the 2009 document, *Personnel Security Inspectors Guide*. By reviewing the list of common deficiencies during the planning phase, assessors can be alert for similar deficiencies during data gathering activities.

- Failure to complete annual security refresher briefing
- Hosting FN visitors prior to or without approval
- Changes in status of cleared personnel
- Inappropriate type of clearance
- Questionable clearance requests/justification
- Incomplete information
- Lack of timely and thorough screening or analysis
- Failure to report information of personnel security interest
- Inadequate briefing content and material
- Inadequate HRP communication/coordination
- Inadequate HRP drug and alcohol testing
- Inadequate HRP medical assessment
- Inadequate reporting of HRP concerns
- Inadequate notice of FN visits
- Deterioration of escort procedures
- Inadequate security plans for visits

ACCESS AUTHORIZATIONS

SUBTOPICAL AREAS: ACCESS AUTHORIZATIONS

Sub-elements include:

- None

CURRENT DIRECTIVES AND REFERENCES

The following references apply to Access Authorizations:

- 10 CFR, Part 710, *Criteria and Procedures for Determining Eligibility for Access to Classified Matter or Significant Quantities of Special Nuclear Material*
- 32 CFR 2001, *Classified National Security Information*
- DOD 5220.22-M, *National Industrial Security Program Operating Manual*
- DOE O 243.1B, *Records Management Program*
- DOE O 472.2, *Personnel Security*
- DOE O 470.4B, *Safeguards and Security Program*
- EO 12968, *Access to Classified Information*
- EO 13549, *Classified National Security Information Program for State, Local, Tribal and Private Sector Entities*
- 5 USC 552a, *Records Maintained on Individuals*

SAMPLE DOCUMENT LIST

The following documents may be requested and reviewed:

- Access authorization requests
- Personnel security files:
  - Has proof of U.S. citizenship been validated using acceptable evidence?
  - Have the appropriate preprocessing checks been completed?
  - If access authorizations are required for both DOE and another federal agency, has the DOE request been requested, processed, and granted first?
  - Have the appropriate forms been completed and submitted?
  - Do procedures include the prohibition of individuals to access classified information/matter or SNM until the DOE has granted, reinstated, extended, or transferred an active access authorization?
  - Are the records current and do they include all records maintenance items required per the Manual?
- Local procedures
- Contractor access authorization requests (justifications)
- Nondisclosure agreement forms
- Training records
- Questionnaires for national security positions, SF-86, and fingerprint cards
- 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
- Reciprocal access authorization documentation

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 LINES OF INQUIRY

Suggested lines of inquiry can be used to (1) assist in determining the scope of assessment activities, (2) assist in developing document call lists, and (3) guide the interview process. Lines of inquiry may include:

1. Is the number of access authorizations appropriate for the mission of the facility?
   - Is proper justification required for all access authorizations? Is the approval appropriate?
   - How often are rejustifications required?
   - Are regular reviews conducted of access authorizations for subcontractors/consultants?

2. Is the need for an access authorization determined prior to processing?
   - What constitutes valid need?

3. What constitutes the type of access authorization to be processed (i.e., are the category and level of classified information/matter or category of SNM for each level requested defined)?

4. What are the criteria for processing interim access authorizations?

5. 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?

6. What procedures are in place to ensure that access authorizations are terminated for individuals who terminate employment or transfer to a position not requiring an access authorization?

7. Are indices checks completed prior to all visits and assignments that involve FNs from sensitive or terrorists countries, are concerned with sensitive subjects, and/or include access to security areas?

SUBTOPICAL AREAS: HRP

Sub-elements include:

- None

CURRENT DIRECTIVES AND REFERENCES

The following references apply to HRP:

- 10 CFR, Part 707, *Workplace Substance Abuse Programs at DOE Sites*
- 10 CFR, Part 710, *Criteria and Procedures for Determining Eligibility for Access to Classified Matter or Significant Quantities of Special Nuclear Material*
- 10 CFR, Part 712, *Human Reliability Program*
- DOE O 470.4B, *Safeguards and Security Program*
- DOE O 473.3, *Protection Program Operations*
- DOE O 474.6, *Information Security*
- DOE O 472.2, *Personnel Security*
- DOE O 474.2, *Material Control and Accountability*

SAMPLE DOCUMENT LIST

The following documents may be requested and reviewed:

- Implementation schedule
- Training records/materials
- Drug testing/handling procedures
- Drug testing records
- Random test procedures
- Site implementation plans, policies, 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 SF-86, signed releases, etc.?
  - 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 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 LINES OF INQUIRY

Suggested lines of inquiry can be used to (1) assist in determining the scope of assessment activities, (2) assist in developing document call lists, and (3) guide the interview process. Lines of inquiry may include:

1. Has a formal process been established for HRP?
   - Has the program been reviewed and approved by DOE?
   - Does the site have an HRP implementation plan?

2. Have program responsibilities been formally assigned?
   - Are supervisors aware of their responsibility for reporting any security concerns to the appropriate officials, and if necessary, taking immediate action?

3. Is there a systematic process for identifying HRP positions that is consistent with policy and are these positions reflected in the SSP?
   - Does the system ensure that vacated HRP positions are filled in a timely manner and that supervisors are notified when positions become vacant?
   - Do individuals in or applying for an HRP position undergo a security review and clearance determination prior to being assigned an HRP position?
   - Do all employees have a Q access authorization prior to assuming the duties of an HRP position?
   - Is there a process that ensures that all annual evaluations, assessments, and determinations are completed for each individual enrolled in the HRP?

4. Have HRP drug testing procedures been developed and implemented that provide for random drug testing of staff in HRP-designated positions?
   - What is the rate of random drug testing?
   - Are appropriate security measures in place concerning selection for drug testing and is there a continuous chain of custody for samples?

CONTROL OF CLASSIFIED VISITS

SUBTOPICAL AREAS: CONTROL OF CLASSIFIED VISITS

Sub-elements include:

- None

CURRENT DIRECTIVES AND REFERENCES

The following references apply to Classified Visits:

- DOD 5220.22-M, *National Industrial Security Program Operating Manual*
- DOE O 470.4B, *Safeguards and Security Program*
- DOE O 472.2, *Personnel Security*
- DOE O 473.3, *Protection Program Operations*
- DOE O 474.6, *Information Security*
- DOE O 475.2A, *Identifying Classified Information*
- EO 12968, *Access to Classified Information*

SAMPLE DOCUMENT LIST

Documentation to be reviewed may include the following:

- Requests for Sigma access
- Processes and procedures (who is authorized to approve the requests)
- Visitor control logs
- Local visitor control procedures
- Do procedures address verification of visitors' identity, programmatic need-to-know, and is clearance (access authorization) equal to or greater than the classification of the information or matter to which access is being requested?
- Are access limitations addressed? How are controls enforced for access limitations?
- Are visit requests submitted at least 15 working days in advance?
- Procedures for urgent or rush requests
- Procedures for emergency visits
- Security infraction records

SAMPLE INTERVIEW CANDIDATES

Interviews should be conducted to determine whether the requirement for an effective need-to-know policy regarding National Security Information, Restricted Data (RD), Formerly Restricted Data (FRD), and nuclear weapon data is fully understood. Interview candidates may include the following:

- 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

SAMPLE LINES OF INQUIRY

Suggested lines of inquiry can be used to (1) assist in determining the scope of assessment activities, (2) assist in developing document call lists, and (3) guide the interview process. Lines of inquiry may include:

1. Is access to facilities adequately controlled?
   - Is there an effective Foreign National Visits and Assignments (FNVA) program in place?
   - Are badges adequately issued and controlled?
   - Are knowledgeable escorts utilized as appropriate?
   - Is sensitive information adequately protected, i.e., are controls in place to prevent FNs from accessing sensitive information via the local area network?
   - Are site- and visit-specific security plans used for visitors from sensitive countries?
   - Who approves requests for classified visits?
   - How are vendors and visitors processed? Is there a difference in the way they are processed?

2. What are the responsibilities of an escort?
   - What is the local policy regarding escort-to-visitor ratios?

3. Are visitor logs used at PAs, MAAs, and exclusion areas?

4. Have procedures been developed and implemented for classified visits by DOE employees, contractors, and subcontractors?

5. Are specific procedures developed for individuals from other government agencies who wish to access classified information?

6. When are briefings provided?

SAFEGUARDS AND SECURITY AWARENESS

SUBTOPICAL AREAS: S&S AWARENESS

Sub-elements include:

- None

CURRENT DIRECTIVES AND REFERENCES

The following references apply to S&S Awareness:

- 10 CFR 1017, *Identification and Protection of Unclassified Controlled Nuclear Information*
- 32 CFR 2001, *Classified National Security Information*
- DOD 5220.22-M, *National Industrial Security Program Operating Manual*
- DOE O 470.4B, *Safeguards and Security Program*
- DOE O 471.1B, *Identification and Protection of Unclassified Controlled Nuclear Information*
- DOE O 471.3, *Identifying and Protecting Office Use Only Information*
- DOE O 473.3, *Protection Program Operations*
- DOE O 474.6, *Information Security*
- DOE O 472.2, *Personnel Security*
- DOE O 475.1, *Counterintelligence Program*
- DOE O 475.2A, *Identifying Classified Information*
- EO 13526, *Classified National Security Information*

SAMPLE DOCUMENT LIST

Documentation to be reviewed may include the following:

- Lesson plans for the initial, comprehensive, refresher, and termination briefings
  - 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 DOE O 470.4B for each briefing?
  - Are briefings given prior to assuming duties or accessing applicable information?
- Instructional aids (includes student handouts)
- S&S awareness coordinator appointment letter
- Attendance records
- Evaluation records
- Supplemental awareness tools (posters, newsletters)
- Sampling of classified information nondisclosure agreements (SF-312) to verify they are appropriately executed before access to classified information or matter is granted
- Security infraction and violation records
- Applicable procedures
  - Do procedures include appropriate notification for failure or refusal to complete an SF-312?
  - Do procedures include all appropriate briefings required by DOE O 470.4B?
- Review records must be maintained to provide an audit trail verifying an individual's receipt of the briefings
  - Are completed SF-312s maintained on all individuals completing the comprehensive briefing?
  - Is DOE F 5631.29 (or written notice) used to document completion for the termination briefing?

- Are lesson plans and records of supplementary activities maintained?
- Are retention and storage of the documents done in accordance with DOE O 470.4B?

SAMPLE INTERVIEW CANDIDATES

Interview candidates may include the following:

- S&S manager/director
- Security awareness coordinators
- Security education training attendees
- OPSEC manager

SAMPLE LINES OF INQUIRY

Suggested lines of inquiry can be used to (1) assist in determining the scope of assessment activities, (2) assist in developing document call lists, and (3) guide the interview process. Lines of inquiry may include:

1. Are employees knowledgeable of their S&S responsibilities?
   - Are meaningful briefings/training provided to staff in a frequency appropriate to their responsibilities?
   - When are attendance records kept?
   - When are evaluation or critique records completed to ensure the information provided as part of S&S awareness is meaningful, adequate, and understood by staff?

