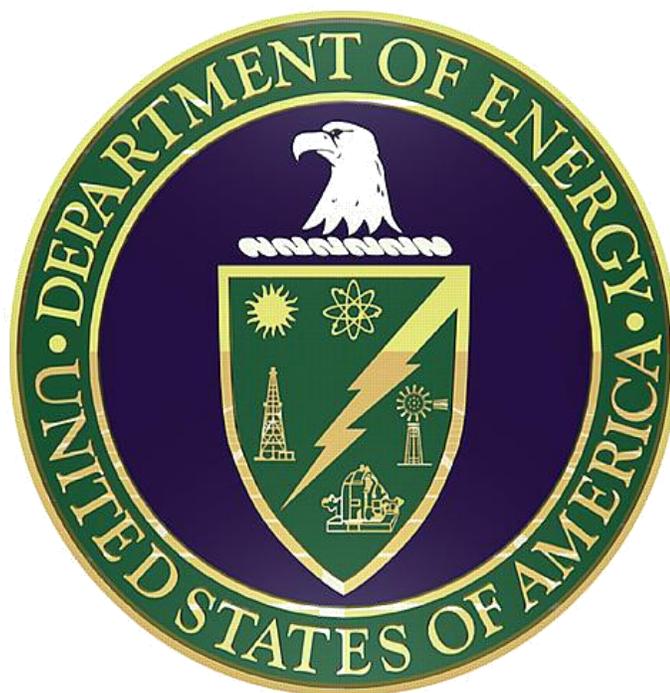


SAFEGUARDS AND SECURITY SURVEY AND SELF-ASSESSMENT TOOLKIT



U.S. Department of Energy
Office of Health, Safety and Security

October 2006

AVAILABLE ONLINE AT:
<http://www.directives.doe.gov>
Security

Initiated by:
Office of Health Safety and

1.0 INTRODUCTION

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

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

This Toolkit is a living document, and it will be modified on an as-needed basis. In order to make it user friendly, we have hyperlinked the Table of Contents. Should you have tools that have proven effective at your site or facility, please forward them to the Office of Policy (HS-61), Office of Health, Safety and Security for inclusion in this Toolkit. Thank you to those who have contributed to the Toolkit and making this document a valuable tool.

Table of Contents

1.0 Introduction

<u>Acronyms</u>	5
-----------------------	---

2.0 Planning Tools

2.1 <u>Sample In-Briefing</u>	9
2.2 <u>Sample Survey Plan Format</u>	12
2.3 <u>Documents for Possible Review</u>	13
2.4 <u>Sample Notification Memo 1</u>	18
<u>Sample Notification Memo 2</u>	19
<u>Sample Documentation Request</u> (attachment to Notification memo 2)	20
<u>Sample Notification Memo 3</u>	22
<u>Sample Presurvey Questionnaire/Data Call</u> (attachment to Notification memo 3)	23
2.5 <u>Sample Accommodation Request</u> (attachment to Notification memo 3)	28
2.6 <u>Sample Training/Safety Checklists for Offsite Assistance</u>	29

3.0 Conduct Tools

3.1 <u>Sample Worksheet</u>	31
3.2 <u>Instructions for Completing the Survey Worksheet</u>	32
3.3 <u>Sampling Methodologies</u>	35
3.4 <u>Sample Performance Test Safety Plan</u>	41
3.5 <u>Sample Performance Test Plan</u>	46

4.0 Topical Area Tools

A. Program Management and Support

<u>Subtopical Elements/Areas for Consideration</u>	49
<u>A.1 Program Management and Support</u>	52
<u>A.2 Safeguards and Security Planning and Procedures</u>	54
<u>A.3 Management Control</u>	56
<u>A.4 Program-Wide Support</u>	58
<u>Sample Worksheets & Performance Tests</u>	62

B. Protective Force

<u>Subtopical Elements/Areas for Consideration</u>	69
<u>B.1 Management</u>	70
<u>B.2 Training</u>	71
<u>B.3 Duties</u>	72
<u>B.4 Facilities and Equipment</u>	74
<u>Sample Worksheets & Performance Tests</u>	76

C. Physical Security

<u>Subtopical Elements/Areas for Consideration</u>	78
<u>C.1 Access Controls</u>	79
<u>C.2 Intrusion Detection and Assessment Systems</u>	81
<u>C.3 Barriers and Delay Mechanisms</u>	83
<u>C.4 Testing and Maintenance</u>	84
<u>C.5 Communications</u>	85
<u>Sample Worksheets & Performance Tests</u>	86

D. Information Protection

<u>Subtopical Elements/Areas for Consideration</u>	89
<u>D.1 Basic Requirements</u>	90
<u>D.2 Technical Surveillance Countermeasures</u>	91
<u>D.3 Operations Security</u>	93
<u>D.4 Classification Guidance</u>	94
<u>D.5 Classified Matter Protection and Control</u>	95
<u>Sample Worksheets & Performance Tests</u>	97

E. Cyber Security

<u>Subtopical Elements/Areas for Consideration</u>	114
<u>E.1 Classified Cyber Security</u>	115
<u>E.2 Telecommunications Security</u>	118
<u>E.3 Unclassified Cyber Security</u>	120
<u>Sample Worksheets & Performance Tests</u>	122

F. Personnel Security Program

<u>Subtopical Elements/Areas for Consideration</u>	123
<u>F.1 Access Authorizations</u>	124
<u>F.2 Human Reliability Program</u>	126
<u>F.3 Control of Classified Visits</u>	128
<u>F.4 Safeguards and Security Awareness</u>	130
<u>Sample Worksheets & Performance Tests</u>	132

G. Unclassified Visits and Assignments by Foreign Nationals

<u>Subtopical Elements/Areas for Consideration</u>	133
<u>G.1 Sponsor Program Management and Administration</u>	134
<u>G.2 Counterintelligence Requirements</u>	136
<u>G.3 Export Control/Technology Transfer Requirements</u>	138
<u>G.4 Security Requirements</u>	139
<u>G.5 Approvals and Reporting</u>	140
<u>Sample Worksheets & Performance Tests</u>	142

H. Nuclear Materials Control and Accountability

<u>Subtopical Elements/Areas for Consideration</u>	145
<u>H.1 Program Administration</u>	147

H.2 Material Accountability	149
H.3 Material Control	151
Sample Worksheets & Performance Tests	153

5.0 [Post-Survey Tools](#)

5.1 Sample Report Format	162
5.2 Sample Termination Survey Report	165
5.3 Report Writing Guide	167
5.4 Sample Exit Briefing	177
5.5 Sample Transmittal Memorandum	179
5.6 DOE F 470.8, Survey/Inspection Report Form	180
5.7 Sample Corrective Action Plan	181
5.8 Sample Root Cause Analysis Form	183
5.9 Sample Request for Finding Closure/Validation	184

Additional information specific to each topical area, such as additional limited scope performance tests, safety plans, random sample methodologies, and data collection forms, may also be found in the Inspector Guides developed by the Office of Independent Oversight (HS-60) at <http://www.ssa.doe.gov/sp40/sp41/docs.html>.

Acronyms

The following list of acronyms includes those that may not specifically appear in this toolkit. However, it would be beneficial to become familiar with the terms, as they will be used in the field and during the conduct of surveys. For a complete listing of acronyms and abbreviations related to DOE's Safeguards and Security Program, please refer to [DOE M 470.4-7](#), *Safeguards and Security Program References*.

ACREM	Accountable Classified Removable Electronic Media
BMS	Balanced Magnetic Switch
C&A	Certification and Accreditation
CAS	Central Alarm Station
CCI	Controlled Cryptographic Item
CCTV	Closed-Circuit Television
CFR	Code of Federal Regulations
CFRD	Classified Formerly Restricted Data
CGS	Classification Guides System
CI	Counterintelligence
CMPC	Classified Matter Protection and Control
CNSI	Confidential/National Security Information
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
CSCS	Contract Security Classification Specification
CSPP	Cyber Security Program Plan
DAA	Designated Approving Authority
DBT	Design Basis Threat
DC	Derivative Classifier
DD	Derivative Declassifier
DNA	Does Not Apply
DOE	U.S. Department of Energy
EOC	Emergency Operations Center
ESM	Electronic Storage Media
FACTS	Foreign Access Central Tracking System
FAR	False Alarm Rate
FDAR	Facility Data and Approval Record
FN	Foreign Nationals
FNVA	Foreign National Visit Administration
FOCI	Foreign Ownership, Control, or Influence
FRAM	Functions, Responsibilities and Authorities Manual
FRD	Formerly Restricted Data
FSO	Facility Security Officer
GAO	Government Accountability Office
GSA	U.S. General Services Administration
HQ	Headquarters
HRP	Human Reliability Program
HS-60	Office of Independent Oversight

HS-61	Office of Security Evaluations
IG	Inspector General
IOSC	Incidents of Security Concern
IP	Internet Protocol
IS	Information Systems
ISOM	Information Systems Security Operations Manager
ISPM	Information System Security Program Manager
ISSM	Information Systems Security Site Manager
ISSO	Information Systems Security Officer
ISSP	Information System Security Plan
JTA	Job Task Analyses
LLEA	Local Law Enforcement Agencies
LSPT	Limited Scope Performance Test
MAA	Material Access Area
MBA	Material Balance Area
MC&A	Material Control and Accountability
MOA	Memorandum of Agreement
MOU	Memorandum of Understanding
NAR	Nuisance Alarm Rate
NATO	North Atlantic Treaty Organization
NMMSS	Nuclear Material Management and Safeguards System
NSA	National Security Agency
NSI	National Security Information
NTC	National Training Center
OODEP	Owners, Officers, Directors, and Executive Personnel
OPSEC	Operations Security
ORO	Oak Ridge Operations
OUO	Official Use Only
PCSP	Program Cyber Security Plan
PF	Protective Force
PIDAS	Perimeter Intrusion Detection and Assessment System
PIV	Personal Identity Verification
POC	Point-of-contact
RD	Restricted Data
RFI	Representatives of Foreign Interests
RIS	Reporting Identification Symbol
RO	Reviewing Official
RQL	Rejectable Quantity Level
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
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
SSMP	Safeguards and Security Management Plan
SSO	Special Security Officer
SSP	Site Security Plan
SSPS	Safeguards and Security Periodic Survey
SSSP	Site Safeguards and Security Plan
STE	Secure Telephone Equipment
STU	Secure Telephone Unit
TID	Tamper Indicating Device
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
UCNI	Unclassified Controlled Nuclear Information
VA	Vulnerability Assessment
WFO	Work for Others

2.0 PLANNING TOOLS

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

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

2.1 Sample In-Briefing

Classification

SAFEGUARDS AND SECURITY PERIODIC SURVEY

Name of Facility Being Surveyed
Facility Code

Dates of Survey

Conducted by
Surveying Office



Surveying Office

Classification

Classification

OBJECTIVE

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



Surveying Office

Classification

Classification

SCOPE & METHODOLOGIES

SCOPE - Assess status of all S&S topical areas

- Compliance
- Performance
- Comprehensiveness

METHODOLOGIES

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



Surveying Office

Classification

Classification

Topical Area Leads & POCs

Ph Pg

Survey Team Lead

Name, Survey Team Lead
Name, Contractor Point of Contact

Program Management & Support

Name, Survey Topical Lead
Name, Contractor Point of Contact

Protective Force

Name, Survey Topical Lead
Name, Contractor Point of Contact

Continue for each topical area.



Surveying Office

Classification

Classification

Schedule of Activities

Data Gathering

M/D/Y through M/D/Y

Report Writing

M/D/Y through M/D/Y

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

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

Surveying Office

Classification



Classification

Schedule of Activities (cont.)

Exit briefing:

Date: (M/D/Y)

Time: (Time)

Conference Room: (Number)

Building: (Number)

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

Surveying Office

Classification



2.2 Sample Survey Plan Format

The following information should be included in the survey plan:

1. Title of survey
2. Location of facility
3. Purpose of survey
4. Survey dates
5. General facility information /description
 - a. Facility data
 - b. Work/activities performed
 - c. Operating organization (contractor)
 - d. S&S interests
 - e. Work for Others (WFO) or other security activities
6. Scope of survey
 - 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. Survey planning and preparation
 - a. Performance tests (associated safety plans)
 - b. Survey guide information
 - c. Presurvey information
8. Survey conduct—approach and methodology
 - a. Documents to be reviewed
 - b. Performance tests
 - c. Individuals to be interviewed
9. Schedule of activities
 - a. Survey schedule
 - b. In-briefing information
 - c. Coordinating instructions
 - d. Exit briefing
 - e. Schedule for report development
10. Team composition/assignments
 - a. Team members
 - b. Assignments/responsibilities
 - c. Contractor support
 - d. Points-of-contact at the facility
11. Authority/governing documents
 - a. Directives
 - b. References (unclassified/classified)
12. Survey report format
13. Administration, support, and logistics
 - a. Work facilities
 - b. Transportation
 - c. Computer support
 - d. Administrative support
 - e. Classification support
 - f. Training requirements
14. Appendices
 - a. Performance tests (including Safety Plans)
 - b. Survey guides
 - c. Forms