2. Do the parameters of the program include coverage for subcontractors?

3. Is the comprehensive briefing conducted after the clearance has been granted?
   - Is a security badge permitting unescorted access to a security area issued only after attendance at the comprehensive briefing?

4. Have training approval programs been implemented to ensure the standardization of S&S training provided onsite?
   - Do individuals assigned the responsibility to coordinate and present S&S awareness briefings possess the proper skills and knowledge?
   - What types of training records are kept relative to S&S training?

5. Do S&S awareness information and/or briefings address site-specific procedures as well as specific topics such as recent espionage cases, foreign intelligence recruitment techniques, incidents and considerations, and S&S threats and vulnerabilities?
   - Has trending been conducted on security incidents/infractions? If so, have trends been included in awareness material?
   - Do awareness briefings/training contain site-specific information and recent threat information?

6. How are the contents of the annual refresher briefing determined?

7. Do all individuals receive a termination briefing when a clearance is no longer required?

SAMPLE WORKSHEETS AND PERFORMANCE TESTS

The following worksheets and sample performance tests can be used during the assessment process to evaluate the status of the personnel security topical area.

PERSONNEL SECURITY: SAFEGUARDS AND SECURITY AWARENESS PROGRAM

Objective: To determine the effectiveness of the facility's S&S awareness program.

Scenario: Review the security education briefings (initial, comprehensive, and refresher). Select a number of employees who have attended the various briefings. The assessment team member interviews these employees with the same questions for the type of briefing they received. (The questions and associated correct answers are prepared during assessment activities as they are site-specific.) The assessment team member completes an evaluation form for each interview (to be prepared during the assessment).

Evaluation Criteria: Ninety percent of the interview questions must be answered correctly.

PRE-EMPLOYMENT DATA COLLECTION FORM

Pre-Employment Check Data Collection Form		
Review Conducted by:		
Name:		
Employer:		
Type of Clearance: DOE Q / L Other Agency Prior/Same Employer		
	Yes	No
Pre-employment Checks Completed		
Credit Check		
Verification of Education		
References Contacted		
Employers Contacted		
Local Law Enforcement Checks		
Evidence of US Citizenship		
Birth Certificate		
Passport		
Derogatory Information Forwarded to DOE/NNSA Date:		
Date Pre-employment Check Completed		
Date Clearance Request Forwarded to DOE/NNSA		

Comments:

CLEARANCE JUSTIFICATION DATA COLLECTION FORM

Name: ____________________________ Job Title: ____

Work Building Number or Facility Designation: ____

Current DOE Security Clearance Level: □ "Q" □ "L"

1. Approximately how long have you possessed a DOE security clearance?

   a. less than 6 months: □
   b. 6 months to 1 year: □
   c. 1-3 years: □
   d. 3-5 years: □
   e. longer than 5 years: □

2. Does your job require you to handle or use classified information?

   Yes: □ No: □

   If Yes, how often and last time: ____

   If Yes, please provide the following additional information by checking all boxes that apply.

   Classification level of the information: □ Top Secret □ Secret □ Confidential
   Category of the classified information: □ Restricted Data □ NSI

   Identify the **primary** location (building/facility) where you handle or use classified information:

   ____

3. Does your job require you to work with SNM?

   Yes: □ No: □

   If Yes, how often and last time: ____

   If Yes, please provide the following additional information by checking all boxes that apply.

   Category of SNM: □ Cat I □ Cat II □ Cat III □ Cat IV

   Identify the **primary** location (building/facility) where you handled (SNM):

   ____

4. Does your work require you to access a limited, exclusion, protected or material access area?

   Yes: □ No: □

   If Yes, how often and last time: ____

5. Do you attend meetings or conferences that include the discussion of classified information?

   Yes: □ No: □

   If Yes, how often and last time: ____

   If Yes, please provide the following additional information by checking all boxes that apply.

   Level of the classified information: □ Top Secret □ Secret □ Confidential
   Category(ies) of the classified information: □ Restricted Data □ NSI

   Identify the **primary** location (building/facility) where you attend a meeting, conference or participate in classified discussions: ____

Purpose of the meeting: ____

[After conducting this interview, complete a review of the last clearance justification/request (recording the results of the review on the following table) that is filed in the individual's personnel security file. The review is intended to determine if there is consistency between the actual work being performed and the clearance justification/request.]

Clearance Justification/Request

DOE PERSONNEL SECURITY FILE REVIEW
OF LATEST CLEARANCE JUSTIFICATION/REQUEST

Name:____
Contract Number:______________________________________

Last Clearance Justification/Request Date:____________

Clearance Level Requested: □ "Q" □ "L"

Requested Clearance Justification Based On Access To:

Protected Area: □ Yes □ No

Material Access Area: □ Yes □ No

SNM: □ Yes □ No

Highest Category: □ Cat I □ Cat II □ Cat III □ Cat IV

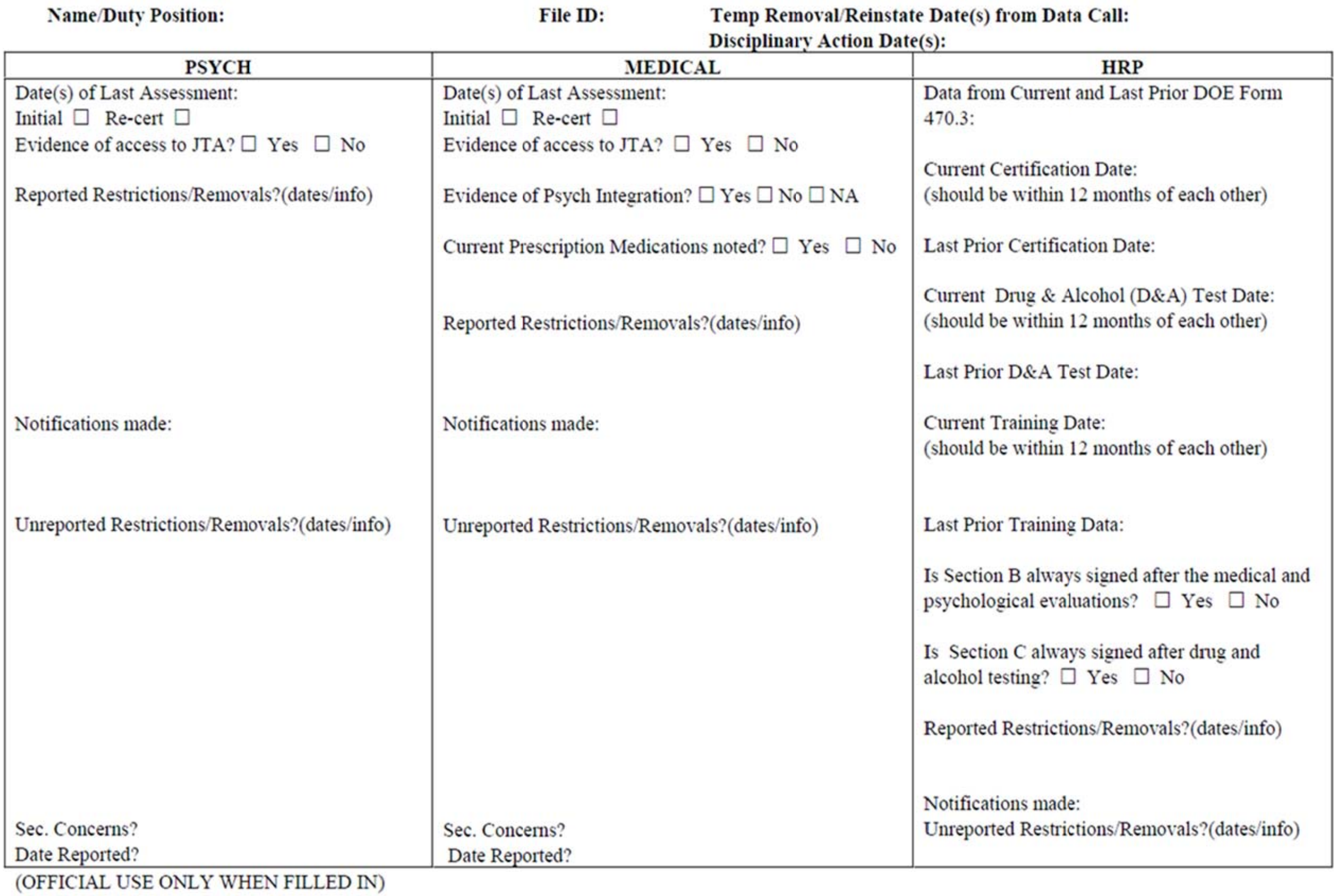
Limited Area: □ Yes □ No

Exclusion Area: □ Yes □ No

Classified Information: □ Yes □ No

Highest Level: □ TS □ S □ C

Category(s): □ RD □ FRD □ NSI



Name/Duty Position: **File ID:** **Temp Removal/Reinstate Date(s) from Data Call:**
Disciplinary Action Date(s):

PSYCH	MEDICAL	HRP
Date(s) of Last Assessment: Initial □ Re-cert □ Evidence of access to JTA? □ Yes □ No Reported Restrictions/Removals?(dates/info) Notifications made: Unreported Restrictions/Removals?(dates/info) Sec. Concerns? Date Reported?	Date(s) of Last Assessment: Initial □ Re-cert □ Evidence of access to JTA? □ Yes □ No Evidence of Psych Integration? □ Yes □ No □ NA Current Prescription Medications noted? □ Yes □ No Reported Restrictions/Removals?(dates/info) Notifications made: Unreported Restrictions/Removals?(dates/info) Sec. Concerns? Date Reported?	Data from Current and Last Prior DOE Form 470.3: Current Certification Date: (should be within 12 months of each other) Last Prior Certification Date: Current Drug & Alcohol (D&A) Test Date: (should be within 12 months of each other) Last Prior D&A Test Date: Current Training Date: (should be within 12 months of each other) Last Prior Training Data: Is Section B always signed after the medical and psychological evaluations? □ Yes □ No Is Section C always signed after drug and alcohol testing? □ Yes □ No Reported Restrictions/Removals?(dates/info) Notifications made: Unreported Restrictions/Removals?(dates/info)

(OFFICIAL USE ONLY WHEN FILLED IN)

3.6 MATERIALS CONTROL AND ACCOUNTABILITY

MATERIALS CONTROL AND ACCOUNTABILITY

- Subtopical Areas
- Common Deficiencies

Subtopical areas will address:

- Current Directives
- Potential Documents for Review
- Potential Interview Candidates
- Lines of Inquiry
- Performance Tests

SUBTOPICAL AREAS

- Program Administration
- Material Accountability
- Material Control

COMMON DEFICIENCIES

The following is a sample of common deficiencies identified by the Office of Independent Oversight (now the Office of Security and Cyber Evaluations) in the 2009 document, *Materials Control and Accountability Inspectors Guide*. By reviewing the list of common deficiencies during the planning phase, assessors can be alert for similar deficiencies during data gathering activities.

- Lack of MC&A participation in VAs
- Deficient authority approvals
- Deficient training program
- Multiple contractors performing MC&A activities
- Deficient MBA categorization
- Deficient performance testing programs
- Lack of root cause analysis of deficiencies
- Deficient internal material transfer practices
- Inadequate shipping/receiving system
- Excessive NMMSS error rates
- MBA categorizations controlled by accounting systems
- Reportable radioactive sealed sources not tracked or reported
- Lack of measurement methods and equipment
- Accountability measurement methods not qualified
- Measurement uncertainties not qualified
- Deficient measurement control programs
- Sampling methods not qualified
- Unmeasured inventory
- Material not amenable to measure not identified in MC&A plan
- Inappropriate warning and alarm limits
- Holdup not included in inventory
- Alternate physical inventory frequency not approved or not appropriate
- MBAs crossing an MAA boundary
- Excessive reliance on the HRP for material surveillance

PROGRAM ADMINISTRATION

SUB-TROPICAL AREA: PROGRAM ADMINISTRATION

Sub-elements include:

- None

CURRENT DIRECTIVES AND REFERENCES

The following references apply to Program Administration:

- 41 CFR 109, *DOE Property Management Regulations*
- *DOE Accounting Handbook*, Chapter 1 and 9
- DOE O 470.4B, *Safeguards and Security Program*
- DOE O 474.2, *Nuclear Material Control and Accountability*
- 42 USC 23, *Atomic Energy Act of 1954*

SAMPLE DOCUMENT LIST

Documentation to be reviewed may include the following:

- MC&A plans and procedures
- SSP and VAs
- Deviations and exceptions
- Organization charts
- Training records, lesson plans
- MC&A assessment program plans
- Internal assessments and CAPs
- MC&A performance testing program 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 SSP/VA documents
- Personnel responsible for MC&A internal reviews and assessments

SAMPLE LINES OF INQUIRY

Suggested lines of inquiry can be used to (1) assist in determining the scope of assessment activities, (2) assist in developing document call lists, and (3) guide the interview process. Lines of inquiry may include:

1. 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?

2. Has a nuclear MC&A program that meets the requirements of DOE directives for all special, source, and other nuclear materials on inventory under a three-letter reporting identification symbol (RIS) been implemented?

3. Is the MC&A program implemented on the basis of the graded safeguards concept?
   - Is an MC&A expert included on the VA team?
   - Is the MC&A program documented in an approved MC&A plan and procedure?
   - Is the MC&A plan properly approved and comprehensive?
   - Are procedures developed and documented for characterizing nuclear materials on inventory to determine categories and attractiveness for implementation of the graded safeguards concept?
   - Is the MC&A management official organizationally independent from responsibilities of other programs?

4. Are there sufficient experienced and qualified staff to accomplish the MC&A functions?
   - Has a documented program to ensure that personnel performing MC&A functions are trained and qualified been implemented?
   - Has the training program received approval from the training approval program?
   - Are MC&A procedures consistent and responsibilities clearly defined?

5. Have MC&A loss-detection elements been included in documented procedures for reporting IOSCs?
   - Is occurrence investigation and reporting defined and incorporated into the overall facility program?

6. Has a program to periodically review and assess the integrity and quality of the MC&A program and practices been implemented?
   - Is the internal review and assessment program defined, comprehensive, and on schedule?

7. Have performance requirements for MC&A system elements been documented and a performance testing program implemented?
   - Is the performance testing program active and effective?
   - How does the performance testing program evaluate its materials loss-detection capability and support and verify VAs?

8. Has a measurement control program been implemented to establish nuclear inventory values and to ensure the quality of the nuclear materials database?

9. Has a physical inventory program been developed and implemented to determine the quantity of nuclear materials on hand both by item and in total?

10. How does the accounting system provide a complete audit trail for all nuclear materials from receipt or production through transfer or disposition?

11. 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?

12. 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 SNM has been identified?

13. Are MBA-specific MC&A plans approved, current, and effectively implemented?
    - Have MBAs been categorized and has rollup been evaluated?
    - Have MBA attractiveness levels been determined?

MATERIAL ACCOUNTABILITY

SUBTOPICAL AREAS: MATERIAL ACCOUNTABILITY

Sub-elements include:

- None

CURRENT DIRECTIVES AND REFERENCES

The following references apply to Material Accountability:

- 41 CFR 109, *DOE Property Management Regulations*
- *DOE Accounting Handbook*, Chapters 1 and 9
- DOE O 474.2, *Nuclear Material Control and Accountability*
- DOE O 470.4B, *Safeguards and Security Program*
- DOE O 534.1B, *Accounting*
- U.S.-International Atomic Energy Agency (IAEA) Safeguards Agreement and Protocols

SAMPLE DOCUMENT LIST

Documentation to be reviewed may include the following:

- MC&A plans and procedures related to materials accounting
- Deviations and exceptions
- 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

Meetings should be scheduled and interviews conducted with 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 LINES OF INQUIRY

Suggested lines of inquiry can be used to (1) assist in determining the scope of assessment activities, (2) assist in developing document call lists, and (3) guide the interview process. Lines of inquiry may include:

1. Is shipment/receipt data accurately entered into the accounting system within appropriate timeframes?
    - Are shipper/receiver agreements appropriate?
    - Are limits of error for shipments calculated?
    - Is a shipper/receiver agreement in place for all offsite receipts and shipments?
2. Does the facility meet the NMMSS error rate goals?
3. Is the inventory reconciliation fully documented and supported?
4. Are TID records properly maintained?
5. Are material transfers timely, and are checks and measurements appropriately completed?
6. Are data from measurement systems accurately entered into the accounting system within appropriate timeframes?
7. How have MBAs been designated?
    - Are the MBA boundaries clearly and properly defined?
    - Does the accounting structure assist in 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?
8. Has the facility properly categorized its nuclear material?
    - Is there a documented categorization process?
    - Were all materials considered when category levels were established?
9. Are holdup locations identified and properly recorded for inventory purposes?
10. What role does the accounting system play during inventory?
11. Which records does the system require be input? Are data transcribed? How are laboratory data input?
12. What output formats are used and who receives copies of the reports?
13. Are the required reports being issued in a timely manner?
14. 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?
    - Are transfer procedures complete and appropriately implemented?

15. Is the inventory difference evaluation program thorough and complete?

16. Is confirmation of measured values on internal transfers required? If so, how are they accomplished?

17. How often are measurement instruments calibrated? Do the calibration standards demonstrate traceability?

18. Have the nondestructive assay measurement methods been approved and certified?

19. How is the inventory stratified? Is a wall-to-wall inventory conducted or is some other means used?

20. Is there an approved statistical sampling plan? If so, who approves this plan?

21. How are measurement methods certified?

22. Are adequate controls in place to ensure categorization limits are not exceeded?

23. How are measurements personnel trained and certified?

24. How are transfer forms controlled?

25. Are material items deemed non-amenable to measurement clearly and accurately defined and documented in the MC&A plan?

26. Is there a documented, approved measurement control program?

27. Are the qualification and requalification requirements for measurers identified?

28. Are measurement uncertainties defined?

29. Are statistical sampling plans properly selected and appropriately implemented?

30. Is the propagation of variance calculation done correctly?

31. Are statistical limits appropriate, approved, and used to monitor and correct measurement system performance?

32. Does the sampling process for measurements yield representative samples?

33. Are control limits established and based on proper statistical assumptions?

34. Are standards appropriate for the material types being assayed? Are they traceable to the national measurement base?

35. 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?

36. Are confirmation/verification measurements conducted for shipments and receipts?

37. For liquids processing, are prescribed solution mixing times required prior to taking a sample for accountability measurement?

MATERIAL CONTROL

SUBTOPICAL AREAS: MATERIAL CONTROL

None

CURRENT DIRECTIVES AND REFERENCES

The following references apply to Material Control:

- 41 CFR 109, *DOE Property Management Regulations*
- 48 CFR 952, *DOE Acquisition Regulation Clause*
- *DOE Accounting Handbook*, Chapter 1 and 9
- DOE O 470.4B, *Safeguards and Security Program*
- DOE O 473.3, *Protection Program Operations*
- DOE O 474.2, *Nuclear Material Control and Accountability*
- 42 USC 23, *Atomic Energy Act of 1954*

SAMPLE DOCUMENT LIST

Documentation to be reviewed may include the following:

- Materials containment documentation
- MC&A plans and procedures
- Facility procedures
- Deviations and exceptions
- SSP/VAs
- Material access program plan
- Authorization access lists
- Combination change records
- MBA custodian lists and training records
- Material surveillance procedures
- Portal monitor records and procedures
- Daily administrative check program and procedures
- TID program procedures and records of receipt, disbursement, application, removal, inventory, and destruction
- Internal assessments and CAPs

SAMPLE INTERVIEW CANDIDATES

Documentation to be reviewed may include the following:

- MC&A program manager
- MBA custodians/alternate custodians
- Seals (TID) and forms
- Training personnel
- Portal monitoring staff
- Personnel responsible for MC&A internal reviews and assessments

SAMPLE LINES OF INQUIRY

Suggested lines of inquiry can be used to (1) assist in determining the scope of assessment activities, (2) assist in developing document call lists, and (3) guide the interview process. Lines of inquiry may include:

1. How are keys and combinations to SNM areas controlled?
2. Does the facility have a documented program to provide controls of nuclear material operations relative to MAAs?
3. Are there approved procedures governing MBA-to-MBA and MAA-to-MAA material transfers?
4. What training is provided to MBA custodians? Frequency?
5. What transfer controls are in place?
6. Are documented controls covering nuclear material being used or stored in processing areas?
7. How is access to SNM use and storage locations approved?
8. How is the two-person rule implemented at the facility?
9. Are material custodians prohibited from hands-on SNM functions?
10. Are searches conducted of all persons exiting an MAA?
11. Is a daily administrative check program implemented at the facility?
12. How is the TID program documented and approved?
13. Does the TID program include sample testing of new TIDs to ensure compliance with requirements?
14. Who is responsible for testing and calibrating portal monitors? Are problems corrected in a timely manner?