2.3 Documents for Possible Review

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

Program Management and Support

- Organization charts depicting the Safeguards and Security (S&S) management structure and S&S functional structure
- Documents depicting responsibilities and authorities of S&S management
- Position descriptions for S&S management
- Local operating instructions for the implementation of S&S programs
- Supplemental orders/directives implementing S&S programs
- Site Safeguards and Security Plan (SSSP) or Site Security Plan (SSP)
- Emergency management plans
- Survey reports, inspection reports, Government Accountability Office and Inspector General audit/appraisal reports, self-assessment reports
- Training records
- The contract, including the Statement of Work
- List of all subcontractors and consultants conducting work for the contractor
- List of U.S. Department of Energy (DOE) directives and security clauses that have been incorporated into applicable contracts
- Approved and pending deviations to DOE directives
- Copy of the facility registration
- Applicable Memoranda of Understanding (MOU)/Agreement (MOA)
- The completed Foreign Ownership, Control or Influence (FOCI) questionnaire
- The Owners, Officers, Directors, and Executive Personnel (OODEP) list
- The dates of all applicable FOCI determinations
- A copy of the contractor's records of all contracts and subcontracts involving access authorizations
- A copy of the contractor's procedures implementing FOCI
- Vulnerability Assessment (VA) reports
- Contingency plans
- Survey and self-assessment program procedures
- Corrective action plans and status updates for all open deficiencies
- Finding/deficiency corrective action validation and closing procedures
- Incidents of Security Concern procedure, including initial notification and inquiry reports
- Contract Security Classification Specification (CSCS)
- Facility Data and Approval Record (FDAR)
- Copy of the approved Performance Assurance Program Plan
- List of essential elements documented in the Performance Assurance program and the testing schedule for each
- Documentation of the integrated contractor assurance system required by DOE O 226.1

Protective Force (PF)

- Organization and function charts
- PF general, special and post orders
- PF shift schedules and post assignments
- PF standard equipment issuance (Security Police Officer [SPO] I, II, III, and Special Response Team [SRT])
- PF weapons and ammunition inventories

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

Physical Security

- Organization and function charts
- Lock and key records and procedures
- Automated access control system records and procedures (including biometric access input as well as access credential issuances (e.g., keycards, tokens))
- Barrier maintenance procedures/records
- Property control procedures
- Access control procedures
- Local performance testing plans and procedures
- Physical security system description(s) and location(s)
- Intrusion detection system (IDS) maintenance and testing records and procedures
- Unscheduled alarm reports
- Central Alarm Station (CAS)/Secondary Alarm Station (SAS) procedures (interface description)
- Emergency response for CAS/SAS recovery
- Emergency power systems (uninterruptible power supply system)
- Compensatory procedures for equipment outages
- Security container documentation and maintenance records
- Automated systems description and procedures
 - Manual

- Procedures
- Controls
- Calibration and testing procedures and records (e.g., X-ray, metal detectors, IDS)
- Inspection procedures
- Limited Scope Performance Test (LSPT) results

Information Protection

- Organization and function charts
- Training records
- Technical surveillance countermeasure (TSCM) survey reports
- Site inventory of accredited systems, showing property tag number, the accrediting authority, and most recent accreditation date for each
- Formal assignments of TSCM Operations Manager 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) Plan
- OPSEC procedures
- OPSEC program files
- Local threat statement
- Critical Program Information
- Counter-Imagery Program Plan (if applicable)
- Number of derivative classifiers and declassifiers
- Appointment letters (e.g., Inquiry Officer, custodians)
- Training records, reports, and lesson plans
- Classification guidance
- Classified Matter Protection and Control (CMPC) procedures
- Control station procedures
- List of classified holdings, including documents and matter
- List of accountable classified removable electronic media (CREM)
- List of authorized CREM custodians
- Number of Special Access Programs (SAPs)

Cyber Security

- Appointment letters for the Designated Approving Authority (DAA), Classified Information Systems Security Operations Manager (ISOM), and Information Systems Security Site Manager (ISSM)
- List of all accredited classified information systems at the site or facility (reference above)
- Information system (IS) plans for major systems and networks, and a sample of plans for distributed and stand-alone systems, including a master plan, if applicable
- Plan approval, test, certification, and accreditation documentation for the systems or networks covered by the plans requested
- Any site deviations from the generic DOE threat statement and risk assessment documentation, including identification of any unique site threats or risks (cyber security with specific statement of threat)
- Site cyber security policies, procedures, or handbooks
- Computer security training materials used to train Information System Security Officers (ISSOs), users, and computer security escorts

- Criteria and decision documents concerning the need for a continuity of operations plan (including contingency planning and disaster recovery planning) for each IS. A statement of the decision and the basis for that decision should be documented in the IS plans
- Continuity of operations plans for the systems identified by the continuity of operations decision, with appropriate management signatures
- Results from continuity of operations plan tests and, if appropriate, procedures for backup of all essential data, utility, and operating system files (including network interface software) on a regular basis
- Policies regarding the installation and/or use of third-party software on the IS, including public-domain software
- A summary of security incidents involving the IS, including severity and resultant actions
- Site-specific procedures related to IS involvement in the design and development of a new IS
- Procedures related to the site configuration management program
- Procedures implemented to authorize user access to IS resources and need-to-know for specific information
- Qualifications and required training of the ISOM and/or the ISSM
- Procedures for configuration management of the IS
- List of all Communications Security (COMSEC) custodians and alternates
- Records of appointments and changes of COMSEC Control Officers, COMSEC Custodians, COMSEC Subcustodians, alternates, and any persons having access to COMSEC materials
- List of access authorizations for the individuals listed above
- Last COMSEC survey completed by DOE Headquarters (DOE-HQ)
- Training records/material for personnel engaged in cryptographic duties
- COMSEC procedures

Personnel Security

- Local procedures for terminations, leave of absences, reinstating clearances, clearance processing, exit briefing process
- Contractor access authorization requests
- Sample training curriculum, briefing materials
- Previous findings and corrective action plans
- Reciprocal access authorization documentation
- Awareness tools (posters, newsletters)
- Security infraction and violation records
- Request for visit or access approval (notification and approval of incoming and outgoing classified visits records)
- Visitor control logs
- Local visitor control procedures
- Central Personnel Clearance Index (CPCI) list of individuals overdue for reinvestigation
- Drug testing/handling procedures
- Drug testing records
- Human Reliability Program (HRP) participants
- HRP criteria/plans/procedures
- Random test procedures
- List of individuals on leaves of absence and the associated procedures for tracking
- List of inactive classified contracts
- List of personnel with access authorizations and the associated contract
- List of clearances terminated during the survey period

- List of all access authorizations being held by the contractor, including all contractors that have cleared employees conducting work at the facility. This list can come from the DOE CPCI of access authorizations held by the contractor. The CPCI and contractor lists, including the current OODEPs' list, should be compared for discrepancies.

Unclassified Visits and Assignments by Foreign Nationals (FNs)

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

Nuclear Material Control and Accountability (MC&A)

- MC&A plans and procedures
- Training records, reports, and lesson plans
- Performance tests
- Categorization process documentation
- Incident reporting process and procedures
- Emergency response plans and facility procedures
- Database descriptions
- Material Balance Area (MBA) account structure
- Material transfer records
- Internal control procedures
- Nuclear Material Management and Safeguards System (NMMSS) reports
- Shipper/receiver difference procedures and records
- Material control indicator program
- Inventory difference program
- Materials containment documentation
- Facility procedures
- Material access program
- Authorization access lists
- Search procedures
- Material surveillance procedures
- Portal monitor records and procedures
- Daily administrative check program and procedures
- Tamper indicating device program

2.4 Sample Notification Memos

2.4.1 Notification and Data Call

DATE:

TO:

FROM:

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

This memorandum is to formally notify you that a representative of the [Surveying Organization] will conduct a periodic S&S survey of the XYZ facility and its satellite offices during the period [Date–Date]. The survey will be conducted in accordance with the requirements of DOE M 470.4-1, *Safeguards and Security Program Planning and Management*, Section G. The topical areas to be evaluated include:

- Program Management and Support
- Protective Force
- Physical Security
- Information Protection
- Cyber Security
- Personnel Security
- Unclassified Visits and Assignments by Foreign Nationals
- Nuclear Materials Control and Accountability.

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

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

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

2 Attachments

2.4.2 Safeguards and Security Periodic Survey

DATE:

TO:

FROM:

SUBJECT: Safeguards and Security Periodic Survey (SSPS)

The [Surveying Organization] will conduct an SSPS of the [Organization to be Surveyed] during the period of [Date–Date]. This will be a comprehensive survey and will be conducted in accordance with Section G of DOE M 470.4-1, *Safeguards and Security Program Planning and Management*. The survey will examine the compliance and performance of safeguards and security programs with DOE policy and will encompass all topical areas on DOE F 470.8, *Survey/Inspection Report Form*.

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

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

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

Attachment

Sample Documentation Request

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

Program Management and Support

1. Organization chart(s) or listings with brief description of organizations functions and responsibilities
2. Site Safeguards and Security Plan or Site Security Plan status
3. Copy of most recent self-assessment report
4. Copy of findings/corrective action plan tracking procedures
5. Current status of all open and closed findings/corrective action plans since the last survey (including Office of Independent Oversight (HS-60), Government Accountability Office and Inspector General) as well as all on- and off-site facilities
6. List of and current status of all approved policy deviations
7. List of all subcontractors performing work (name of company, contract number, names of individuals with access authorizations)
8. Foreign Ownership, Control, or Influence procedures

Protective Force

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

Physical Protection

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

Information Protection

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

Cyber Security

1. Master personal computer security plan and list of all classified systems
2. Site-specific computer security policies, procedures, and plans
3. Information System plans for major systems and networks

Personnel Security

1. List of all assigned (cleared) employees/subcontractors who have traveled to sensitive countries (official and unofficial)
2. List of all visits and assignments of foreign nationals
3. List of all subcontractors
4. List of uncleared visitors
5. List of outgoing classified visits
6. List of all incoming classified visitors
7. List of Human Reliability Program participants
8. List of terminated clearances (including name, date termination statement signed, date clearance terminated, Central Personnel Clearance Index [CPCI] number)

Unclassified Visits and Assignments by Foreign Nationals (FNs)

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

Nuclear Material Control and Accountability (MC&A)

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

2.4.3 Safeguards and Security Survey of XYZ Company

Date:

To:

From:

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

This memorandum confirms informal arrangements between [Surveying Office] and [Organization to be Surveyed] Safeguards and Security Organization personnel that established [Date–Date] as the dates for the [Surveying Office] S&S survey of the [Organization to be Surveyed] facility. The survey will be directed toward the requirements of DOE M 470.4-1, *Safeguards and Security Program Planning and Management*, Section G, as well as other applicable DOE directives.

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

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

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

Enclosures

Sample Presurvey Questionnaire/ Data Call

The survey team needs the following to be delivered to Room XXX no later than [Date] for the XYZ facility and satellite office buildings: (*Note: If the current information is contained in the Site Safeguards and Security Plan (SSSP), annotate this list with the formal reference to the appropriate section of the plan. If the reference is contained in another plan, provide formal reference and/or a copy of the specific plan and/or formal reference to where it is being provided within this data call.*)

A. PROGRAM MANAGEMENT AND SUPPORT

1. A list reflecting security staffing since January 2005. This list should include name of person, date of hire/termination, job title, and security functions (responsibilities)
2. Copies of all memoranda of understanding and management agreements relating to safeguards and security (S&S) programs
3. A copy of all internal operations procedures/practices index
4. Copies of the most recent S&S risk assessments, including documentation reflecting risk determination methodology
5. A list of all security training courses that have been approved as part of the training approval plan process
6. A list that reflects the training courses taken by personnel responsible for security functions. Include name, title of course, number of hours, and date of completion
7. Copies of any procedures or other guidance pertaining to the identification and development of S&S training
8. A list of all facilities (copies of Facility Data and Approval Records are acceptable) where the *XXX DOE Field/Operations Office* is identified as the Lead Responsible Office.
9. A list of all classified activities (including the contract), classification level and category of the activity, identification by office and/or Operations Office, identification by contract number, purchase order number, task statement, or proposal number (including classified Work for Others) (*Note: Copies of the Contract Security Classification Specification (CSCS) form may be used in lieu of a listing.*)
10. List of all terminated and completed contracts since January 2005. This listing should identify the company/vendor, address/location, Contracting Officer name, organization, office location, and telephone number (*Note: Copies of terminated CSCS forms may be used in lieu of a listing.*)
11. List of pending Foreign Ownership, Control, or Influence (FOCI) determinations
12. List of FOCI determinations completed since January 2005
13. List of FOCI approved companies, including the FOCI determination date and date of the latest FOCI update
14. A copy of any desktop procedures or other formal XYZ-originated guidance documentation used for the development of the SSSP and other security-related planning documents
15. A list that reflects all S&S plans (e.g., response, emergency, and contingency plans) including title, date, and approval vehicle. Also list any draft plans and plans pending approval
16. Copies of all XYZ-generated guidance or direction (hardcopy or electronic) provided for the conduct of self-assessments and other internal evaluations since the publication of the current DOE directives
17. List of all open findings
18. List of open findings pending validation
19. Copy of Incidents of Security Concern program procedures

20. A list of all security incidents, including computer security incidents, occurring since January 2005. This list should identify the date of the incident, the date of the inquiry report, and the nature of the incident
21. Copies of award fee data (Award Fee Plan, performance criteria)

B. PROTECTIVE FORCE (PF)

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

C. PHYSICAL SECURITY

1. Copy of key control and property pass procedures
2. Copy of documentation that reflects the total value of capital and sensitive/equipment items (include precious metals as applicable)
3. Listing of all controlled substances and locations, including copies of Drug Enforcement Agency certificates
4. Listing that identifies all security alarm transmission and monitoring systems, including type, model, manufacturer, and purpose for each (i.e., describe the DOE assets being protected)
5. List of all alarm points identified by system application (Argus or Litton) and location that provides protection for classified matter and property
6. Copy of the approved alarm test plan and a copy of the DOE approval correspondence
7. Copy of the procedures for making changes to alarm transmission/monitoring systems databases or software
8. Copies of reports since January 2005 of unscheduled alarm activations
9. Copy of false alarm rate and nuisance alarm rate since January 2005
10. Copies of maintenance procedures and test results since January 2005