MC&A SAMPLE WORKSHEETS AND PERFORMANCE TESTS

The following worksheets and sample performance tests can be used during the assessment process to evaluate the status of the MC&A topical area.

DOCUMENT SAMPLING

Objective: This test will determine whether the accounting system is in compliance with all reporting requirements.

Scenario: Randomly select a sample of accounting documents to verify accuracy and completeness and use this sample to physically locate material. (May be used with the tests for accountability, data traceability, and item location.)

Evaluation Criteria:

1. Were all records complete, accurate, and submitted in a timely manner?

2. If discrepancies exist, are they a systemic problem or isolated cases?
3. Does the information in the records agree with the physical inventory?

Vulnerability Assessment Validation Checks

Objective: Determine whether the detection probabilities used by the facility are supported in the VA.

Scenario: Review the VA and select several detection probabilities. Ask the facility to produce the documentation that supports the detection probability.

Evaluation Criteria:

1. Does documentation exist to support the VA detection probability?
2. Does performance testing data support the detection probability that was assigned?
3. Does the facility have an ongoing performance testing program to support the detection probability?

Internal Review and Assessment Program Observations

Objective: Determine whether the facility can perform an internal review by observing an actual assessment.

Scenario: Select an internal review topic and an area to be reviewed. Ask the facility to conduct an internal review. Observe the review or introduce an anomaly by having a finding (using the individual to be reviewed as a trusted agent) to determine whether the internal review is effective in detecting that finding.

Evaluation Criteria:

1. Is the reviewer knowledgeable in the area being reviewed?
2. Is the topic being reviewed documented in the IRAP?
3. Are communications between the reviewer and reviewee clear and concise?
4. If there were any findings, did the reviewer effectively communicate them to the reviewee?
5. If an anomaly was introduced by the inspector, was it detected?
6. Were appropriate actions taken?

Accounting System

Objective: This test will determine whether the materials accounting system can function following system failures at different levels and whether the system can be recovered.

Scenario: Simulate failure of different levels of the accounting system, including online data entry points on process lines or sensors, primary accountability computers, and primary storage media.

Evaluation Criteria:

1. Were operations successfully restarted?
2. Was there resolution of all items, operations, and measurements affected while the system was down?
3. Was the system successfully restarted from backup data or systems?

Closure of Corrective Active Validation

Objective: Determine whether closed findings from the internal review and assessment program have been appropriately closed.

Scenario: From a list of closed findings from the internal review and assessment program, select several closed findings. Validate the closed findings through field inspections.

Evaluation Criteria:

1. Were findings stated as closed by the facility still closed?
2. Were findings appropriate for the identified deficiency?
3. Were the closure actions still in place?
4. Did the corrective action address the root cause of the deficiency?

Material Transfer Checks for MBA Categorization

Objective: This test will validate the facility controls to ensure that a Category II or III MBA cannot receive material that would increase the category level.

Scenario: Attempt a material transfer (using only documentation not actual material) to a Category II or III MBA to increase the category of the MBA.

Evaluation Criteria:

1. Do procedures exist to prohibit the increase in category level for MBAs?
2. Was the attempted transfer detected?
3. Was the facility response to the attempted transfer appropriate?

Material Accounting: Item Identification Front and Back Checks

Objective: This test will determine whether the facility records accurately reflect the identity, value, and location of inventory items.

Scenario: Select a sample of items from either the inventory listing or during the field inspections. Record the item ID, location, plutonium weight, and TID. Verify the items in the field or the sample taken from the field against accountability system records.

Evaluation Criteria: Were items in the field successfully reconciled to the nuclear material accounting system records?

SNM Receipt Closure

Objective: Determine whether transactions (receipts) with unmeasured values or significant shipper/ receiver differences are entered into the process.

Scenario: Utilize a TJ-14, “Transaction Activity Summary by Facility,” generated by NMMSS to test facility records.

Evaluation Criteria:

1. Are receipts measured and transactions closed prior to introducing material to the process?
2. Are exceptions granted for those materials that do not have a measurement or for transactions not completed?

Material Accounting: Accounting System Forms

Objective: This test will determine the effectiveness of the filing system for controlled accountability forms used in the MBA. Check key information on documents reviewed, including form used for transfers of SNM.

Scenario: For each type of control and accountability record, randomly select 10 percent (or a minimum of one record) of the forms used in the MBA during the review period. Locate specific records and check key entries for completeness.

Evaluation Criteria:

1. Could all forms be located during the field investigation portion of the review?
2. Were all corrections or lineouts initialed by the custodian done in accordance with requirements?
3. Did all of the forms contain the required information?

Material Control: Tamper Indicating Device System

Test Objective: This test will determine whether TID discrepancies are detected and if proper resolution is achieved.

Scenario: Replace a TID with another TID without initiating changes in accounting records OR make a change in the TID number in the accounting records.

Evaluation Criteria:

1. Was the different number detected?
2. Were records checked to verify which TID should be on the item?
3. Was the item remeasured to verify the SNM content?

Material Control: Material Surveillance – Two-Person Rule

Test Objective: This test will determine if the two-person rule can be compromised.

Scenario: One person of the two-person rule requests that the other person leave to get additional supplies. The scenario can be tested in vaults, processing areas, waste assay and packaging areas, TID applications, etc.

Evaluation Criteria:

1. Did the person leave the area?
2. Was a second authorized person called to provide two-person coverage?

Material Accounting: Measurements and Measurements Control – Scales and Balances

Objective: This test will determine whether the scales and balances program provides data of the quality required for MC&A records.

Scenario: Select a sample of accountability weighing instruments from the MC&A organization records and verify the frequency and currency of the calibration and performance of daily linearity checks. Check performance of the instrument against standards normally used or against independent weight standards that are in the normal weighing range of the instrument.

Evaluation Criteria:

1. Was instrument calibration current?
2. Are appropriate standards being used?
3. Are daily checks being made?
4. Were personnel familiar with the operation and MC&A procedures?

5. Did the instruments perform to the stated specification?

SNM Item Listing Generation

Objective: Determine whether the facility can generate a physical inventory listing for MBAs possessing Category I SNM within 3 hours, or within 24 hours for other MBAs.

Scenario: Ask the facility to generate an inventory listing and note how long it takes to generate. (This scenario can be combined with an actual physical inventory. The inspector can introduce an anomaly into the inventory list and evaluate the facility response.)

Evaluation Criteria:

1. Was the inventory list generated within the appropriate timeframe?
2. Was the list accurate?
3. How did the facility consider items in transit or data that had not been entered into the computer system?
4. If an anomaly was introduced, did the facility detect it and initiate appropriate action?

Internal Transfer Forms Falsified

Objective: Determine whether the facility can detect a falsified internal transfer.

Scenario: A facility transfer form is prepared by an unauthorized individual and processed through the accountability system.

Evaluation Criteria:

1. Did the facility procedure for processing transfers detect the falsified transfer?
2. Was the facility response appropriate and timely?

3.7 Foreign Visits and Assignments

FOREIGN VISITS AND ASSIGNMENTS

- Subtopical Areas
- Common Deficiencies

Subtopical areas will address:

- Current Directives
- Potential Documents for Review
- Potential Interview Candidates
- Lines of Inquiry
- Performance Tests

SUBTOPICAL AREAS

- Sponsor Program Management and Administration
- CI Requirements
- Export Controls/Technology Transfer Requirements
- Security Requirements
- Approvals and Reporting

COMMON DEFICIENCIES

The following is a sample of common deficiencies identified by the Office of Independent Oversight (now the Office of Security and Cyber Evaluations) in the 2009 document, *Personnel Security Inspectors Guide*. By reviewing the list of common deficiencies during the planning phase, assessors can be alert for similar deficiencies during data gathering activities.

- Inadequate notice
- Inadequate security plans for visits
- Deterioration of escort procedures
- Inadequate computer access controls
- Failure to close out visits in the Foreign Access Central Tracking System (FACTS)

SPONSOR PROGRAM MANAGEMENT AND ADMINISTRATION

SUBTOPICAL AREAS: SPONSOR PROGRAM MANAGEMENT AND ADMINISTRATION

Sub-elements include:

- None

CURRENT DIRECTIVES AND REFERENCES

The following references apply to Sponsor Program Management and Administration:

- 10 CFR 110, *Export and Import of Nuclear Equipment and Material*
- 10 CFR Ch III, *Assistance to Foreign Energy Activities*, Part 810
- 15 CFR Ch I, *Export Administration Regulations*, Parts 730-744
- DOE O 142.2A, *Voluntary Offer Safeguards Agreement and Additional Protocol with the International Atomic Energy Agency*
- DOE O 142.3A, *Unclassified Foreign Visits and Assignments Program*
- DOE O 200.1A, *Information Technology Management*
- DOE O 360.C, *Federal Employee Training*
- DOE O 470.4B, *Safeguards and Security Program*
- DOE O 471.1A, *Identification and Protection of Unclassified Controlled Nuclear Information*
- DOE O 471.6, *Information Security*
- DOE O 472.2, *Personnel Security*
- DOE O 473.3, *Protection Program Operations*
- DOE O 475.1, *Counterintelligence Program*
- DOE O 475.2A, *Identifying Classified Information*
- DOE O 551.1D, *Official Foreign Travel*
- NSDD 189, *National Policy on the Transfer of Scientific, Technical and Engineering Information*
- PDD 61, *Energy Department Counterintelligence*
- 50 USC 2652 / Public Law (PL) 106-65, *National Defense Authorization Act*

SAMPLE DOCUMENT LIST

The following documentation may be considered for review:

- Documentation authorizing approval for specific categories of visits and assignments
- Indices checks
- Training records (escort and hosts)
- Security incidents/infractions
- Escort/host procedures
- Visit-specific security plans
- Unclassified computer security review
- OPSEC reviews/assessments
- CI program reviews/assessments
- Notification of approval documentation
- Deviations pertinent to visits and assignments
- FNVA closeout information
- Justification-for-visit request approvals and denials
- FACTS submittals

- SSP

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 supervisors
- Local FACTS coordinator
- OPSEC coordinator and/or OPSEC working group members
- Hosts/escorts
- Visit control

SAMPLE LINES OF INQUIRY

Suggested lines of inquiry can be used to (1) assist in determining the scope of assessment activities, (2) assist in developing document call lists, and (3) guide the interview process. Lines of inquiry may include:

1. Which organization maintains the responsibility for indices checks?

2. Who has approval authority for all unclassified visits and assignments at the site?

3. Who approves the security plans for unclassified foreign visits and assignments to security areas?

4. What is the process for ensuring adequate coordination among security, CI, export control, and foreign intelligence should a FN require access to a security area or sensitive subject, or if the individual is visiting the site from a sensitive country?

5. Are approved procedures in place for unclassified visits and assignments by FNs?

COUNTERINTELLIGENCE REQUIREMENTS

SUBTOPICAL AREAS: CI REQUIREMENTS

Sub-elements include:

- None

CURRENT DIRECTIVES AND REFERENCES

The following references apply to CI Requirements:

- 10 CFR 110, *Export and Import of Nuclear Equipment and Material*
- 10 CFR Ch III *Assistance to Foreign Energy Activities*, Part 810
- 15 CFR Ch I, *Export Administration Regulations*, Parts 730-744
- DOE O 142.2A, *Voluntary Offer Safeguards Agreement and Additional Protocol with the International Atomic Energy Agency*
- DOE O 142.3A, *Unclassified Foreign Visits and Assignments Program*
- DOE O 200.1A, *Information Technology Management*
- DOE O 360.C, *Federal Employee Training*
- DOE O 470.4B, *Safeguards and Security Program*
- DOE O 471.1A, *Identification and Protection of Unclassified Controlled Nuclear Information*
- DOE O 471.6, *Information Security*
- DOE O 472.2, *Personnel Security*
- DOE O 475.1, *Counterintelligence Program*
- DOE O 475.2A, *Identifying Classified Information*
- DOE O 551.1D, *Official Foreign Travel*
- NSDD 189, *National Policy on the Transfer of Scientific, Technical and Engineering Information*
- PDD 61, *Energy Department Counterintelligence*
- 50 USC 2652 / PL 106-65, *National Defense Authorization Act*

SAMPLE DOCUMENT LIST

The following documentation may be considered for review:

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

SAMPLE INTERVIEW CANDIDATES

The following individuals may be considered candidates for interviews:

- S&S manager (DOE and contractor)
- CI program manager (DOE and contractor)

- OPSEC coordinator and/or OPSEC working group members
- Hosts/escorts
- Visit control

SAMPLE LINES OF INQUIRY

Suggested lines of inquiry can be used to (1) assist in determining the scope of assessment activities, (2) assist in developing document call lists, and (3) guide the interview process. Lines of inquiry may include:

1. Which organization maintains the responsibility for indices checks?

2. Who has approval authority for all unclassified visits and assignments at the site?

3. Who approves the security plans for unclassified FNVA to security areas?

4. Is there a process covering the conduct and approval of CI consultations in lieu of indices not returning when return of indices is required?

5. Do records indicate indices checks were requested and/or completed as required?

6. What is the process for ensuring adequate coordination among security, CI, export control, and foreign intelligence should an FN require access to a security area or sensitive subject, or if the individual is visiting the site from a sensitive country?

7. How does CI provide review and input to approval authority on FNVA requests?

EXPORT CONTROLS/TECHNOLOGY TRANSFER REQUIREMENTS

SUBTOPICAL AREAS: EXPORT CONTROLS/TECHNOLOGY TRANSFER REQUIREMENTS

Sub-elements include:

- None

CURRENT DIRECTIVES AND REFERENCES

The following references apply to Export Controls/Technology Transfer Requirements:

- 10 CFR 110, *Export and Import of Nuclear Equipment and Material*
- 10 CFR Ch III, *Assistance to Foreign Energy Activities*, Part 810
- 15 CFR Ch I, *Export Administration Regulations*, Parts 730-744
- DOE O 142.2A, *Voluntary Offer Safeguards Agreement and Additional Protocol with the International Atomic Energy Agency*
- DOE O 142.3A, *Unclassified Foreign Visits and Assignments Program*
- DOE O 200.1A, *Information Technology Management*
- DOE O 360.C, *Federal Employee Training*
- DOE O 470.4B, *Safeguards and Security Program*
- DOE O 471.1A, *Identification and Protection of Unclassified Controlled Nuclear Information*
- DOE O 471.6, *Information Security*
- DOE O 472.2, *Personnel Security*
- DOE O 475.1, *Counterintelligence Program*
- DOE O 475.2A, *Identifying Classified Information*
- DOE O 551.1D, *Official Foreign Travel*
- NSDD 189, *National Policy on the Transfer of Scientific, Technical and Engineering Information*
- PDD 61, *Energy Department Counterintelligence*
- 50 USC 2652 / PL 106-65, *National Defense Authorization Act*

SAMPLE DOCUMENT LIST

The following documentation may be considered for review:

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

SAMPLE INTERVIEW CANDIDATES

The following people should be interviewed regarding the export control and tech transfer programs:

- S&S manager (DOE and contractor)
- Export control/technology transfer manager or subject matter expert

- Program managers and supervisors
- Hosts/escorts
- Visit control

SAMPLE LINES OF INQUIRY

Suggested lines of inquiry can be used to (1) assist in determining the scope of assessment activities, (2) assist in developing document call lists, and (3) guide the interview process. Lines of inquiry may include:

1. Is export control and technology transfer involved in the FNVA approval process? How and at what level?

2. Who approves the security plans for unclassified FNVA to security areas?

3. What is the process for ensuring adequate coordination among security, CI, export control, and foreign intelligence should an FN require access to a security area or sensitive subject, or if the individual is visiting the site from a sensitive country?

SECURITY REQUIREMENTS

SUBTOPICAL AREAS: SECURITY REQUIREMENTS

Sub-elements include:

- None

CURRENT DIRECTIVES AND REFERENCES

The following references apply to Security Requirements:

- 10 CFR 110, *Export and Import of Nuclear Equipment and Material*
- 10 CFR Ch III, *Assistance to Foreign Energy Activities*, Part 810
- 15 CFR Ch I, *Export Administration Regulations*, Parts 730-744
- DOE O 142.2A, *Voluntary Offer Safeguards Agreement and Additional Protocol with the International Atomic Energy Agency*
- DOE O 142.3A, *Unclassified Foreign Visits and Assignments Program*
- DOE O 200.1A, *Information Technology Management*
- DOE O 360.C, *Federal Employee Training*
- DOE O 470.4B, *Safeguards and Security Program*
- DOE O 471.1A, *Identification and Protection of Unclassified Controlled Nuclear Information*
- DOE O 471.6, *Information Security*
- DOE O 472.2, *Personnel Security*
- DOE O 475.1, *Counterintelligence Program*
- DOE O 475.2A, *Identifying Classified Information*
- DOE O 551.1D, *Official Foreign Travel*
- NSDD 189, *National Policy on the Transfer of Scientific, Technical and Engineering Information*
- PDD 61, *Energy Department Counterintelligence*
- 50 USC 2652 / PL 106-65, *National Defense Authorization Act*

SAMPLE DOCUMENT LIST

The following documentation may be considered for review:

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

SAMPLE INTERVIEW CANDIDATES

The following people may be interviewed regarding the export control and tech transfer programs:

- S&S manager (DOE and contractor)
- Program managers and supervisors
- Hosts/escorts
- Visit control

SAMPLE LINES OF INQUIRY

Suggested lines of inquiry can be used to (1) assist in determining the scope of assessment activities, (2) assist in developing document call lists, and (3) guide the interview process. Lines of inquiry may include:

1. Does the facility have a standard or generic security plan in place?

2. Does the security plan adequately ensure security interests and sensitive information/technologies are not placed at risk?

3. Does the security plan identify general restrictions on access?

4. Is there a specific security plan for each visit/assignment involving a sensitive country national, security area, and/or subject?

APPROVALS AND REPORTING

SUBTOPICAL AREAS: APPROVALS AND REPORTING

Sub-elements include:

- None

CURRENT DIRECTIVES AND REFERENCES

The following references apply to Approvals and Reporting:

- 10 CFR 110, *Export and Import of Nuclear Equipment and Material*
- 10 CFR Ch III, *Assistance to Foreign Energy Activities*, Part 810
- 15 CFR Ch I, *Export Administration Regulations*, Parts 730-744
- DOE O 142.2A, *Voluntary Offer Safeguards Agreement and Additional Protocol with the International Atomic Energy Agency*
- DOE O 142.3A, *Unclassified Foreign Visits and Assignments Program*
- DOE O 200.1A, *Information Technology Management*
- DOE O 360.C, *Federal Employee Training*
- DOE O 470.4B, *Safeguards and Security Program*
- DOE O 471.1A, *Identification and Protection of Unclassified Controlled Nuclear Information*
- DOE O 471.6, *Information Security*
- DOE O 472.2, *Personnel Security*
- DOE O 475.1, *Counterintelligence Program*
- DOE O 475.2A, *Identifying Classified Information*
- DOE O 551.1D, *Official Foreign Travel*
- NSDD 189, *National Policy on the Transfer of Scientific, Technical and Engineering Information*
- PDD 61, *Energy Department Counterintelligence*
- 50 USC 2652 / PL 106-65, *National Defense Authorization Act*

SAMPLE DOCUMENT LIST

The following documentation may be considered for review:

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

SAMPLE INTERVIEW CANDIDATES

The following may be interviewed regarding the unclassified FNVA program:

- S&S manager (DOE and contractor)

- Program managers and supervisors
- Hosts/escorts

SAMPLE LINES OF INQUIRY

Suggested lines of inquiry can be used to (1) assist in determining the scope of assessment activities, (2) assist in developing document call lists, and (3) guide the interview process. Lines of inquiry may include:

1. Which organization maintains the responsibility for indices checks?

2. Who has approval authority for all unclassified visits and assignments at the site?

3. Who approves the security plans for unclassified FNVA to security areas?

4. What is the process for ensuring adequate coordination among security, CI, export control, and foreign intelligence should an FN require access to a security area or sensitive subject, or if the individual is visiting the site from a sensitive country?

5. What is the process to ensure that the approval authority considers information from the review process and subject matter expert reviews?

6. How are approval determinations being documented in DOE FACTS when required?

7. Who is the approval authority? Has that approval authority been further reassigned? Has it been reassigned in writing and what was the distribution?

8. Are there plans and procedures for reassignment of approval authority and has that reassignment been reviewed and approved by the head of the cognizant DOE field element and the approval authority?

9. Who is the designated POC for the unclassified FNVA program management? Has that POC information been provided to the DOE CSA?

WORKSHEETS AND PERFORMANCE TESTS

The following worksheets and sample performance tests may be used during the assessment process to evaluate the status of the Unclassified Visits and Assignments by Foreign Nationals topical area.

Foreign National Checklist

- Are there approved procedures for unclassified visits and assignments by FNs?
- Are the persons signing the requests as the final approval authority for the facility designated in writing as having final approval authority?
- Is the approval authority fully aware he/she is accountable for all approval decisions?
- Does the approval process ensure that officials with responsibility for CI, security, export control, and technology transfer concur before final approval is granted? Appropriate approvals can be verified through sample record review; all concurrences should be documented.
- Are all visits/assignments by FNs from terrorist countries approved by the U.S. Secretary of Energy? This can be verified through sample record review.