D. INFORMATION PROTECTION

1. A list of all current XYZ original and derivative classifiers, as well as Official Use Only and Unclassified Controlled Nuclear Information
2. A list of reviewing officials, including name, title, organization, office location, and telephone number
3. A list of all classification guides, including title and date
4. A list of all XYZ shipping/mailroom logs pertaining to the transmission of classified matter since January 2005
5. A list of all areas authorized for processing and storage of classified information/matter, including the classification level authorized and functions performed in each area
6. List of all classified document control stations, including the custodian names, organization, location, and telephone extension.
7. Copy of Classified Matter Protection and Control procedures (marking, destruction)
8. List of all classified removable electronic media (CREM)
9. List of all CREM custodians
10. Copy of DOE-approved Technical Surveillance Countermeasures (TSCM) Plan
11. Copy of the TSCM officers appointment memoranda
12. Copy of the site-wide procedures for the control and use of potential TSCM equipment
13. Copy of the procedures controlling TSCM equipment, the DOE approval for purchasing and controlling TSCM equipment, and an inventory listing, if appropriate
14. Copy of Operations Security (OPSEC) Plan
15. Copy of OPSEC assessment and review reports conducted since January 2005
16. List of contractors (on- and off-site) under the OPSEC program
17. Copy of OPSEC working group meeting minutes for meetings conducted since January 2005

E. CYBER SECURITY

1. Any automated information systems security manager (ISSM) or information systems security officer appointment letters
2. Copies of system security tests, with results since January 2005
3. Policy on incident reporting
4. Description of training conducted (syllabus)
5. Procedures for and determinations of major applications
6. Site computer security handbook (if applicable)
7. Procedures for implementing management controls

8. Copy of the operational procedures for unclassified video teleconferencing systems
9. List of all systems currently approved and pending approval
10. List of risk assessments and procedures for classified video conferencing
11. List of all Communications Security (COMSEC) custodians and alternates and their access authorizations
12. Last COMSEC survey completed by DOE-HQ
13. Training records/material for personnel engaged in cryptographic duties
14. COMSEC procedures (standard operating procedures)

F. PERSONNEL SECURITY

1. A list of all cleared personnel whose access authorization has been terminated since January 2005 (Note: This list should include the date of termination, name of person, and organization for whom individual worked.)
2. A list of names of all consultants/vendors issued security clearances that conduct business with XYZ
3. A list of all individuals by name and clearance number terminated for cause
4. A list of individuals by name and clearance number who have had clearances canceled/terminated prior to completion of the background investigation
5. A list by name and clearance number of all foreign nationals who are/were clearance applicants or incumbents. Include in the listing the country of origin and level of clearance
6. A list by name and clearance number of all dual citizens processed for access authorization (clearance) since January 2005
7. A list of individuals on leave-of-absence or extended leave. This list should include name, clearance number, reason for leave, date leave commenced, expected date of return to duty, and/or date of termination
8. Have available each report submitted for derogatory information since January 2005
9. Copy of attendance records for initial, comprehensive, and termination briefings for all contractor employees since January 2005
10. Copies of most current security education briefing/lesson plans for initial, comprehensive, refresher, and termination briefings since January 2005
11. Copy of the test and/or measurement mechanism associated with the most current refresher briefing
12. Documentation describing the badging system and operating procedures for classified visits. Provide examples of all badge types in use
13. Copy of the procedures for administering incoming and outgoing classified visits
14. Copies of DOE F 5631.20 since January 2005
15. Classified visitor logs since January 2005
16. Copies or log of classified visitor badge requests since January 2005
17. List of all personnel, by name and clearance number, enrolled in the personnel assurance program
18. A listing of the number and dates of each positive substance abuse test report
19. A copy of drug test policy
20. A list of all personnel, by name and clearance number, enrolled in the Human Reliability Program (HRP)
21. List of all individuals, by name and clearance number, removed from the HRP since January 2005
22. Justifications for HRP positions and date of last review
23. Procedures for Personal Identify Verification process

G. UNCLASSIFIED VISITS AND ASSIGNMENTS BY FOREIGN NATIONALS (FNs)

1. Lists of all host reports submitted since January 2005 including date submitted
2. Local procedures for requesting, processing, and approving visits and assignments
3. List of FN visitors or assignees, including hosts, for survey period
4. Incident reports involving foreign nationals
5. Requests for foreign national visits
6. Indices checks
7. Documentation authorizing approval for specific categories of visits and assignments
8. Sensitive country listings

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

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

2.5 Sample Accommodation Request

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

- Two conference rooms or a two-office suite with tables and seating for 15 to 20 people
- Four desktop computers running Microsoft® Windows® 2003 operating system, loaded with Microsoft Word 7.0, and two Hewlett-Packard LaserJet printers
- Telephones with outside lines and official site phone books
- White board and associated supplies
- U.S. General Services Administration-approved security container (with appropriate markings and required forms)
- Office supplies (staplers, scissors, tape, disks, etc.)
- Copies of XYZ procedures and policy manuals related to survey topics, SSSP, Vulnerability Assessments, and applicable DOE directives.

2.6 Sample Training/Safety Checklist

Training/Safety Checklist for Offsite Assistance			
Team Member: Date Arriving Onsite: Topical Area: Area Access Required: Material Access Area (MAA) 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: <hr/> Topical Area Lead Date			
<hr/> Survey Team Leader Date			

3.0 CONDUCT TOOLS

This section contains tools and forms that have been developed and field-tested by survey and self-assessment teams.

- Sample Worksheet
- Instructions for Completing the Survey Worksheet
- Sampling Methodology
- Sample Safety Plan
- Sample Performance Test Plan

3.1 Sample Worksheet

CLASSIFICATION

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

CLASSIFICATION

3.2 Instructions for Completing the Survey Worksheet

ORIGINATION DATE: Date form completed.

RESPONSIBLE AGENCY: Agency responsible for implementing corrective actions.

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

Example of a finding number:

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

- 1: the date of the survey/inspection (year/month/day)
- 2: the office responsible for correcting the finding
- 3: the facility code of the facility surveyed/inspected
- 4: the type of survey (e.g., Safeguards and Security Initial Survey, Office of Independent Oversight (HS-60), Inspector Government Accountability Office)
- 5: the subtopical area code
- 6: the sequential number of an individual finding within the topical area
- 7: the facility code of another facility if a finding was issued to it during the survey

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

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

CODE	TYPE OF DOCUMENT OR ORGANIZATION
EPR	Excluded Parent Review
GAO	Government Accountability Office Reports
IG	Inspector General Reports
NPR	Non-possessing Review
OSE	Security Evaluations Inspections
SPEC	Special Surveys
SSIS	Safeguards and Security Initial Surveys
SSPS	Safeguards and Security Periodic Surveys
SSTS	Termination Surveys
TSCM	TSCM Reports

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

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

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

For example:

A review was conducted of all current classified contracts at XYZ. This list was compared to a current badge listing, dated 3-1-05, which showed employees, by company, who currently hold a DOE access authorization. This comparison revealed that individuals holding access authorizations are employed by organizations that do not have current favorable Foreign Ownership, Control, or Influence (FOCI) determinations on file with XYZ.

Based on the FOCI report provided by XYZ personnel, dated 3-1-05, and the employee list by contractor, dated 3-1-05; TCY Company currently holds 7 “Q” clearances and Smith Manufacturing currently holds five “Q” clearances. Neither organization has an approved FOCI determination on file with XYZ.

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

For example:

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

IMPACT Statement: Clearly identify the impact of the deficiency.

DOE DIRECTIVE: Each finding is to have alpha/numeric references to the DOE directive(s), or other documents that identify the requirement(s) not being met in the finding. This reference should be written as DOE O XXX.XX or DOE M XXX.XX-X followed by the chapter, section, and subsection reference numbers and/or letters (e.g., DOE M 470.1-4 Section A.4.(b)).

OTHER: Identify alternative sources stating the requirement, (e.g., specific procedures and plans).

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

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

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

3.3 Sampling Methodologies

STATISTICAL SAMPLING METHODOLOGY

The following statistical sampling methodology can be readily applied to most safeguards and security 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 can be located in its entirety by accessing the DOE Office of Security Evaluations (HS-61), Office of Independent Oversight, Classified Matter Protection and Control Inspectors Guide at <http://www.ssa.doe.gov/sp40/guidedocs/0207cmpr/200509cmpr.pdf>.

Introduction

The Office of Independent Oversight (HS-60) conducts inspections to assess the effectiveness of U.S. Department of Energy safeguards and security 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-percent 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. 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-percent inspection because of the limited time and other resources available. 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 statement of 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 on these items are usually quite 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 at the site, then the population is only those documents at these 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-percent level of confidence are correct 95 percent of the time. Thus, if a random sample of 200 items is selected and zero defects are observed, it can be stated with 95-percent confidence that the true proportion of defectives in the population is at most 0.015 (1.5 percent). In this same case of a sample

of 200 items and zero defects, it can also be stated with 80-percent confidence that the true proportion of defectives in the population is at most 0.008 (0.8 percent). 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 5-percent chance of being wrong versus a 20-percent 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 from which inferences are drawn 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 of documents is selected so that the probability of individual documents being chosen as the sample is the same as that 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 corresponding to that order. 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, the use of computer systems 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. Computer programs for generating random numbers 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 computer 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

this set of random 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 the purposes of 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 front-check document accountability performance 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 2 documents cannot be located, then one can state with 95-percent confidence that no more than 3.114 percent of the total accountable document inventory is unaccounted for. Or one can state with 95-percent confidence that at least 0.178 percent 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-percent confident that at least 178 accountable documents are unaccounted for in this system. Finally, one can also make the statement with 90-percent confidence that the number of unaccounted-for documents in this system is somewhere between 0.178 percent and 3.114 percent, 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 percent used in the previous two statements to 90 percent. 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)

Table 1. (Continued)

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)			

3.4 Sample Performance Test Safety Plan

SAMPLE PERFORMANCE TEST SAFETY PLAN

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

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

Name _____

Signature _____

Position _____

Date _____

Detection of Contraband and Prohibited Items

(Type of Performance Test)

Ongoing 365 Days per Year; 24 Hours per Day

(Performance Test Date and Time)

Detection of Contraband and Prohibited Items, John Doe

(Safety Plan Name and Person Preparing)

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

Scenario:

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

purpose of the LSPTs is to evaluate the ability of the PF to detect contraband and prohibited items prior to their release into the aforementioned areas. The LSPTs are not designed to test what actions the PF undertakes once they detect or fail to detect the contraband or prohibited item.

IN THE EVENT OF AN ACTUAL SECURITY ALARM OR SECURITY INCIDENT, THE CONTROLLER WILL IMMEDIATELY ANNOUNCE AND CONCLUDE THE LSPT, TAKE POSSESSION OF THE TEST ITEM/CONTAINER, AND FOLLOW ALL INSTRUCTIONS ISSUED BY PF PERSONNEL.

Requirements:

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

PF Response:

_____ Yes _____ No

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

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

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

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

X Controllers are located at the exercise location.

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

_____ Prior notification of CAS.

_____ Prior notification of PF.

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

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

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

List other specific safety measures below:

1. All personnel attempting to gain entrance into one of the identified areas will be briefed on the LSPT objectives and how they should conduct themselves during the LSPT.
2. All contraband or prohibited items will be photographed prior to the initiation of the LSPT.
3. All personnel attempting to gain entry or exit with contraband items will be photographed prior to the initiation of the LSPT.
4. All personnel attempting to gain entry or exit with contraband or prohibited items will be instructed to keep their hands in plain view, not to make any sudden moves, and comply with all instructions given by PF personnel.
5. Only epoxy-encased, DOE cognizant security authority-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 DOE participants, the level of risk is actually below that experienced during normal day-to-day operations.

Radiation Safety Provisions:

- Applicable
- Not applicable

If yes, check those applicable to this LSPT:

- Personnel participating in the LSPT have been briefed concerning radiation safety requirements for the area with which the LSPT will be conducted.
- Personnel will be continuously escorted while in the radiation areas in which the LSPT will be conducted.

List any other specific radiation safety provisions for this LSPT:

Personnel Assignments (list below):

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

Protective Force Appendix Required:

- Yes
- No

DOE Safety Review:

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

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

APPROVALS:

Director, Safety and Health Organization
DOE Cognizant Security Authority

Date _____

Contractor Safety and Health Representative

Date _____

Director, Security Organization
DOE Cognizant Security Authority

Date _____

3.5 Sample Performance Test Plan

SAMPLE PERFORMANCE TEST PLAN

TEST OBJECTIVE

This performance test is designed to

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

SCENARIO DESCRIPTION

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

TEST METHODOLOGY AND EVALUATION CRITERIA

1. A simulated SRD document consisting of approximately five pages of unclassified text and drawings shall be placed on the table next to a copy machine located in Building xxx, Room zzz. The document shall be placed in the designated location at approximately 7:30 am.
2. Upon notification of the unattended “classified” document, the CDCO will verify that the individual finding the document completed the following actions:
 - a) Xxxx
 - b) Xxxx
 - c) Xxxx

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

- a) Xxx
- b) Xxx
- c) Xxx

Pass/Fail Criteria

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

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

TEST CONTROLS

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

- Only survey team members involved with the conduct and evaluation of this performance test will be made aware of all information surrounding the conduct of the test.
- There are no additional safety requirements for this performance test. All current facility safety requirements will be adhered to during this performance test.
- This will be a no-notice exercise; therefore, the surveyed organization will not be given any information regarding the conduct of this performance test prior to the test.
- The simulated SRD document used during this exercise will consist of an unclassified document marked at the SRD level with all appropriate markings and covers. There will be no indications to a casual observer that the document is not classified.

RESOURCE REQUIREMENTS

The following resources are needed to conduct this performance test.

- Simulated SRD document
- Identified location to place the document
- Three survey team members to be assigned the following:
 - a) Monitor the document
 - b) Monitor the PF response
 - c) Monitor the CDSCO

TEST COORDINATION REQUIREMENTS

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

OPERATIONAL IMPACT(S) OF TESTING PROGRAM

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

COMPENSATORY MEASURES

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

COORDINATION AND APPROVAL PROCESS

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

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

- A participant log containing name, job title, organization, telephone number, and date will be completed by all participants of this exercise.
- A data collection form containing the date, performance test type, name of evaluator, and chronological description of actions observed will be completed by all survey team members participating in the evaluation of this performance test.