- Are all visits/assignments being added to the FACTS? If other recordkeeping systems are used, do they contain all the information required? Pull a small random sample to verify that data was added to FACTS.
- Has the facility official notified all employees 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?
- Do records indicate indices checks were conducted (and completed) on every sensitive country visit or assignment and any FN visit/assignment involving a sensitive subject and/or security area? Pull a sample of visits/assignments involving sensitive country nationals, security areas, and sensitive subjects to verify.
- Does the facility have a standard or generic security plan in place? 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 by FNs? Has the plan been reviewed and approved by the DOE CSA?
- Is there a specific security plan for each visit and assignment where a specific security plan is required? Pull a sample of visits/assignments involving sensitive country nationals, security areas, and sensitive subjects to verify. Do the security plans adequately ensure security interests and sensitive information/technologies are not placed at risk? Do the security plans impose specific access restrictions and security countermeasures to ensure effective protection of DOE assets? Do the plans contain sufficient detail? Have each of the plans been reviewed and approved by the DOE CSA?
- Do the areas identified as security areas in the standard or specific security plans match the current list of security areas of the facility?
- Who determines whether or not a visit/assignment involves a sensitive subject? If the sensitive subject is the host, does anyone in the approval process have the responsibility to validate whether or not he/she is a sensitive subject?
- How are hosts/escorts made aware of their responsibilities? Are hosts/escorts briefed on specifics of the visit/assignment (e.g., security plan requirements)? How is the briefing documented?
- How is the visitor/assignee made aware of his/her responsibilities? Does anyone discuss prohibited articles, badging, areas where access is limited, etc., with the visitor?
- Are the FNs issued a unique badge that identifies them as non-U.S. citizens?
- Do badging and visitor control procedures address what approvals must be in place before an FN is issued a visitor or permanent badge?
- Are FN badges terminated at the end of a visit/assignment? Can a sample be pulled from terminated assignments and cross-referenced against permanent badge records to see if the badge has been destroyed?
- Who reviews FN requirements, as they relate to cyber security, coordinate with the unclassified cyber security?

Sponsor Program Management and Administration

Objective: This test will be used to determine that a system/process is implemented to ensure DOE requirements are met regarding a visit by an FN from a non-sensitive country.

Scenario:

1. The assessment team member prepares a request for an unclassified visit to the facility by an FN from a non-sensitive country.
2. The assessment team member reviews the facility procedures for implementation and then coordinates with a facility representative to submit the request to the visitor control staff.
3. The assessment team member observes the visitor control staff in the processing of the visit request from start to finish, noting if correct forms and plans are used.

Conditions: Normal work conditions.

Evaluation Criteria: Facility implementation procedures are followed.

4.0 POST-ASSESSMENT TOOLS

IN THIS SECTION:

- Sample Report Format
- Report Writing Guide
- Sample Slides for the Exit Briefing
- Transmittal Memorandum
- DOE F 470.8, Survey/Inspection Report Form
- Sample CAPs
- Sample Root Cause Analysis Form
- Sample Request for Finding Closure/Validation

Tab 4

SAMPLE REPORT FORMAT

Report Format

The report should be formatted with the 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. Reports should contain the following items and should *always* be reviewed by an authorized derivative classifier (ADC).

- A completed DOE F 470.8 or equivalent
- An executive summary containing:
  - The scope, methodology, period of coverage, duration, date of exit briefing to management
  - A brief overview of the facility, function, scope of operations, and contractual information (e.g., contract number, award and expiration dates, contract type, identification of security clauses, identification of the security, and overall scores assigned to the most recent contract appraisal)
  - 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
  - The overall composite facility rating with supporting rationale, if given
  - A list of findings identified during the review
- An introduction containing:
  - The scope, methodology, period of coverage, duration, date of exit briefing to management
  - A description of the facility, its function and scope of operations, security interests, and contractual information (e.g., contract number, award and expiration dates, contract type, identification of security clauses, identification of the security, and overall scores assigned to the most recent contract appraisal)
- Narrative for all rated topical and subtopical areas that includes:
  - A description of the site's implementation of the program element
  - Scope of the assessment
  - A description of activities conducted
  - Results and associated issues (including other department elements or GAO review, or inspection results related to this topic/subtopic that were included in the assessment)
  - Identification of all findings, including new and previously identified open findings, regardless of source (e.g., Office of Security and Cyber Evaluations, IG, GAO, and their current corrective action status
  - An analysis that provides justification and rationale of the factors responsible for the rating
- Attachments may include:
  - Copy of the current DOE F 470.2 FDAR;
  - List of all active DOE F 470.1 or DD F 254 CSCS
  - List of all new findings
  - List of all previous findings that are open, to include the current status of corrective action
  - List of team members including names, employer, and assigned area(s) of evaluation
  - List of all source documentation used to support the results

Narrative

The narrative section of the report should clearly describe the facility being assessed, its S&S interests and activities, protective measures, and status of the S&S program at the time of the assessment. The report should also explain how the protection measures were evaluated. Use of statistical data will help describe the facility's S&S interests and the assessment efforts. For example, data might include numbers of employees with each level of access authorization, the number of classified documents in each level and category, and the number of documents sampled for compliance/performance.

The report should reflect the compliance and performance segments of the assessment. Discussions of topical areas in the report should follow the order of the topics identified in DOE F 470.8. Reports should explain what the S&S program is supposed to do, what was assessed, and what was found. A summary of content appears below.

- The status (e.g., approved, pending) of any required planning documents (e.g., SSP, MC&A, Information System Security).
- All new findings, with SSIMS finding numbers, should be identified. Open findings from the previous reviews should be identified in the narrative portion of the report. Open findings will maintain their original finding number. A new finding that is a repeat of a closed finding will receive a new number, but reference the closed finding in the body of the narrative.
- The program deficiencies (findings) and supporting data should be clearly described. The term "finding" refers to deficiencies or concerns found during the assessment.
- A description of the facility's strengths and weaknesses should correlate to the results from the compliance and performance segments and discuss the bases for the ratings. The report should reflect validated and defensible ratings. Assigned performance ratings should be based on well-conducted and replicable performance tests. The narrative description should be consistent with and support the composite and topical area ratings (including "Does Not Apply").
- The report should identify findings corrected on the spot. The findings and corrective actions should be clearly described in the narrative.
- The status of corrective actions for open findings and findings from the previous assessments should be included in the narrative (also included in Resolution of Findings under the Program Management and Support topical area).
- A concluding analysis of each topical area should be included in the narrative.
- Reasons for a less-than-satisfactory rating should be explained in detail. The report should address the scope, scope of operations, corrective actions or findings, discussion of significant impact, and analysis of each topical area.

REPORT WRITING GUIDE

INTRODUCTION

This guide describes the philosophy, scope, and general procedures for documenting the activities associated with the conduct of S&S self-assessments. It addresses the requirements specified in DOE O 470.4B as it pertains to the writing of self-assessment reports; however, it is also important to note that this guide goes further by offering suggestions beyond those identified in the DOE directive or the DOE Technical Standard. This guide is designed to give the user specific direction on what level of content is expected within the report, along with some general information on how to present this information in a more clear and direct manner.

The first part of this guide focuses on report writing mechanics. It describes the basic elements of the report (narrative, findings). The purposes of these elements are described along with some examples of how they may be written. It also addresses the appropriate use and documentation of other assessment reports to augment the self-assessment report. Lastly, it addresses the most critical aspect of the report, the end product of analyzing all collected data and the resulting conclusion about the effectiveness of the S&S program.

The second part provides examples of an exit briefing, transmittal memo, report form, CAP and root cause analysis forms, and request for finding form.

REPORT WRITING MECHANICS

The Report Writing Guide is applicable to all types of self-assessment reports, regardless of the objectives. The report must communicate a message, or tell a story about the status of the S&S program at a given facility; however, more critical than just telling the story, the report must be written in such a way that all potential audiences can understand it with equal clarity. One error of those responsible for writing self-assessment reports is the failure to recognize the many audiences that may encounter the report. Certainly it will be used internally at the site, but copies of the report might also be sent to DOE-HQ elements or other DOE elements that have an interest in the facility.

Writing for a wide range of audiences with significantly varying degrees of familiarity with the operations of the facility does not mean that one must include vast amounts of descriptive data about all aspects of the facility. It is important to determine how much description is necessary to ensure understanding of the detached third-party reader. Keep in mind that the ultimate goal of the report is to document the status of the S&S program and its capability to protect target assets. To be an acceptable report, one must convey the basic information of who, what, when, where, why, and how, otherwise the reader will have doubts about the breadth and scope of the evaluation as well as unanswered questions about the effectiveness of the S&S program.

Basic Report Contents

Self-assessment reports describe the conduct, evaluation activities, and results of the evaluation. The report should contain certain minimum requirements. Most reports are divided into four main parts: executive summary, introduction, body of the report, and attachments. The specific information required for each part of the report is described below:

- **Executive Summary –** In some cases, the executive summary is the only portion of the report that is read. It is therefore critical that this section capture all the important "big-picture" details associated with the self-assessment activity. The executive summary is normally one to three pages in length and contains, at a minimum, the following information:

- A statement reflecting scope. This should specify if any topical or subtopical areas were not evaluated and the reason for this omission. If all topical and subtopical areas were evaluated, then a simple statement to that effect will suffice.
- The period of time covered by assessment.
- The methodologies/techniques used (e.g., document reviews, observations, interviews, performance tests). Keep in mind these are simply a broad list of the methods and techniques used during the assessment. It is not intended to address the activities associated with each subtopical area.
- A brief overview of the facility, function, and scope of operations. Brief is the key word here so detailed descriptions would be inappropriate. This overview should provide the reader with enough information to understand what type of facility was reviewed, why the facility exists, and what kinds of operations occur there that are important to national security.
- A brief synthesis of major (big-picture) strengths and weaknesses that impact the effectiveness of the overall S&S program. This is perhaps the single most important statement in the executive summary. This should provide the rationale for the ratings.
- Identify any topic or subtopical areas rated less than satisfactory. The significant weaknesses associated with this rating should be described (as explained in the paragraph above).
- The overall composite facility rating, if given, with supporting rationale. The supporting rationale may be explained in conjunction with the syntheses of major strengths and weaknesses or may be addressed separately; however, it is equally important to explain the rationale for awarding a composite rating of satisfactory as it is when rating at a lower level.