REFERENCES

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

- DOE M 470.1-4, *Information Security Program*
- Information Security Standard Operating Procedure #
- PF Standard Operating Procedure #
- PF Post Order #

SURVEY TEAM LEADER: _____

DATE: _____

(Signature of Approval)

4.0 TOPICAL AREA TOOLS

This section contains items that can be used to assist a team member in conducting surveys and self-assessments by providing a series of guidelines, such as: (1) subtopical areas, (2) current directives, (3) sample documents list, (4) listing of sample interview candidates, and (5) suggested interview questions. Sample worksheets and/or performance tests are also provided at the end of each topical area to assist in survey and self-assessment activities.

A. PROGRAM MANAGEMENT AND SUPPORT

Subtopical Areas to Program Management and Support

A.1 PROTECTION PROGRAM MANAGEMENT

- A.1.1 Program Management and Administration
- A.1.2 Resources and Budgeting
- A.1.3 Personnel Development and Training

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

A.3 MANAGEMENT CONTROL

- A.3.1 Surveys and Self-Assessment Programs
- A.3.2 Performance Assurance Program
- A.3.3 Resolution of Findings
- A.3.4 Incident Reporting and Management

A.4 PROGRAM-WIDE SUPPORT

- A.4.1 Facility Approval and Registration of Activities
- A.4.2 Foreign Ownership, Control, or Influence (FOCI)
- A.4.3 Security Management in Contracting

Areas of Consideration

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

Is the organization adequately staffed to accomplish its mission?

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

Has management established an effective and efficient organization structure?

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

Is there a formal, coordinated effort regarding the development, approval, and updates associated with S&S plans?

- Do key S&S plans match procedures actually used at a facility?
- Is there a process in place to ensure S&S plans are reviewed and updated in a timely manner?
- Is expertise available to provide a meaningful review of S&S plans and procedures?
- Are the various protection systems adequately integrated?

Are Vulnerability Assessment (VA) documents and the validation results from performance tests on hand and reviewed during the annual update process?

- What is the status of Site Safeguards and Security Plan (SSSP) activities?
- Is the facility in compliance with contents of the SSSP?
- Are there any deviations in place at the facility? Are they current?
- What methodologies are used for site VAs?
- Are these methodologies adequate to evaluate the site's vulnerabilities in light of the operational environment?

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

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

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

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

Are there any inquiries currently open?

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

Have all applicable security requirements been incorporated into the contract?

- What is the process for incorporating new directives into the site contract?
- How are new directives incorporated into daily implementation for site-related DOE organizations?
- Has the incorporation of any directives been unduly delayed?
- Are all deviations correctly characterized as variances, waivers, or exceptions?

Are there any Work for Others programs being preformed at the facility?

A.1 PROGRAM MANAGEMENT AND SUPPORT

Subtopical areas to Program Management and Support

- A.1.1 Program Management and Administration
- A.1.2 Resources and Budgeting
- A.1.3 Personnel Development and Training

Current Directives:

The following references apply to Program Management and Support:

- DOE O 331.1B, *Employee Performance Management System*, 3-14-01
- DOE O 360.1B, *Federal Employee Training*, 10-11-01
- DOE O 470.4, *Safeguards and Security Program*, 8-26-05
- DOE P 470.1, *Integrated Safeguards and Security Management (ISSM) Policy*, 5-8-01
- DOE M 360.1-1B, *Federal Employee Training Manual*, 10-11-01
- DOE M 470.4-1, *Safeguards and Security Program Planning and Management*, 8-26-05

Sample Document List:

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

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

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

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

Sample Interview Candidates:

Interview candidates may include:

- DOE Operations/Field/Area Office Manager
- DOE Assistant Manager or Director responsible for S&S
- Individual DOE S&S Operational Program Managers

- DOE and contractor management assigned responsibility for developing and implementing this element of the S&S program
- Contracts and Procurement Department management
- Budget and/or Finance Department management
- Human Resources Department management
- Security management assigned responsibility for developing and implementing the S&S programs
- Property management
- Training management
- Contractor Program Managers/Coordinators responsible for S&S training activities (including protective force)

Sample Interview Questions:

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

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

A.2 SAFEGUARDS AND SECURITY PLANNING AND PROCEDURES

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

None

Current Directives:

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

- DOE O 470.4, *Safeguards and Security Program*, 8-26-05
- DOE M 470.4-1, *Safeguards and Security Program Planning and Management*, 8-26-05
- DOE P 470.1, *Integrated Safeguards and Security Management (ISSM) Policy*, 5-8-01

Sample Document List:

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

- Site Safeguards and Security Plan (SSSP) or Site Security Plan (SSP)
- Approved or pending deviations
- Safeguards and Security Information Management System (SSIMS) reports
- Emergency plans
- Contingency plans
- Procedures
- Material Control and Accountability plans
- S&S training plan
- Survey and inspection reports
- Update projects and current compensatory measures
- Data from evidence files
- Current compensatory measures

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

Sample Interview Candidates:

Interview candidates may include:

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

Sample Interview Questions:

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

- How does the facility comply with the contents of the SSSP?
- Is there a local procedure for developing the SSSP?
- What is the protection strategy used at this facility?
- Is the Design Basis Threat used for addressing threats? If not, is this approved in writing?

- What deviations are in place? When were they approved and by whom?
- How do deviations impact protection strategy?
- Have SSPs been developed and implemented for all facilities not requiring an SSSP?
- Are any S&S plans currently being updated? If so, why?
- What process is used for reviewing, approving, and/or updating major S&S plans? Is this process documented?
- Is expertise available to provide a meaningful review of S&S plans and procedures?
- How is integration of major S&S plans ensured?
- Who is responsible for maintaining SSSP/VA data?
- Are VA documents and validation results from performance tests reviewed during the update process or are data obtained from new sources?
- How are changes in policy and/or procedures communicated to those with implementing responsibilities? How are these versions maintained?
- How has management effectively established program direction?
- What is the process used for procedure development/update/approvals?
- How are inspection/survey results used by management to evaluate the effectiveness and viability of S&S plans?

A.3 MANAGEMENT CONTROL

Subtopical Areas to Management Control

- A.3.1 Survey and Self-Assessment Programs
- A.3.2 Performance Assurance Program
- A.3.3 Resolution of Findings
- A.3.4 Incident Reporting and Management

Current Directives:

The following references apply to Management Control:

- DOE M 470.4-1, *Safeguards and Security Program Planning and Management*, 8-26-05
- DOE O 470.4, *Safeguards and Security Program*, 8-26-05
- DOE P 470.1, *Integrated Safeguards and Security Management (ISSM) Policy*, 5-8-01
- DOE O 221.1, *Reporting Fraud, Waste, and Abuse to the Office of Inspector General*, 3-22-01
- DOE N 221.10, *Reporting Fraud, Waste, and Abuse*, 9-15-04
- DOE G 231.1-1, *Occurrence Reporting and Performance Analysis Guide*, 8-20-03
- DOE M 231.1-2, *Occurrence Reporting and Processing of Operations Information*, 8-19-03
- DOE G 231.1-2, *Occurrence Reporting Causal Analysis Guide*, 8-20-03

Sample Document List:

Documentation to be reviewed may include the following:

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

Sample Interview Candidates:

Interview candidates may include:

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

Sample Interview Questions:

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

- Are survey and self-assessment programs in place to determine the effectiveness of the S&S program? Are the programs documented?
- When was the last self-assessment conducted? Did it include all applicable topical and subtopical elements?
- How does the S&S survey/self-assessment provide assurance that Departmental assets are being protected at appropriate levels?
- What ratings were given?
- Have recent survey or self-assessment activities resulted in any repeat findings?
- What is the status of open findings? What is the status of the associated corrective action plans?
- What method of root cause analysis is used? What training has staff received?
- Are the results of surveys and self-assessments factored into performance measures or award fees?
- Is there a corrective action tracking system in place? If so, does it cover the entire site/facility?
- Does the tracking system for findings include all periodic surveys, self-assessments, Technical Surveillance Countermeasure services, and DOE review findings?
- Are the milestones for completing the corrective actions reviewed on a recurring basis?
- Have staff members conducted inquiries into incidents of security concern? Were these individuals appointed in writing?
- What kind of trending and analysis is performed on IOSCs? How are the results disseminated to management & staff?
- What kind of IOSC awareness is provided?
- Are infraction reports maintained in individual personnel security files?
- How are corrective action plans coordinated with management?
- Have any inquiries established any possible crimes or fraud, waste, and abuse?
- Are there inquiries currently open?
- Have there been any formal inquiry reports developed?
- Was it determined that any damage assessments were required?
- If a damage assessment(s) was conducted, who appointed the damage assessment team(s) and approved the damage assessment report(s)?
- Have any incidents of S&S concern have occurred since the last survey? If so, how many?
- Of those incidents, how many were known compromises and how many were potential compromises?
- 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?
- What training do staff receive prior to conducting inquiries?
- Is there a formal process for implementing a performance assurance program?
- How often is testing conducted?
- Who reviews and approves the Performance Assurance Program Plan?
- Who determines what tests will be conducted and the criteria for evaluation? What is the basis for this determination?

A.4 PROGRAM-WIDE SUPPORT

Subtopical Areas to Program-Wide Support

- A.4.1 Facility Approval and Registration of Activities
- A.4.2 Foreign Ownership, Control, or Influence (FOCI)
- A.4.3 Security Management in Contracting

Current Directives:

The following references apply to Program-Wide Support:

- DOE O 142.3, *Unclassified Foreign Visits and Assignments*, 6-18-04
- DOE O 231.1A, *Change 1, Environment, Safety and Health Reporting*, 6-3-04
- DOE O 470.4, *Safeguards and Security Program*, 8-26-05
- DOE M 470.4-1, *Safeguards and Security Program Planning and Management*, 8-26-05
- DOE O 481.1C, *Work for Others (Non-Department of Energy Funded Work)*, 1-24-05
- Title 10 CFR, Part 1016, *Safeguarding Restricted Data*
- Title 42 U.S.C. 2011, et seq., *Atomic Energy Act of 1954*
- Title 48 CFR Chapter 9, *Department of Energy Acquisition Regulation (DEAR)*
 - a. DEAR Subpart 904.70, *Foreign Ownership, Control, or Influence over Contractors*
 - b. DEAR 952.204-2, *Security* [Security Clause]
 - c. DEAR 952.204-70, *Classification* [Classification Clause]
 - d. DEAR 952.204-73, *Foreign Ownership, Control, or Influence (FOCI) Over Contractor (Representation)*
 - e. DEAR 952.204.74, *Foreign Ownership, Control, or Influence (FOCI) Over Contractor* [FOCI Clause]
- DOE Acquisition Letter 92-2, 3-4-92
- Executive Order 10865, *Safeguarding Classified Information within Industry*, 2-20-60
- Executive Order 12829, *National Industrial Security Program*, 1-6-93
- Executive Order 12958, *Classified National Security Information*, 4-17-95
- National Industrial Security Program Operating Manual, 1-95
- National Industrial Security Program Operating Manual Supplement, 2-95

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 surveyed (list of all contractors/subcontractors registered)
- Approved Site Safeguards and Security Plan (SSSP)/Site Security Plan (SSP)
- Facility data sheets
- Copy of current award fee criteria and award fee documentation (including performance measurement data) for the last two years
- Most recent FOCI determination
- Approved Contract Security Classification Specification (CSCS) F 470.1
- Signed Facility Data and Approval Record (FDAR) F 470.2
- Deviations to DOE directives (pending and approved)
- Master facility registration, in the Safeguards and Security Information Management System, and local facility registration listings (if used)
- Previous survey and inspection reports and self-assessments
- List of cleared personnel, including access authorization number and date of latest background investigation by contract (including all contractors that have cleared employees conducting work at the facility). This list can come from the DOE Central

Personnel Clearance Index (CPCI) of access authorizations held by the contractor. The CPCI and contractor lists, including the list of current Owners, Officers, Directors, and Executive Personnel (OODEP), should be compared for discrepancies.

- Internal procedures (facility clearance, FOCI)
- Applicable Memoranda of Understanding/Agreement
- Completed FOCI questionnaire
- The OODEP list
- The FOCI determination
- A list of all employees of the company possessing or in the process of obtaining DOE access authorizations who are Representatives of Foreign Interests (RFIs)
- A list identifying any other organization conducting work at the facility and access authorizations requested for each of their respective organizations
- A copy of the contractor's records of all contracts and subcontracts involving access authorizations
- A 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 of the lenders involved, as well as the aggregate amount of the loan or credit agreement.
- Board of Director's meetings minutes to determine if any actions taken by the Board resulted, or will result, in changes that should be reported to DOE
- Copies of all Schedules 13D and 13G submitted to the Securities and Exchange Commission (SEC), if publicly traded
- Annual report and/or financial statement of the company
- Shareholders' agreements to determine if amount of stock is sufficient to elect representation to the Board or an agreement exists whereby the shareholder(s) is permitted representation on the Board, currently or at a future date
- Proxy statements (Notice of Annual Meeting of Stockholders) to determine (1) current beneficial owners of 5% or more of the company's securities; (2) changes to the company's directors; and (3) changes in location of its principal executive offices, state of incorporation, or the company's business, management, proposed mergers
- Annual report and SEC Form 10-K Report to determine (1) changes in revenue/income derived from foreign interests; (2) loan or credit agreements entered into with foreign lenders or in which foreign lenders are participants; and (3) joint ventures/contracts with foreign interests
- Internal Revenue Service Form 5471, Information Return of U.S. Persons with Respect to Certain Foreign Corporations to determine whether all foreign holdings were reported
- Articles of Incorporation and By-Laws or Partnership Agreement to determine if any changes have been made to the company's/partnership's business, management.

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

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

Sample Interview Candidates:

Interview candidates may include the following:

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

Sample Interview Questions:

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

- Have all applicable DOE directives been incorporated into contracts as appropriate? Are there any pending incorporation?
- Have all applicable security clauses been incorporated into contracts as appropriate? What is the process for ensuring contracts are made aware of security considerations?
- How are you informed of the security requirements to be included in a contract?
- Who has input into the award fee process?
- How is the criteria 'weighted' and by whom?
- Are facility clearances granted prior to allowing DOE S&S interests on the premises of the facility?
- Has the contractor and subcontractors been given a favorable FOCI determination?
- Does the facility have an approved SSSP or SSP?
- Is the FSO's access authorization equivalent with the facility clearance?
- Has an FDAR been completed and approved?
- Has a CSCS form been completed for all activities?
- Has a FOCI determination been made on all contractors and subcontractors that require access authorizations?
- Do the contractor and subcontractor provide notifications of any changes that may affect the FOCI determination?
- Do the key management personnel have appropriate access authorizations?
- If appropriate, has an RFI statement been provided for each employee of the company possessing or in process of obtaining a DOE access authorization?
- Has a Nondisclosure Certificate been provided for each interlocking OODEP?
- 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?

WORK FOR OTHERS (NON-DOE-FUNDED WORK)

An area of Registration of Activities that requires special attention is Work for Others (WFO). *WFO is the performance of work for non-DOE entities by DOE/National Nuclear Security Administration (NNSA) personnel and/or their respective contractor personnel or the 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)*, dated 1-24-05

As stated in DOE O 481.1C, Definitions,

For work performed in the field, the following determinations must be made and certified in writing by the responsible DOE/NNSA contracting officer or authorized DOE/NNSA designee. For work performed at Headquarters, these determinations must be made and certified in writing by a DOE/NNSA authorized designee. Certification must not be delegated to the contractor. The proposed work---

- 1. is consistent with or complementary to missions of DOE/NNSA and the facility to which the work is to be assigned,*
- 2. will not adversely impact programs assigned to the facility,*
- 3. will not place the facility in direct competition with the domestic private sector, and*
- 4. will not create a detrimental future burden on DOE/NNSA resources*

WFO projects should be surveyed during periodic surveys. Termination surveys and project closeout should also be accomplished and reported to the sponsor. In addition to the program management aspects of WFO, as discussed above, the topical and subtopical guidance applicable to each project should be used when surveying WFO projects.

PROGRAM MANAGEMENT & SUPPORT SAMPLE WORKSHEETS & PERFORMANCE TESTS

The following worksheets and sample performance tests can be utilized during the survey process to evaluate the status of the program management and support topical area.

Topic 1.0: Program Planning and Management							
Facility:				Date:		Inspector:	
Subtopic: 1.3 Management Control, 1.3.4 Incidents Reporting and Management						Manual Reference: DOE M 470.4-1, Section N	
Verification Elements				Verified By:		Adequacy	
				R	I	O	T
Comment							
Incidents of Security Concern (IOSC) Self-Assessment Checklist							
Implementation							
1	Are Inquiry Officers (IO) appointed in writing?						
2	Are all IO properly trained? (<i>IO must have attended the DOE Conduct of Inquiries course or previous law enforcement investigative experience</i>)						
3	Have local IOSC procedures been developed based on DOE M 470.4-1, Section N?						
4	Are local procedures approved by the DOE Cognizant Security Authority (CSA)?						
5	Are monthly status reports provided to the Office of Health, Safety and Security and the Departmental element for IMI-1 and IMI-2 incidents that have not been closed within 60 working days of notification of the incident?						
6	Does the CSA at each facility maintain a compilation of IMI-4 incidents by month?						
7	If no reportable incidents occurred during the calendar month, is a summary stating "no reportable incidents" forwarded to the Office of Health, Safety and Security by the fifth working day of each month?						
8	Were status reports submitted by the fifth working day of each month?						
9	Were any incidents reported as an occurrence under contractor requirements relating to DOE O 231.1A, chg 1, <i>Environment, Safety, and Health Reporting</i> , dated 6-3-04 (i.e., event affects both safety and security) incorporated into the contract?						
10	Were any incidents reportable under the contract provisions of DOE O 151.1B incorporated into the contract that were also reported under DOE M 470.4-1, Section N?						
Incident Reporting							
11	Do initial reports (DOE F 471.1) contain local incident tracking number?						

Topic 1.0: Program Planning and Management										
Facility:					Date:			Inspector:		
Subtopic: 1.3 Management Control, 1.3.4 Incidents Reporting and Management					Manual Reference: DOE M 470.4-1, Section N					
Verification Elements					Verified By:			Adequacy		Comment
					R	I	O	T	Y	
Incidents of Security Concern (IOSC) Self-Assessment Checklist										
12	If the facility has open inquiries, was an inquiry report submitted within 60 working days after categorization or submitted on monthly status report?									
13	How many IMI-1 IOSCs have been reported since the last assessment? Were initial reports submitted within the one-hour time frame as required?									
14	How many IMI-2 IOSCs have been reported since the last assessment? Were initial reports submitted within the eight-hour time frame as required?									
15	How many IMI-3 IOSCs have been reported since last assessment? Were initial reports submitted within the eight-hour time frame as required?									
16	Were corrective actions identified in each initial and subsequent incident reports?									
17	Was documentation for corrective actions submitted with the initial and/or subsequent inquiry reports?									
18	How many IMI-4 IOSCs have been reported since last assessment? Are the IMI-4 IOSCs reported monthly as required in local procedures?									
19	Are copies of 5639.3 "Report of Incident/Infraction" transmitted and placed in official DOE personnel security files?									
20	Is awareness material regarding reporting the discovery of IOSCs transmitted to site personnel?									
21	Was there any unaccounted for classified matter during the reporting period? If so, was a DOE F 5639.2, <i>Reporting Unaccounted-for Documents</i> , completed?									
22	If no reportable incidents occurred during the calendar month, is a summary stating "no reportable incidents" forwarded to the Office of Health, Safety and Security by the fifth working day of each month?									

CONTRACT REVIEW FORM

Review Date: _____

Company Name: _____

Subcontractor
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: _____

**Sample Performance Test
Facility Approval and Registration of Activities**

<p>FACILITY:</p> <p>TOPICAL AREA: PROGRAM MANAGEMENT & SUPPORT</p> <p>SUBTOPIC: PROGRAM-WIDE SUPPORT: FACILITY APPROVAL & REGISTRATION OF ACTIVITIES</p>																								
<p>TEST OBJECTIVE: To determine if facility approval personnel are knowledgeable of facility approval and registration procedures.</p>																								
<p>REFERENCES: DOE M 470.4-1, <i>Safeguards and Security Program Planning and Management</i>, 8-26-05</p>																								
<p>TEST PROCEDURES AND CONDITIONS:</p> <p><u>Procedures:</u> Provide the attached written test to facility approval personnel.</p> <p><u>Conditions:</u> Normal office and operating conditions.</p>																								
<p>EVALUATION CRITERIA OR STANDARDS: All test questions answered correctly.</p>																								
<p>TEST RESULTS:</p> <table style="width: 100%; border: none;"> <tr> <td style="width: 20%;">Question Number:</td> <td style="width: 30%;">1.</td> <td style="width: 30%;">Correct Answer:</td> <td style="width: 20%;">e</td> </tr> <tr> <td>Question Number:</td> <td>2.</td> <td>Correct Answer:</td> <td>e</td> </tr> <tr> <td>Question Number:</td> <td>3.</td> <td>Correct Answer:</td> <td>e</td> </tr> <tr> <td>Question Number:</td> <td>4.</td> <td>Correct Answer:</td> <td>FDAR</td> </tr> <tr> <td>Question Number:</td> <td>5.</td> <td>Correct Answer:</td> <td>c</td> </tr> <tr> <td>Question Number:</td> <td>6.</td> <td>Correct Answer:</td> <td>b</td> </tr> </table>	Question Number:	1.	Correct Answer:	e	Question Number:	2.	Correct Answer:	e	Question Number:	3.	Correct Answer:	e	Question Number:	4.	Correct Answer:	FDAR	Question Number:	5.	Correct Answer:	c	Question Number:	6.	Correct Answer:	b
Question Number:	1.	Correct Answer:	e																					
Question Number:	2.	Correct Answer:	e																					
Question Number:	3.	Correct Answer:	e																					
Question Number:	4.	Correct Answer:	FDAR																					
Question Number:	5.	Correct Answer:	c																					
Question Number:	6.	Correct Answer:	b																					
<p>PASS: _____ FAIL: _____ DATE OF TEST: _____</p>																								
<p>Survey Team Member: _____ Date: _____</p> <p>Team Lead: _____ Date: _____</p> <p>DOE Safety: _____ Date: _____</p> <p>Site Representative: _____ Date: _____</p>																								

**FACILITY APPROVAL AND REGISTRATION OF ACTIVITIES
SURVEY SAMPLE QUESTIONNAIRE**

Answer all questions by filling in the blanks with the appropriate answer or by circling the letter(s) of the correct answer(s).

1. Safeguards and security activities involving access authorizations, classified information, nuclear or other hazardous material presenting a potential radiological or toxicological sabotage threat, or over \$5,000,000 of departmental property will be registered to ensure proper levels of protection are in place to prevent adverse impact on:
 - a. National security
 - b. Health and safety of DOE and contractor employees
 - c. The public
 - d. The environment
 - e. All of the above

2. The determination of a valid facility clearance for a possessing facility will be based upon:
 - a. An approved safeguards and security plan
 - b. Results of surveys
 - c. A favorable FOCI determination
 - d. Completion of a DOE F 470.1, *Contract Security Classification Specification (CSCS)*
 - e. All of the above

3. The determination of a valid facility clearance for a non-possessing facility will be based upon:
 - a. An approved safeguards and security plan
 - b. Results of surveys
 - c. If applicable, a favorable FOCI determination
 - d. Completion of a DOE F 470.1, *Contract Security Classification Specification (CSCS)*
 - e. All of the above

4. Facility clearances are recorded on DOE F 470.2, _____.

5. A facility clearance may be suspended for reason of findings or other deficiencies by:
 - a. The facility security officer
 - b. The facility survey and approval program manager
 - c. The responsible head of the Departmental element, in coordination with the Office of Health, Safety and Security
 - d. The responsible head of the Departmental element, in coordination with the Office of Civilian Radioactive Waste Management

6. When a facility has completed all safeguards and security activities involving work requiring access authorizations, and there are no other active security activities, the facility clearance is terminated.
 - a. True
 - b. False

**Sample Performance Test
Foreign Ownership, Control or Influence**

<p>FACILITY:</p> <p>TOPICAL AREA: PROGRAM MANAGEMENT & SUPPORT</p> <p>SUBTOPIC: PROGRAM-WIDE SUPPORT: FOREIGN OWNERSHIP, CONTROL OR INFLUENCE (FOCI)</p>										
<p>TEST OBJECTIVE: To determine if FOCI personnel are knowledgeable of FOCI requirements.</p>										
<p>REFERENCES: DOE M 470.4-1, <i>Safeguards and Security Program Planning and Management</i>, 8-26-05</p>										
<p>TEST PROCEDURES AND CONDITIONS:</p> <p><u>Procedures:</u> Provide the attached written test to FOCI personnel.</p> <p><u>Conditions:</u> Normal office and operating conditions.</p>										
<p>EVALUATION CRITERIA OR STANDARDS: All test questions answered correctly.</p>										
<p>TEST RESULTS:</p> <table style="width: 100%; border: none;"> <tr> <td style="width: 30%;">Question Number: 1</td> <td style="width: 30%;">Correct Answer: b</td> </tr> <tr> <td>Question Number: 2</td> <td>Correct Answer: d</td> </tr> <tr> <td>Question Number: 3</td> <td>Correct Answer: b</td> </tr> <tr> <td>Question Number: 4</td> <td>Correct Answer: CSA</td> </tr> <tr> <td>Question Number: 5</td> <td>Correct Answer: b</td> </tr> </table>	Question Number: 1	Correct Answer: b	Question Number: 2	Correct Answer: d	Question Number: 3	Correct Answer: b	Question Number: 4	Correct Answer: CSA	Question Number: 5	Correct Answer: b
Question Number: 1	Correct Answer: b									
Question Number: 2	Correct Answer: d									
Question Number: 3	Correct Answer: b									
Question Number: 4	Correct Answer: CSA									
Question Number: 5	Correct Answer: b									
<p>PASS: _____ FAIL: _____ DATE OF TEST: _____</p>										
<p>Survey Team Member: _____ Date: _____</p> <p>Team Lead: _____ Date: _____</p> <p>DOE Safety: _____ Date: _____</p> <p>Site Representative: _____ Date: _____</p>										

**FOREIGN OWNERSHIP, CONTROL, OR INFLUENCE
SURVEY SAMPLE QUESTIONNAIRE**

Answer all questions by filling in the blanks with the appropriate answer or by circling the letter(s) of the correct answer(s).

1. The main purpose for conducting a FOCI is to:
 - a. Provide supporting documentation in the development of the FDAR
 - b. Eliminate or minimize risk to the common defense and security
 - c. Ensure the personnel security staff are given the most essential information for awarding a clearance

2. FOCI applies to:
 - a. Contractors
 - b. Subcontractors
 - c. Tier Parents
 - d. All the above

3. A favorable FOCI determination must be rendered after granting a facility clearance requiring access authorization.
 - a. True
 - b. False

4. The _____ will provide the successful offer/bidder with written notification that DOE has reviewed the FOCI submission and determined the organization is not under FOCI.