- **Introduction –** There is certain information that is too detailed to be included in the executive summary, but is applicable to all aspects of the assessment report. The introduction provides a place for this information and sets the tone of the report. Information that should be included in the introduction includes:
  - The period of coverage. Although mentioned in the executive summary, it is important to include this information in the body as well. If long-standing issues are being evaluated (e.g., resolution of past findings, status of line-item budget upgrade) activities occurring outside of the review window may be subject to review. This should be specified in the introduction.
  - Composition of team members and the areas evaluated. This serves as a record for management if questions arise in the future or as a resource in assisting with the validation of corrective actions.
  - Description of the facility, its function, and scope of operations. Without question this has been one of the more controversial items to be contained in the report; the controversy surrounds the level of detail necessary. The report should contain enough information to give the reader a basic understanding of what types of operations are occurring at the facility and a brief description of the physical layout; however, detailed information about the operations of particular programs should not be addressed. Include information that provides a description of the function and scope of operations and protective measures employed. This may be accomplished by referring to the descriptions in S&S plans when no changes have occurred, or it can be cut and pasted directly from the facility description section of the SSP. This issue will be addressed again in the narrative section of the report.

- **Report Body**
  - Narrative

    The narrative section of the report is where the "story" of the assessment is told. The narrative explains what actually occurred and how the protection measures were evaluated. There are actually two parts to the narrative: the first serves as an introduction to the topical/subtopical area being evaluated and the second describes the assessment process.

    This topical/subtopical area information is principally descriptive in nature and should discuss very broad-based issues relative to that area. Examples of this type of information would include:

    - A description of the function and scope of program operations and associated protective measures in place.
    - Status of corrective actions for all open findings and for all open and closed findings from previous reviews for each program area. This may be discussed in the narrative or in a separate section of the report; however, if covered in a separate section, the impacts of these open findings should not be neglected in the overall evaluation of the topical/ subtopical area.

    While much work and effort goes into planning and conducting a self-assessment, the extent of this effort is often lost due to a failure to adequately document the activities in the report. Because the narrative tells a story, all parts of the story must be included. The following assessment process information should be contained, at a minimum, in the report narrative.

    Scope of Subtopical Area Evaluation. Describe what activities were evaluated within the subtopical area. For example, if the IDAS subtopical area was evaluated, then the scope would include review of internal and external sensors, alarm communication, alarm testing and maintenance, protective lighting, etc. The reader should be able to readily determine what activities associated with this subtopical area were reviewed.

    Description of Activities. Explain what was evaluated and how the evaluation was performed. Include information such as how many personnel or items were sampled and the basis of the evaluation (i.e., purpose of evaluation and what the assessor was attempting to validate or verify). Use specific numbers (e.g., 125 records evaluated out of 1,000) or detailed information (number of hours observed at which types of locations) to give the reader a perspective of the extent of activities. If a deficiency is noted, describe how the deficiency was identified, characteristics of the deficiency (isolated or systemic), and its implications.

    Description of Evaluation Results and Associated Issues. Explain what all of the activities mean. Document results of the individual evaluation efforts by indicating the presence or lack of any deficiencies. This can be accomplished in a broad, sweeping statement describing the collective results of a number of activities or individually. If deficiencies are noted, the analysis of results can focus on a single isolated deficiency, or the significance of the deficiency in light of other deficiencies noted in this and other subtopical areas or open findings without adequate compensatory measures.

    Although it has been mentioned several times that the report must document the review activities, the question arises how much documentation is too much? Remember, the narrative is the part of the report that tells the story of what and how the S&S program was evaluated and whether or not the program is capable of protecting DOE security interests. As mentioned, the report should document what was evaluated, how it was evaluated, and the results of evaluation. If providing lengthy detail about how a program is structured and operates is not relevant to the discussion of an identified deficiency, then this information should not be included.

For example, if no deficiencies were noted in the lock and key program, the narrative should state what was examined, how the evaluation was performed, and the results (i.e., no deficiencies were noted). It would serve no purpose to include two pages of narrative explaining how the lock and key program is organized and describing in minute detail the procedures associated with the issuance of new security keys. If there were some deficiency associated with issuance of new keys that resulted in a vulnerability to an S&S interest, then a description of this procedure would be necessary to clarify the elements of concern. However, if there was no deficiency, such information is a distraction and degrades the report quality.

– Finding

A finding is the formal documentation of a recognized deficiency (i.e., a non-compliance with a specific DOE directive, SSP, or program implementing procedure, or failure to meet a performance standard) that requires implementation and tracking of corrective actions sufficient to prevent recurrence. Findings can be written for deficiencies that are isolated, single-point failures or systemic and capable of impacting other facilities or sites; however, the real art is in the ability to write a "good" finding. A good finding is one that is firmly based in DOE policy, clearly communicates what is deficient, and ultimately improves the S&S program when corrected.

There are two keys to remember about findings. First, no finding should be written that, by its existence (and ultimate correction), would not improve the overall effectiveness of the S&S program being evaluated, including the preclusion of an actual or potential vulnerability to a security interest. Second, all findings should be worded in a manner that clearly and accurately reflects the originating deficiency, allowing for implementation of appropriate corrective actions and eventual closure of the finding. Nebulous and ambiguously worded findings that do not clearly identify the deficiency or are not based on established DOE directives, approved SSPs, or procedures developed to implement DOE directives are a common problem. Such findings are nearly impossible to close and a waste of valuable resources. The time and effort spent attempting to understand the deficiency and developing corrective actions is not worth the costs involved because the end result will not positively impact the S&S program's effectiveness.

This guide focuses on construction of the finding and the formula for writing a "good" finding. It is important to note that a finding is only as good as its supporting narrative. As discussed above, the narrative tells the story and explains what is deficient, how the deficiency was validated, and the significance of that deficiency. Because findings are to be written succinctly, an in-depth description of the circumstances surrounding the deficiency is not needed. That is the job of the narrative. The job of the finding is to provide an accurate reflection of the conditions that were identified during the evaluation and show how that condition fails to comply with DOE or site directives or meet documented performance standards. This may be reflected simply as:

Condition at the facility + DOE directives/requirements = Finding

Example: During data collection, you have taken a representative sample of the 300 SPO IIs at the facility and are reviewing training records to determine if all have completed annual refresher training. Out of your sample of 40 SPO II personnel, 10 have not completed their annual refresher training and are still staffing active posts on a daily basis. It was later determined that these personnel were not present during the scheduled training day and makeup training was never provided. The associated directive states that each SPO must successfully complete formal annual refresher training to maintain the level of competency required for the successful performance of tasks associated with SPO job responsibilities. Because your sample indicates a 20 percent deficiency rate, further sampling is not deemed necessary due to this deficiency rate and the limitation of time resources.

The finding for this deficiency could be written as follows:

> FINDING: *Twenty percent of all SPO II personnel sampled have not successfully completed formal annual refresher training to maintain the level of competency required for the successful performance of tasks associated with SPO job responsibilities.*

A more succinct way to write the same finding would be:

> FINDING: *Not all SPO II personnel have successfully completed formal annual refresher training.*

In both of these examples, the overall condition of the site is clearly stated along with words directly from the directive. There is little room for misinterpretation or subjectivity. The narrative should explain how the deficiency was identified and the implications associated with the deficiency.

Another approach attempts to take over the job of the narrative and include more specific information about the condition found at the facility.

> FINDING: *SPO II personnel not present for scheduled annual refresher training, were not provided makeup training, and, as a result, did not complete annual refresher training as required by DOE directive.*

This approach is not recommended principally because it may create the false assumption that annual refresher training is not completed because of the failure of the personnel to attend the makeup training that occurred when they were absent. Remember, only 40 personnel were sampled and time constraints did not allow you to review the records of all 300 personnel. If there were other problems that prevented an SPO II from completing all required training, these problems may not be identified (or resolved) if the finding is focused on the reasoning rather than the situation; however, if the review team did review all 300 records and this was the only reason that personnel did not complete the annual refresher training, then this finding would be acceptable.

Following are a few other requirements associated with findings that must be remembered:

- Each finding and subsequent corrective action should be required to have a standalone security classification (i.e., be portion-marked).
- Findings will be documented in each assessment report and listed separately at the end of the report. Each report should include an attachment, summary, or other section in which all the findings are listed. The data for each finding on this list should include (1) the finding number, (2) the finding synopsis, (3) the classification of each finding, and (4) the DOE or site directive reference number.
- Each finding should have a reference to the DOE directive or other site documents that identify the requirement(s) not being met.
- Each finding should have a unique identification number assigned that can be used throughout the reporting and tracking process.

- **Attachments –** The report may also contain certain forms and other documentation that can be collectively defined as attachments. This documentation may include:
  - Completed DOE F 470.8

- Copy of the current DOE F 470.2 FDAR
- Copy of each active DOE F 470.1 CSCS or DD 254
- Any other items necessary to provide supportive documentation regarding the scope of evaluation or associated results

Analysis and Conclusions

Each team member invests much effort in planning and research for a self-assessment. The team member spends extensive time (day and night) observing, asking questions, and conducting performance tests. This portion of the narrative allows for an explanation of what all this effort means. What do the results tell us about the status of the program and its ability to protect DOE S&S interests?

The concluding analysis should justify with a clearly stated, rational rating for this area based on the results of the evaluation. The narrative should support the conclusion and resulting rating. If there is inconsistency here, the validity of the entire effort may be called into question.

Use of Other Assessment Reports

Reviews or inspections conducted by departmental elements may be used to meet assessment requirements. All topical and subtopical areas, as specified on DOE F 470.8, should be included in the review or a written justification provided for why it was omitted. The assessing office can use the reviews of a topical or subtopical area if that area was included in an external review.

When using reviews to meet requirements of the self-assessment, the following guidelines must be followed:

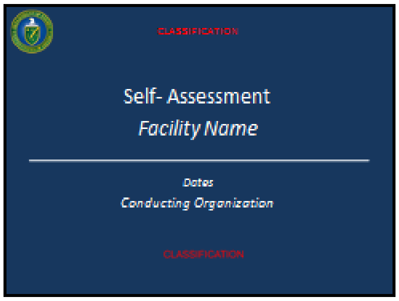
- The review/inspection should have been conducted within the period being assessed.
- Applicable portions of the review/inspection may be attached to the report.
- Portions of topical and subtopical areas not covered by the review should be assessed.
- If ratings were not assigned, the assessing office should analyze the impact of any deficiencies.

To ensure the integrity of the report, the methodology used to perform the assessment should be formally documented. This methodology should be available to all personnel responsible for performing self-assessment activities. Management should ensure that this methodology is being used to conduct the assessment. If not, the self-assessment program has no integrity and management cannot trust the results of the effort.

The self-assessment should be performed in an integrated fashion, much as a survey is performed. Evaluating programs in isolation does not provide sufficient information to adequately analyze the effectiveness of the S&S system in protecting DOE security interests. If segments of the S&S program are evaluated in isolation, conscious and deliberate steps must be taken to ensure results of the evaluation are examined in light of results of all other evaluations.