5. An acceptable method to negate or reduce risks associates with a controlling foreign majority case is:
 - a. Trustees voting title
 - b. Voting trust agreement
 - c. Bankruptcy petition

B. PROTECTIVE FORCE

Subtopical Areas

B.1 MANAGEMENT

B.2 TRAINING

B.3 DUTIES

B.4 FACILITIES AND EQUIPMENT

Areas of Consideration

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

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

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

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

- What is the status of Site Safeguards and Security Plan (SSSP) activities?
- Is the facility in compliance with contents of the SSSP?
- Does the SSSP/Site Security Plan (SSP) accurately reflect current site assets and operations?
- Are deviations in place at the facility? Are they current?

What are the assets of the site/facility?

- Where are they located?
- What is the importance level?
- Are all assets identified in the SSSP or SSP?
- Are the assets readily identifiable by the PF?

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

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

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

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

B.1 MANAGEMENT

Subtopical Areas to Management

None

Current Directives:

The following references apply to Management:

- *HS-61 Protective Force Inspectors Guide*, 4-05
- DOE O 470.4, *Safeguards and Security Program*, 8-26-05
- DOE M 470.4-3, *Protective Forces*, 8-26-05
- DOE M 470.4-1, *Safeguards and Security Program Planning and Management*, 8-26-05

Sample Document List:

Documentation to be reviewed may include:

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

Sample Interview Candidates:

Interview candidates may include the following:

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

Sample Interview Questions:

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

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

B.2 TRAINING

Subtopical Areas to Training

None

Current Directives:

The following references apply to Training:

- *HS-61 Protective Force Inspectors Guide*, 4-05
- DOE O 470.4, *Safeguards and Security Program*, 8-26-05
- DOE M 470.4-3, *Protective Forces*, 8-26-05
- DOE M 470.4-1, *Safeguards and Security Program Planning and Management*, 8-26-05
- 10 CFR 1046, *Physical Protection of Security Interests*
- 10 CFR 1047, *Limited Arrest Authority and Use of Force by Protective Force Officers*

Sample Document List:

Documentation to be reviewed may include:

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

Sample Interview Candidates:

Interview candidates may include:

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

Sample Interview Questions:

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

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

B.3 DUTIES

Subtopical Areas to Duties

None

Current Directives:

The following references apply to Duties:

- *HS-61 Protective Force Inspectors Guide, 4-05*
- DOE O 470.4, *Safeguards and Security Program, 8-26-05*
- DOE M 470.4-3, *Protective Forces, 8-26-05*
- DOE M 470.4-1, *Safeguards and Security Program Planning and Management, 8-26-05*
- 10 CFR 1046, *Physical Protection of Security Interests*
- 10 CFR 1047, *Limited Arrest Authority and Use of Force by Protective Force Officers*

Sample Document List:

Documentation to be reviewed may include the following:

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

Sample Interview Candidates:

Interview candidates may include the following:

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

Sample Interview Questions:

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

- How are compensatory measures determined? Relayed to PF?
- What are the critical targets associated with this facility? How are they recognized?
- How are communication channels determined to be effective (both internal to the PF organization and external to its counterparts)?

- What role does the EOC play during shipments?
- When was the last Force-on-Force exercise conducted?
- How are changes in operations (e.g., material movements, compensatory measures, increase threat levels) communicated?
- How are changes to policies and procedures transmitted? Who is responsible for ensuring Post Orders are approved and current?
- How are security locks and keys controlled within the PF?
- What training is provided relative to the identification of critical targets? Who has received this training and what is the criteria?
- What are the critical targets at this facility?

B.4 FACILITIES AND EQUIPMENT

Subtopical Areas to Facilities and Equipment

None

Current Directives:

The following references apply to Facilities and Equipment:

- *HS -61 Protective Force Inspectors Guide*, 4-05
- DOE M 470.4-3, *Protective Forces*, 8-26-05
- DOE M 470.4-1, *Safeguards and Security Program Planning and Management*, 8-26-05
- DOE O 460.1B, *Packaging and Transportation Safety*, 4-4-03
- DOE G 460.1-1, *Packaging and Transportation Safety*, 6-5-97
- DOE G 460.1-1 *Att, Packaging and Transportation Attachments*, 6-5-97
- 10 CFR 1046, *Physical Protection of Security Interests*
- 10 CFR 1047, *Limited Arrest Authority and Use of Force by Protective Force Officers*

Sample Document List:

Documentation to be reviewed may include the following:

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

Sample Interview Candidates:

Interview candidates may include the following:

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

Sample Interview Questions:

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

- What are the critical targets associated with this facility? How are they recognized? Where are they located?
- Are communication channels effective (both internal to the PF organization and external to its counterparts)?
- Is the PF equipped to meet its mission?
- Are training facilities adequate?
- Are modifications in equipment or facilities anticipated? If so, when and why?

- Has there been a change in mission that would affect the appropriateness of equipment used in the protection strategy at this facility?
- Are the vehicles used at this facility suitable and reliable to meet the mission?

PROTECTIVE FORCE SAMPLE WORKSHEETS & PERFORMANCE TESTS

The following worksheets and sample performance tests can be utilized during the survey process to evaluate the status of the protective force topical area.

Security Vehicle Inspection Check Sheet

Date:	Survey 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: _____ Inspector: _____

Portal Number: _____ Patrol Number: _____

Post Order: Available _____ Current

Duress Alarm: (Y/N) _____

Portal Condition: _____

Number of SI: _____ Number of Guards: _____

General Appearance : _____

Equipment:

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

Safety Glasses _____ [Extra pair required? (Y/N)] [Extra pair carried? (Y/N)]

Gas Mask _____ [Mask correctly fitted? (Y/N)]
[Vision correction required? (Y/N)]
[Vision inserts in use? (Y/N)]

Weapons: _____

Ammunition: _____

Auxiliary Weapons: _____

Auxiliary Ammunition: _____

Accessibility of Auxiliary Weapons:

Communications Equipment: Radio _____
Telephone _____
Other _____

Comments: _____

C. PHYSICAL SECURITY

Subtopical Areas

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

Areas of Consideration

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

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

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

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

- Is the facility in compliance with contents of the Site Safeguards and Security Plan (SSSP)?
- Does the SSSP/Site Security Plan (SSP) accurately reflect current site assets and operations?
- Does the SSSP/SSP accurately reflect current site physical protection elements and systems?
- Are deviations in place at the facility? Are they current?
- Does the site have an approved, current Response Plan for security emergencies?
- Does the site have an approved, current Compensatory Measures document?

What are the assets of the site/facility?

- Where are assets located?
- What is the impact of theft and/or diversion?
- Are all assets identified in the SSSP or SSP?

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

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

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

- How are the Design Basis Threat, local threat guidance, and Vulnerability Assessment used in protection and control planning?
- Are recapture, recovery, and pursuit strategies documented?
- How are programs designed to mitigate the consequences of radiological/toxicological sabotage?
- Are there agreements with local agencies in place for assistance and/or notification responsibilities?

C.1 ACCESS CONTROLS

Subtopical Areas to Access Controls

None

Current Directives:

The following references apply to Access Controls:

- DOE M 470.4-1, *Safeguards and Security Program Planning and Management*, 8-26-05
- DOE M 470.4-2, *Physical Protection*, 8-26-05
- DOE M 470.4-3, *Protective Force*, 8-26-05
- *HS-61 Physical Security Systems Inspectors Guide*, 9-00

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. In addition, the following documentation should be reviewed:

- 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 and procedures, records of past performance tests
- Documents identifying security areas and safeguards and security interests
- Termination/transfer procedures and notifications
- Building plans and protection area diagrams
- Comparison of Human Reliability Program (HRP) data with access control data
- Badge control procedures and automated system descriptions
- Date of last badge inventory and results (including issued, lost, recovered, destroyed)

Sample Interview Candidates:

Interview candidates may include the following:

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

Sample Interview Questions:

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

- What types of access control systems are used at the facility (e.g., receptionists, badge readers)?
- How are various functions notified of terminations and transfers?

- What policies are in place to ensure timely termination of access through retrieval of keys and access credentials upon termination or transfer?
- Have building lock-up procedures been established?
- How are records secured, maintained, and retrieved?
- Who performance-tests the systems, and how are the records kept?
- What happens in the event of an unsuccessful test or system failure?
- Is there a documented process for ensuring access is terminated as appropriate (e.g., HRP status changes, clearances terminated, employees terminated)?
- How is the site badging system equipment secured after hours?
- Have auxiliary power sources been provided to all critical systems? What are the testing and maintenance procedures for ensuring auxiliary power is available?
- What type of temporary badge system is used at the facility?
- What types of records are maintained relative to badging?

C.2 INTRUSION DETECTION AND ASSESSMENT SYSTEMS

Subtopical Areas to Intrusion Detection and Assessment Systems

None

Current Directives:

The following references apply to Intrusion Detection and Assessment Systems:

- DOE M 470.4-1, *Safeguards and Security Program Planning and Management*, 8-26-05
- DOE M 470.4-2, *Physical Protection*, 8-26-05
- DOE M 470.4-3, *Protective Force*, 8-26-05
- *HS-61 Physical Security Systems Inspectors Guide*, 9-00

Sample Document List:

Documentation to be reviewed may include the following:

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

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

Sample Interview Candidates:

Interview candidates may include the following:

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

Sample Interview Questions:

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

- Are approved deviations in place or pending?
- Are any line-item construction projects associated with physical security systems? If so, when were they last reviewed and who conducted the review?
- Is there a documented Testing and Maintenance Plan?
- How well is the physical security system program functioning?
- Is equipment calibrated according to documented specifications?

- Are response times consistent with those documented in security plans and Vulnerability Assessment?
- What areas of the system could be improved, and what steps have been taken toward the improvements?

C.3 BARRIERS AND DELAY MECHANISMS

Subtopical Area to Barriers and Delay Mechanisms

None

Current Directives:

The following references apply to Barriers and Delay Mechanisms:

- DOE M 470.4-1, *Safeguards and Security Planning and Management*, 8-26-05
- DOE M 470.4-2, *Physical Protection*, 8-26-05
- DOE M 470.4-3, *Protective Force*, 8-26-05
- *HS-61 Physical Security Systems Inspectors Guide*, 9-00

Sample Document List:

Documentation to be reviewed may include the following:

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

Sample Interview Candidates:

Interview candidates may include the following:

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

Sample Interview Questions:

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

- Are approved deviations in place or pending?
- Are any line-item construction projects associated with physical barriers? If so, when were they last reviewed and who conducted the review?
- Is there a documented Testing and Maintenance Plan for barrier systems?
- How well are automated barrier systems functioning?
- Is equipment calibrated according to documented specifications?
- Are response times consistent with those documented in security plans and VAs?
- What areas of the system could be improved, and what steps have been taken toward the improvements?
- What technologies could be deployed at this facility to enhance the overall protection?
- How often are key inventories conducted? How are discrepancies resolved and what are the reporting requirements?

C.4 TESTING AND MAINTENANCE

Subtopical Areas to Testing and Maintenance

None

Current Directives:

The following references apply to Testing and Maintenance:

- DOE M 470.4-1, *Safeguards and Security Planning and Management*, 8-26-05
- DOE M 470.4-2, *Physical Protection*, 8-26-05
- DOE M 470.4-3, *Protective Force*, 8-26-05
- *HS-61 Physical Security Systems Inspectors Guide*, 9-00

Sample Document List:

Documentation to be reviewed may include the following:

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

Sample Interview Candidates:

Interview candidates may include the following:

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

Sample Interview Questions:

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

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

C.5 COMMUNICATIONS

Subtopical Areas to Testing Communications

None

Current Directives:

The following references apply to Communications:

- DOE M 470.4-1, *Safeguards and Security Planning and Management*, 8-26-05
- DOE M 470.4-2, *Physical Protection*, 8-26-05
- DOE M 470.4-3, *Protective Force*, 8-26-05
- *HS-61 Physical Security Systems Inspectors Guide*, 9-00

Sample Document List:

Documentation to be reviewed may include the following:

- Performance tests of communication equipment
- Protective Force (PF) Post Orders
- PF General Orders
- Vulnerability Assessment/Site Safeguards and Security Plan
- Description of communication equipment, its location and test documentation
- Types of communication issued to PF
- Shipment procedures

Sample Interview Candidates:

Interview candidates may include the following:

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

Sample Interview Questions:

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

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

PHYSICAL SECURITY SAMPLE WORKSHEETS & PERFORMANCE TESTS

The following worksheets and sample performance tests can be utilized during the survey process to evaluate the status of the physical security topical area.

**Sample Performance Test
Access Control**

<p>FACILITY:</p> <p>TOPICAL AREA: PHYSICAL SECURITY</p> <p>SUBTOPIC: Access Controls</p>
<p>TEST 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.</p>
<p>REFERENCES: DOE M 470.4-2, <i>Physical Protection</i>, 8-26-05</p>
<p>TEST PROCEDURES AND CONDITIONS:</p> <p><u>Procedures:</u> The survey team member, with a site representative, will attempt to enter a security area where access is controlled by either a Security Officer (SO) or receptionist. The survey team member will have an old badge or will conceal his/her badge before attempting entry.</p> <p><u>Conditions:</u> Normal operating conditions.</p>
<p>EVALUATION CRITERIA OR STANDARDS: The SO or receptionist shall challenge the survey team member, and deny access until a positive identification is made.</p>
<p>TEST RESULTS: The SO or receptionist challenged the survey team member and followed established site procedures.</p>
<p>PASS: _____ FAIL: _____ DATE OF TEST: _____</p>
<p>Survey Team Member: _____ Date: _____</p>
<p>Team Lead: _____ Date: _____</p>
<p>DOE Safety: _____ Date: _____</p>
<p>Site Representative: _____ Date: _____</p>

**Sample Performance Test
Intrusion Detection and Assessment System: Security Lighting**

FACILITY:

TOPICAL AREA: PHYSICAL SECURITY

SUBTOPIC: INTRUSION DETECTION AND ASSESSMENT SYSTEMS: Security Lighting

TEST 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 or unauthorized personnel attempting access, and to properly check credentials.

REFERENCES:

DOE M 470.4-2, *Physical Protection*, 8-26-05

TEST PROCEDURES AND CONDITIONS:

Procedures:

- a. The test will be conducted approximately one hour after sunset.
- b. The site representative will provide a calibrated light meter that displays light levels in foot-candles.
- c. Light-level readings will be taken within the perimeter intrusion detection and assessment system (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.
- d. Light-level readings will be taken around Protective Force (PF) posts out to 30 feet from the post. Additional readings will be taken out to 150 feet from the post.

Conditions:

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

EVALUATION CRITERIA OR STANDARDS:

- a. Lighting must be at least 2 foot-candles within 30 feet of entry control points for personnel to check credentials.
- b. Lighting must be at least 0.2 foot-candles within 150 feet of PF Post for unaided assessment of alarms by PF.
- c. Lighting for PIDAS zones must be at least 0.2 foot-candles to allow the PF to assess alarms using closed-circuit television (CCTV).
- d. All lighting must meet the requirements outlined in DOE directives.

TEST RESULTS:

All evaluation criteria must be answered "yes" to pass the test.

- a. Lighting is at least 2 foot-candles within 30 feet of entry control points for personnel to check credentials.
- b. Lighting is at least 0.2 foot-candles within 150 feet of PF Post for unaided assessment of alarms by PF.
- c. Lighting for PIDAS zones is at least 0.2 foot-candles to allow the PF to assess alarms using CCTV.
- d. All lighting meets the requirements outlined in DOE directives.

PASS: _____ **FAIL:** _____ **DATE OF TEST:** _____

Survey Team Member: _____ **Date:** _____

Team Lead: _____ **Date:** _____

DOE Safety: _____ **Date:** _____

Site Representative: _____ **Date:** _____

Sample Performance Test
Intrusion Detection and Assessment System: Balanced Magnetic Switches (BMS) Sensors

<p>FACILITY:</p> <p>TOPICAL AREA: PHYSICAL SECURITY</p> <p>SUBTOPIC: INTRUSION DETECTION AND ASSESSMENT SYSTEMS: Balanced Magnetic Switches (BMS)</p>
<p>TEST OBJECTIVE:</p> <p>The objective of this test is to determine if door mounted BMS can be moved more than one inch (measured from the leading edge of the door to door frame) without indicating an alarm condition.</p>
<p>REFERENCES:</p> <p>DOE M 470.4-1, <i>Safeguards and Security Program Planning and Management</i>, 8-26-05</p> <p>DOE M 470.4-2, <i>Physical Protection</i>, 8-26-05</p>
<p>TEST PROCEDURES AND CONDITIONS:</p> <p><u>Procedures:</u></p> <ol style="list-style-type: none"> a. The survey team member will select ___ BMSs to test. b. The survey team member and site representative will proceed to the selected alarm location(s) equipped with a Protective Force (PF) radio. c. The Central Alarm Station (CAS) will be notified to announce when the alarm is received. When the alarm has been received the test is complete for that sensor. d. The survey team member will observe as the site representative attempts to open an alarmed door, a distance greater than one inch, without causing an alarm. e. The survey team member will ensure that the BMS is moved slow enough to allow the CAS to detect and announce the alarm. <p><u>Conditions:</u></p> <p>This test will be conducted during operational or non-operational hours depending on location of test and impact on operations.</p>
<p>EVALUATION CRITERIA OR STANDARDS:</p> <ol style="list-style-type: none"> a. Ensure an alarm signal is received by the CAS. b. The BMS must sound an alarm prior to being opened greater than one inch. c. Ensure that the CAS receives the alarm and that it has an individual address and is not part of a loop of alarms. d. Ensure maintenance records reflect proper maintenance. e. Ensure that a record of previous tests exists and that the tests were performed in accordance with established procedures and time frames.
<p>TEST RESULTS:</p> <p>All evaluation criteria must be answered with a “yes” in order to pass this test.</p> <ol style="list-style-type: none"> a. An alarm signal was received by the CAS. b. The BMS alarm sounded prior to being opened greater than one inch. c. The CAS received the alarm and it has an individual address and is not part of a loop of alarms. d. Maintenance records reflect proper maintenance. e. A record of previous tests exists and the tests were performed in accordance with established procedures and time frames.
<p>PASS: _____ FAIL: _____ DATE OF TEST: _____</p>
<p>Survey Team Member: _____ Date: _____</p>
<p>Team Lead: _____ Date: _____</p>
<p>DOE Safety: _____ Date: _____</p>
<p>Site Representative: _____ Date: _____</p>

D. INFORMATION PROTECTION

Subtopical Areas

- D.1 BASIC REQUIREMENTS**
- D.2 TECHNICAL SURVEILLANCE COUNTERMEASURES (TSCM)**
- D.3 OPERATIONS SECURITY (OPSEC)**
- D.4 CLASSIFICATION GUIDANCE**
- D.5 CLASSIFIED MATTER PROTECTION AND CONTROL (CMPC)**
 - D.5.1 Control of Classified Matter
 - D.5.2 Special Access Programs and Intelligence Information

Areas of Consideration

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

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

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

How is classification guidance disseminated?

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

Does the facility have Special Access Programs (SAPs)?

- Have the SAPs been properly registered with DOE-Headquarters (HQ) using the Facility Data and Approval Record process?
- Do all persons having access to SAPs have proper clearance and briefings?
- Are there specific security plans and operating procedures associated with SAPs?

How are DOE-HQ guidance and directives distributed?

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

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

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

D.1 BASIC REQUIREMENTS

Subtopical Areas to Basic Requirements

None

Current Directives:

The following references apply to this subtopical area:

- DOE M 475.1-1A, *Identifying Classified Information*, 2-26-01
- DOE M 470.4-4, *Information Security*, 8-26-05
- DOE O 205.1, *Cyber Security Management Program*, 3-21-03
- DOE M 471.2-2, *Classified Information Systems Security Manual*, 8-3-99

Sample Document List:

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

- Training records for personnel with information security responsibilities
- Information security procedures
- Classification guidance
- Local site-specific policy
- Site Safeguards and Security Plan (SSSP) or Site Security Plan (SSP)
- Specific safeguards and security (S&S) plans
- Unclassified controlled information procedures

Sample Interview Candidates:

Interview candidates may include the following:

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

Sample Interview Questions:

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

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

D.2 TECHNICAL SURVEILLANCE COUNTERMEASURES

Subtopical Areas to Technical Surveillance Countermeasures (TSCM)

None

Current Directives:

The following references apply to TSCM:

- Executive Order 12333, *United States Intelligence Activities*, 12-4-81
- DOE TSCM Annex (classified)
- DCID 6/9, *Physical Security Standards for Sensitive Compartmented Information Facilities*, 11-18-02 (if applicable)
- DOE M 470.4-4, *Information Security*, Section E, 8-26-05
- DOE M 470.4-2, *Physical Protection*, 8-26-05

Sample Document List:

The following documents should be reviewed:

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

Sample Interview Candidates:

The following individuals may be interviewed as appropriate:

- DOE TSCMOM
- Local Sensitive Compartmented Information Facility Special Security Officer (if applicable)
- Contractor TSCMO(s)
- TSCM Team Manager and TSCM Technicians

Sample Interview Questions:

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

- Are local TSCM capabilities available and sufficient to detect, deter, and/or nullify technical penetrations and hazardous conditions? If not, is a signed memorandum of understanding (MOU) to provide for appropriate TSCM support with another DOE site approved and coordinated through the TSCM Program Manager?
- What kind of training has been provided to the TSCM team members?
- What reporting procedures of a TSCM penetration or hazard are in place? Are these procedures included in the site TSCM awareness briefing?
- Is there a TSCM awareness program?
- Is there a list of all facilities that meet TSCM service criteria?

- What procedures are followed to request TSCM services or report TSCM concerns?
- Are TSCM assets effectively utilized to conduct TSCM services in areas that discuss, process, and/or produce classified information?
- Is an annual schedule of TSCM activities in writing and approved? Is the schedule completed before the beginning of each new fiscal year?
- Are complete and up-to-date TSCM reference documents and memoranda, including DOE TSCM Manual and classified TSCM Annex, available?
- Is there an annual re-certification eligibility of TSCM Technicians sent to TSCM Program Manager?
- Are an appropriate number of contractor TSCMOs assigned to provide for effective management and coordination of local TSCM services?
- Have TSCMOs attended any training concerning TSCM services and activities?
- Does TSCM Technician training include safety, administrative, and specialized technical course (e.g., telephony, Operations Security, counterintelligence, information systems)?

D.3 OPERATIONS SECURITY

Subtopical Areas to Operations Security (OPSEC)

None

Current Directives:

The following references apply to OPSEC:

- DOE O 471.4-4, *Information Security*, Section B, 8-26-05
- National Security Decision Directive 298

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 Program Information (CPI) list
- Indicators list
- Counter-Imagery Program Plan (if applicable)
- Results of Internet Website assessments

Sample Interview Candidates:

Interview candidates may include the following:

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

Sample Interview Questions:

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

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

D.4 CLASSIFICATION GUIDANCE

Subtopical Areas to Classification Guidance

None

Current Directives:

The following references apply to Classification Guidance:

- DOE M 475.1-1A, *Identifying Classified Information*, 2-26-01
- DOE M 470.4-4, *Information Security*, 8-26-05
- DOE M 452.4-1A, *Protection of Use Control Vulnerabilities and Design*, 3-11-04
- DOE O 452.2B, *Safety of Nuclear Explosive Operations*, 8-7-01

Sample Document List:

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

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

Sample Interview Candidates:

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

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

Sample Interview Questions:

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

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

D.5 CLASSIFIED MATTER PROTECTION AND CONTROL

Subtopical Areas to Classified Matter Protection and Control (CMPC)

- D.5.1 *Control of Classified Matter*
- D.5.2 *Special Access Programs and Intelligence Information*

Current Directives:

The following references apply to CMPC:

- DOE O 470.4, *Safeguards and Security Program*, 8-26-05
- DOE M 470.4-4, *Information Security*, 8-26-05
- DOE M 470.4-1, *Safeguards and Security Program Planning and Management*, 8-26-05
- DOE M 452.4-1A, *Protection of Use Control Vulnerabilities and Designs*, 3-11-04
- DOE M 471.2-3A, *Special Access Program Policies, Responsibilities, and Procedures*, 7-11-02
- DOE O 5639.8A, *Foreign Intelligence Information and SCI Facilities*, 7-23-93
- DOE M 475.1-1A, *Identifying Classified Information*, 2-26-01
- DOE M 471.2-2, *Classified Information Systems Security Manual*, 8-3-99
- DOE O 481.1C, *Work for Others (Non-Department of Energy Funded Work)*, 1-24-05

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)
- Site Safeguards and Security Plan (SSSP)/Site Security Plan (SSP)
- Recent self-assessment, survey reports, security appraisals and inspections
- Incidents of Security Concern (IOSC) involving CMPC
- Classified Removable Electronic Media (CREM) procedures
- List of CREM Custodians
- List of equipment used to reproduce and destroy classified matter with locations and associated approvals
- Recent CREM inventories
- Accountable matter inventory list(s)
- Special Access Program (SAP) security plans
- Results of accountable annual inventories
- Corrective action plan packages for recent findings

Sample Interview Candidates:

Interviews may be conducted with the following individuals:

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

Sample Interview Questions:

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

- How are site-specific policies disseminated to facility staff?
- What kind of training is provided to Control Station Operators, custodians, and authorized users of classified information? How often?
- Does the facility have any special or unique equipment to generate classified documents? What kind of training and procedures are available for this equipment?
- What procedures are used to enforce limiting access, need-to-know, and handling classified documents outside storage locations?
- What is the process for receipts not returned within the suspense period? How are follow-up actions documented?
- How are fax transmissions documented for verbal receipts?
- What are the hand carry procedures? How are staff identified and approved for hand carry? What kind of contingency plans are in place?
- How is information from other government agencies handled?
- What are the emergency procedures pertaining to CMPC?
- What procedures are available for intra-site messengers or post office couriers to ensure they constantly attend and control classified matter?
- What check-out procedures are used for staff who have transferred, terminated employment, or are otherwise unavailable for employment?
- What is the notification process for suspensions/revocations of access authorizations?
- What are the procedures for inventorying CREM?
- Have there been discrepancies of past CREM inventories? If so, how often and what was deemed to be the cause?
- When was the last inventory conducted of accountable matter? What were the results?
- Is classified email a common practice at this facility?
- How are classified document facilities managed (is there overnight storage, how is classified waste handled)?
- How is security managed for SAPs at this facility?
- How is need-to-know for SAPs determined?
- How are intelligence-related efforts coordinated with the Office of Intelligence?
- Has an individual been designated as being responsible for procurements involving field intelligence elements and/or Sensitive Compartmented Information?

INFORMATION SECURITY SAMPLE WORKSHEETS & PERFORMANCE TESTS

The following worksheets and sample performance tests can be utilized during the survey process to evaluate the status of the information security topical area.