Finally, documented results of the self-assessment must be presented in a manner that will assist management in guiding and directing S&S activities at those facilities. Self-assessments are not performed to “check a box” to simply ensure compliance with a DOE directive; the self-assessment program is the foundation upon which all other evaluation and inspection methods are built. If the assessment is not performed in accordance with established methodology, the results subjected to insightful analysis, and the effort documented in a way that helps management effectively direct the program, then nothing has been gained.

SAMPLE EXIT BRIEFING



CLASSIFICATION

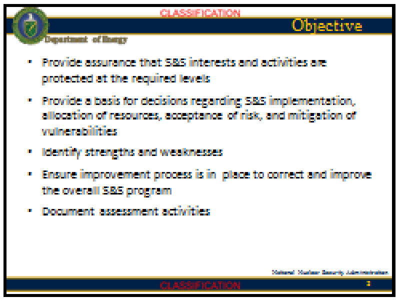
Self- Assessment

Facility Name

Dates

Conducting Organization

CLASSIFICATION



CLASSIFICATION

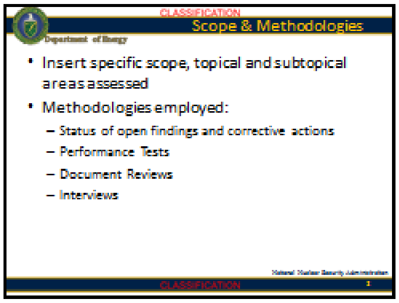
Objective

Department of Energy

- Provide assurance that S&S interests and activities are protected at the required levels
- Provide a basis for decisions regarding S&S implementation, allocation of resources, acceptance of risk, and mitigation of vulnerabilities
- Identify strengths and weaknesses
- Ensure improvement process is in place to correct and improve the overall S&S program
- Document assessment activities

National Nuclear Security Administration

CLASSIFICATION 2



CLASSIFICATION

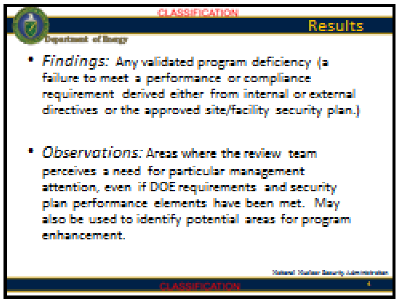
Scope & Methodologies

Department of Energy

- Insert specific scope, topical and subtopical areas assessed
- Methodologies employed:
  - Status of open findings and corrective actions
  - Performance Tests
  - Document Reviews
  - Interviews

National Nuclear Security Administration

CLASSIFICATION 3



CLASSIFICATION

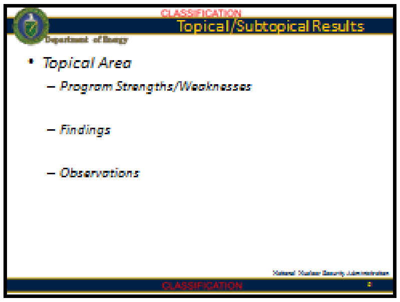
Results

Department of Energy

- *Findings:* 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.)
- *Observations:* Areas where the review team perceives a need for particular management attention, even if DOE requirements and security plan performance elements have been met. May also be used to identify potential areas for program enhancement.

National Nuclear Security Administration

CLASSIFICATION 4



CLASSIFICATION

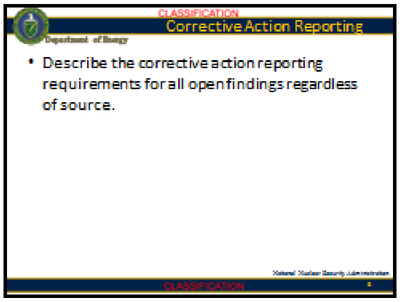
Topical/Subtopical Results

Department of Energy

- *Topical Area*
  - *Program Strengths/Weaknesses*
  - *Findings*
  - *Observations*

National Nuclear Security Administration

CLASSIFICATION 5



CLASSIFICATION

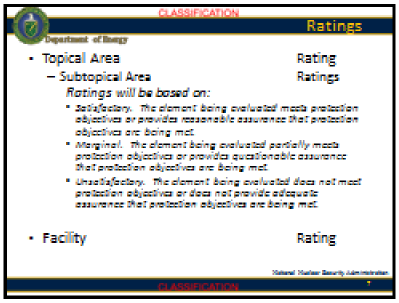
Corrective Action Reporting

Department of Energy

- Describe the corrective action reporting requirements for all open findings regardless of source.

National Nuclear Security Administration

CLASSIFICATION 6



CLASSIFICATION

Ratings

Department of Energy

- Topical Area Rating
  - Subtopical Area Ratings

    Ratings will be based on:
    - *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.*
- Facility Rating

National Nuclear Security Administration

CLASSIFICATION 7

SAMPLE TRANSMITTAL MEMORANDUM

The attached report outlines results of the recent Safeguards and Security Self-Assessment of the [Organization Assessed] conducted by the [Organization, Office]. This self-assessment conducted [insert timeframe] encompassed all security topical areas as defined on DOE F 470.8, *Survey/Inspection Report Form*.

The composite rating assigned to [organization] is [rating]. The assignment of this rating dictates that CAPs be developed within [number] working days. The [Organization, Office] will verify the adequacy and completeness of these action plans in accordance with DOE O 470.4B, *Safeguards and Security Program.*

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

[Include classification information as appropriate.]

SURVEY/INSPECTION REPORT FORM

DOE F 470.8 U.S. Department of Energy

SURVEY / INSPECTION REPORT FORM

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

12. Ratings:

a) PROGRAM MANAGEMENT AND SUPPORT
- Protection Program Management ____
  - Program Management and Administration ____
  - Resources and Budgeting ____
  - Personnel Development and Training ____
- S&S Planning And Procedures ____
- Management Control ____
  - Surveys and Self-Assessment Programs ____
  - Performance Assurance Program ____
  - Resolution of Findings ____
  - Incident Reporting and Management ____
- Program Wide Support ____
  - Facility Approval and Registration of Activities ____
  - Foreign Ownership, Control or Influence ____
  - Security Management in Contracting ____
- OVERALL RATING ____

b) PROTECTIVE FORCE
- Management ____
- Training ____
- Duties ____
- Facilities and Equipment ____
- OVERALL RATING ____

c) PHYSICAL SECURITY
- Access Controls ____
- Intrusion Detection and Assessment Systems ____
- Barriers and Delay Mechanisms ____
- Testing and Maintenance ____
- Communications ____
- OVERALL RATING ____

d) INFORMATION PROTECTION
- Basic Requirements ____
- Technical Surveillance Countermeasures ____
- Operations Security ____
- Classification Guidance ____
- Classified Matter Protection and Control ____
  - Control of Classified Matter ____
  - Special Access Programs & Intelligence Info ____
- OVERALL RATING ____

e) CYBER SECURITY
- Classified Cyber Security ____
  - Leadership, Responsibilities and Authorities ____
  - C&A, Risk Management and Planning ____
  - Policy, Guidance and Procedures ____
  - Technical Implementation ____
  - Performance Eval Feedback & Cont. Improve. ____
- Telecommunications Security ____
- Unclassified Cyber Security ____
  - Leadership, Responsibilities and Authorities ____
  - C&A Risk Management and Planning ____
  - Policy, Guidance and Procedures ____
  - Technical Implementation ____
  - Performance Eval Feedback & Cont. Improve. ____
- OVERALL RATING ____

f) PERSONNEL SECURITY PROGRAM
- Access Authorizations ____
- Human Reliability Program ____
- Control of Classified Visits ____
- Safeguards and Security Awareness ____
- OVERALL RATING ____

g) UNCLASSIFIED VISITS & ASSIGNMENTS BY FOREIGN NATIONALS
- Sponsor Program Management and Administration ____
- Counterintelligence Requirements ____
- Export Controls/Tech Transfer Requirements ____
- Security Requirements ____
- Approvals and Reporting ____
- OVERALL RATING ____

h) NUCLEAR MATERIALS CONTROL & ACCOUNTABILITY
- Program Administration ____
- Material Accountability ____
- Materials Control ____
- OVERALL RATING ____

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

SURVEYS: S = Satisfactory M = Marginal U = Unsatisfactory D = Does Not Apply NR = Not Rated (SPEC only)
INSPECTIONS: EP = Effective Performance NI = Needs Improvement SW = Significant Weakness D = Does Not Apply

SAMPLE CORRECTION ACTION PLAN

Finding No:	Copied directly from the final report
Finding:	Copied directly from final report
Root Cause:	Lead organization subject matter experts complete the root cause worksheet (attached) and provide documentation to the FSO
Lead Person:	POC provided by lead organization (usually a member of management)
Lead Organization:	Assigned by FSO (in conjunction with the organization) based on DOE's final report
Man-Hour Costs:	POC to provide feedback on costs estimated for closure/validation of finding (e.g., labor, contracts, materials, equipment)
Summary:	Lead organization should use this field for clarifying deficiency, discussing any mitigating factors, and explaining the overall strategy for correcting the finding.

Milestone Number	Description	Projected Date	Completion Date
	Lead organization (and secondary organizations, if applicable) determines corrective actions, which ***must*** address the results of the root cause analysis. *NOTE: FSO is available to advise the lead organization's POC/subject matter experts in composing the milestones and projected completion dates.* Reasonable projected completion dates are determined based on coordination with all affected organizations.		

SAMPLE CORRECTIVE ACTION PLAN TEMPLATE

Security Analysis
Corrective Action Plan

Report Number	Title	Finding Number

Finding:

SA Project Manager Concurrence:	**Date:**

Review:	(name)	(name)	(name)	**Date:**

Corrective Action Plan:

Estimated Completion Date:	**Date CAP Approved:**	**Date CAP Completed:**
Responsible Manager's Signature/Date:	**Auditor's Signature:**	**Verified By/Date:**

SAMPLE ROOT CAUSE ANALYSIS FORM

Finding Number and Description:	Copied directly from final report.
Participants:	Names, titles, organizations.
Date(s):	
Methodology:	How was root cause analysis conducted? What methodology was used?
Results:	Root cause to include contributing factors. Break down in sufficient detail to describe how root cause was determined. Contributing causes: Root cause:
Background:	Attach meeting notes, diagrams, etc.
Risk Statement:	Describe any risk to classified information or assets. If risk is present, describe actions taken to mitigate risk. If there is no risk, provide rationale (i.e., protective measures in place).

SAMPLE REQUEST FOR FINDING CLOSURE/VALIDATION

Request for Finding Closure/Validation

Assessment Title:	**Assessment Date:**
Finding Number:	
Finding Narrative:	
Response Narrative:	
Status:	
Compliance Verified by: **Name/Position**	**Date:**
Comments:	
Validated by: **Name/Position**	**Date**
Validation Actions Completed:	