Topic 4.0 Information Protection										
Facility:					Date:			Inspector:		
Subtopic: 4.2 Technical Surveillance Countermeasures (TSCM)								Manual Reference: DOE M 470.4-4, Section E		
Verification Elements					Verified By:			Adequacy		Comment
					R	I	O	T	Y	
TSCM Self-Assessment Checklist										
1	Is the TSCM Operations Manager (TSCMOM) appointed in writing by the Oak Ridge Operations (ORO) Office Manager?									
2	Does the TSCMOM possess the knowledge and/or has the TSCMOM attended training? <i>(Have general working knowledge of DOE Counterintelligence Policy [Presidential Decision Directive-NSC-61, U.S. Department of Energy Counterintelligence Program, dated February 1998], attend the ITC Executive Overview Course or the DOE TSCM Program Course, and attend the Basic DOE OPSEC Course.)</i>									
3	Has a current TSCM Operations Plan been developed?									
4	Has an annual schedule of requested TSCM support services been developed?									
5	findings and corrective actions entered into the and Security Information Management System									
6	Was the annual TSCM report transmitted to the TSCM Program Manager and the Departmental element by the end of the previous fiscal year?									
7	Does the TSCM Officer (TSCMO) identify and submit a list of all facilities meeting TSCM service criteria contained in this section to the cognizant TSCMOM for inclusion in the annual TSCM schedule?									
8	Are corrective actions reports prepared and forwarded by the TSCMO to the cognizant TSCMOM within 90 days of the completion of TSCM services?									
9	Are the TSCMOs providing quarterly corrective action status reports as required until the finding is corrected?									
10	Is the TSCMO properly trained and formally appointed? <i>(Have general working knowledge of DOE Counterintelligence policy [Presidential</i>									

Topic 4.0 Information Protection											
Facility:					Date:			Inspector:			
Subtopic: 4.2 Technical Surveillance Countermeasures (TSCM)								Manual Reference: DOE M 470.4-4, Section E			
Verification Elements					Verified By:				Adequacy	Comment	
					R	I	O	T	Y		N
<i>Decision Directive-NSC-61, U.S. Department of Energy Counterintelligence Program, dated February 1998], attend the DOE TSCM Program Course, and attend the Basic DOE OPSEC Course.)</i>											
11	Is TSCM awareness material transmitted to employees?										
12	Do the TSCMOM and/or TSCMO have a copy of the local threat statement?										
13	How is TSCM integrated into security disciplines?										
14	Are there procedures identifying the reporting requirements for Incidents of Security Concern involving technical security?										
15	Are training records maintained and current for all personnel involved in the local TSCM program?										

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)?

- a. Derivative Classifier (DC)
- b. Derivative Declassifiers (DD)
- c. Reviewing Officials (RO)

2. Do you have a letter authorizing your authority as an:
(review and discuss authority letter)

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 Classification Officer?

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)

- a.
- b.
- c.

Are these guides current? Yes No Don't know
Do you have a DOE-HQ-issued Classification Guide index (e.g., INDEX-05-2 issued July 2005)?

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

Yes No

Discuss: _____

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

Yes No

Discuss response: _____

8. Have you met with the your Classification Officer or a representative from the Classification Office to discuss classification issues within the last month, 3 months, 6 months, a year?

Yes No

If Yes, obtain feedback – positive and negative

If No, why not

9. Do you feel comfortable contacting your Classification Office?

Comment: _____

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

Yes No

If so, when: _____

If not, why not? _____

11. When did you perform the last review for?

Classification _____

Declassification _____

Unclassified Controlled Nuclear Information (UCNI) _____

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

Yes No

Comments: _____

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

a. When: _____

b. Why/Reason: _____

14. Do you have any classification stamps?

Yes No

List stamps: _____

Do you need additional stamps?

Yes No

List stamps needed: _____

15. Have you Portioned-Marked a document?

Yes No

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

Yes No

Discuss: _____

17. Have you applied all required classification stamps or remarked/re-stamped a declassified document?

Yes No NA

Discuss: _____

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

Yes No

19. Does your management support your classification authority?

Yes No

Discuss: _____

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

Official Use Only	Yes	No
Export Control Information	Yes	No

Discuss: _____

21. Overall Comments: _____

SURVEY/SELF-ASSESSMENT CHECKLIST
CLASSIFICATION AND DECLASSIFICATION OF CLASSIFIED MATTER

The following can be used, when interviewing the Classification Officer (CO) or a document reviewer, as a guide for conducting an audit/survey/self-assessment of the methods for reviewing, protecting, classifying/declassifying, and marking classified matter. It is intended to be used by the auditor to trigger questions and ensure the major classification/declassification topic areas are discussed.

Classification/Declassification Program

1. Size of classification program (circle one):

Small (1 to 10) Medium (11 to 50) Large (51 to 100) Huge (101+)

2. Level/Category of programs (circle all that apply):

CNSI CFRD CRD SNSI SFRD SRD TSNSI TSFRD TSRD

3. Number of classification reviewers:

Derivative Classifier (DC): (obtain list)*
Derivative Declassifier (DD): (obtain list)*
Reviewing Official (RO): (obtain list)*

*Identify from these lists those individuals who will be interviewed using the attached “DC/DD/RO Questionnaire” as a suggested guide as well as some of the questions/information identified below.

Classification Guides

1. Are classification guides available to the reviewer?
2. Format of guides being used by the reviewer—hardcopy, Classification Guide System (CGS) CD format, Classification Office’s guides.
3. Are up-to-date guides being used? How is that determined?
4. What method is used to determine whether the guides are current?
5. Which method is used to obtain the latest version? Headquarter issued; Other DOE Site’s issued; Local issue
6. Is DOE-HQ’s Classification Guide Index current/available?
7. How are classification guides distributed to the DCs/DDs/ROs?
8. What is the method for determining distribution? If the guides are not being distributed, why not? Explain..
9. Can the reviewer explain how classification guides are used?

Training

1. Did the CO receive training to become
 - a. DC
 - b. DD
 - c. RO

2. How was training provided?
 - a. Classroom
 - b. On-the-Job
 - c. Classroom and On-the-Job
 - d. Not at all
 - e. Other (explain)

3. Who provided the training?
 - a. CO/Designated trainer
 - b. Local DOE CO
 - c. DOE-HQ
 - d. DC/DD within organization
 - e. Reviewed some guides and took the test provided by
 - i. Another contractor CO/trainer
 - ii. DOE CO
 - iii. DOE-HQ
 - iv. Individual – state person’s name

4. Does the CO receive retraining?
 - a. Monthly
 - b. Quarterly
 - c. Semi-annually
 - d. Never

5. Does the CO provide retraining to the DCs/DDs/ROs?
 - a. Monthly
 - b. Quarterly
 - c. Semi-annually
 - d. Never

6. Has the CO been required to re-certify as an
 - a. DC
 - b. DD
 - c. RO

7. Have the DCs/DDs/ROs been required to re-certify as an
 - a. DC
 - b. DD
 - c. RO

8. Does the DOE CO communicate with contractor CO regularly? In what format:
 - a. Meetings
 - b. Mail (hardcopy and email)
 - c. Personal visits
 - d. Other

9. Frequency of communications with the DOE CO
 - a. Daily
 - b. Weekly
 - c. Monthly
 - d. Quarterly
 - e. Specify frequency

10. Frequency of communications by the CO with reviewers?
 - a. Daily
 - b. Weekly
 - c. Monthly
 - d. Quarterly
 - e. Specify frequency

Management

Has the reviewer and the CO met with the review's management?

1. Determine highest level of management when meeting occurred.
 - a. Immediate Manager
 - b. One above Immediate Manager
 - c. Two above Immediate Manager
 - d. Director/Vice President level
 - e. Director/President level

2. Frequency of these meetings
 - a. Weekly
 - b. Monthly
 - c. Quarterly
 - d. Semi-annually
 - e. Yearly

3. Can you name the facility's CO?

4. Can you name the DOE field CO?

5. Have you met the DOE field CO?

6. Have you ever attended a CO meeting?
 - a. At DOE-HQ Germantown
 - b. At another DOE site

7. Has your CO provided feedback from any CO meetings?

8. Does the last performance appraisal of the reviewers (CO/DC/DD/RO) contain statements concerning his/her activities as an:
 - a. DC Yes No
 - b. DD Yes No
 - c. RO Yes No

If “No,” discuss this issue with:

- a. The reviewer’s immediate manager
- b. The CO

Classified Matter Storage

1. Does the CO and/or reviewer maintain classified matter in their work area?
2. Is their work area in a security controlled area?
3. Is the storage container approved by security?
4. Are DOE SF 702 forms being used regularly?
5. Is there any unclassified matter in this security container?
6. Is classified matter separated from unclassified matter? (If unclassified matter is stored with classified, determine reason.)
7. Does the container contain any electronic storage media (ESM) – e.g., Sigma 1, 2, 14 and/or 15 classified matter contained on CDs, tapes, floppy disc? If yes, does storage of this material meet current separation requirements?
8. Inspect the reviewer’s security container’s weekly inventory listings of ESM classified matter. (Review of this classified matter is not required.)

Classification/Declassification Stamps

The following questions apply to the CO, the DCs, the DDs, and the ROs.

1. Are required classification/declassification stamps available for use?
2. Are the stamps up to date to ensure they contain the information and issue date of the required guide?
3. What are the locations of classification stamps and are they sufficiently protected?
4. Does the reviewer understand the document stamping requirements?
 - a. Understand when to use?
 - b. Understand preferred location for placement of stamp’s information on document?
 - c. Understand the review and signature requirements?
5. Has the reviewer stamped documents correctly? Is he/she able to explain his/her actions? (Obtain several documents for review to confirm actions.)

Document Marking

1. Demonstrate how to properly apply classification or declassification markings on the following types of documents.
 - a. Classification
 - (a) Restricted Data (RD)
 - (b) Formally Restricted Data (FRD)
 - (c) National Security Information (NSI)
 - (d) Official Use Only (OUO)
 - (e) Unclassified Controlled Nuclear Information (UCNI)
 - (f) Naval Nuclear Propulsion Information (NNPI)
 - (g) Unclassified (U)
 - b. Declassification
 - (a) Removal of classified markings
 - (b) Required stamps
 - (c) Required signatures
 - c. Portion-Marking – when done and why
 - d. Importance of guide issue date
2. Is there a procedure available to assist the DC/DD/RO to ensure proper document-marking? If not, why not?
3. Does the reviewer maintain a record of the documents reviewed and stamped for classification, declassification, and/or UCNI?
4. Does the document reviewer ensure that proper markings are placed on the document as they are being identified during the review process?
5. During a document review, does the reviewer identify classification concerns (elimination of words and terms and suggested rework of the document to reduce or eliminate classification issues) to the document preparer?

Classification Knowledge

1. Knowledge (Document reviewer should be able to provide sufficient knowledge of the following items or know where to obtain the information.)
 - a. Classification
 - (1) Levels
 - (2) Categories
 - b. UCNI – discuss to ensure understood and why needed
 - c. Sigmas – know differences
 - d. Mosaic complication
 - e. No-Comment Policy
 - f. Adverse Effect Test
 - g. OUO
 - h. Who can classify subject matter?
 - i. Who can declassify subject matter?
 - j. Who can upgrade classified matter?
 - k. Who can downgrade classified matter?
 - l. Does reviewer have authority to release information to the general public?

- m. Does reviewer have access to a Secure Telephone Unit (STU) phone?
 - n. Number of classification/declassifications decisions (average) made per:
 - (1) Day
 - (2) Week
 - (3) Month
 - (4) Semi-annually
 - (5) Other
 - o. Are classification decisions reviewed by another reviewer prior to final classification markings/approval/release (explain, provide examples)
2. What subject matter does your authority cover as an:
(Obtain list or copy of their authority letter.)
- a. DC
 - b. DD
 - c. RO
3. Is the reviewer involved with “Work for Others” contracts? Discuss scope of authority and limits.

Auditors Concerns/Comments Section:

**Sample Performance Test
Classified Matter Protection and Control: Accountability**

<p>FACILITY:</p> <p>TOPICAL AREA: INFORMATION PROTECTION</p> <p>SUBTOPIC: CLASSIFIED MATTER PROTECTION & CONTROL: Accountability</p>
<p>TEST OBJECTIVE: To evaluate the accuracy of the document accountability system and determine whether documents are marked in accordance with DOE requirements.</p>
<p>REFERENCES: DOE M 471.4-4, <i>Information Security</i>, 8-26-05; Site-specific procedures</p>
<p>TEST PROCEDURES AND CONDITIONS:</p> <p><u>Procedures:</u> The survey team member will select a computer-generated, random sample of documents listed on the accountability record. Selected documents are reviewed to ensure that each item is the item described in the accountability record. Further, each document is checked for markings, documentation, dates, titles, cover sheets, and other applicable requirements to determine compliance with DOE directives. Each repository is also inspected for compliance with DOE storage requirements.</p> <p><u>Conditions:</u> Normal operating conditions.</p>
<p>EVALUATION CRITERIA OR STANDARDS: Each item is accurately described in the accountability record. Each item is appropriately marked in accordance with DOE directives, to include required coversheets. Each repository complies with DOE storage requirements, to include access authority and combination changes.</p>
<p>TEST RESULTS: All evaluation criteria must be answered “yes” in order to pass the test.</p> <p>Each item is accurately described in the accountability record. Each item is appropriately marked in accordance with DOE directives, to include required coversheets. Each repository complies with DOE storage requirements, to include access authority and combination changes.</p>
<p>PASS: _____ FAIL: _____ DATE OF TEST: _____</p>
<p>Survey Team Member: _____ Date: _____</p> <p>Team Lead: _____ Date: _____</p> <p>DOE Safety: _____ Date: _____</p> <p>Site Representative: _____ Date: _____</p>

**Sample Performance Test
Classified Matter Protection and Control: Reproduction**

<p>FACILITY:</p> <p>TOPICAL AREA: INFORMATION PROTECTION</p> <p>SUBTOPIC: CLASSIFIED MATTER PROTECTION & CONTROL: Reproduction</p>
<p>TEST OBJECTIVE: To determine whether classified documents are reproduced in accordance with DOE directives and site-specific procedures.</p>
<p>REFERENCES: DOE M 470.4-4, <i>Information Security.</i>, 8-26-05; Site-specific procedures</p>
<p>TEST PROCEDURES AND CONDITIONS:</p> <p><u>Procedures:</u> The survey team member selects a sample of personnel who normally reproduce classified documents for testing. 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/marketing reproduced copies.</p> <p><u>Conditions:</u> Normal operating conditions.</p>
<p>EVALUATION CRITERIA OR STANDARDS:</p> <ol style="list-style-type: none"> a. Determine if equipment is approved and properly posted. b. Determine if the appropriate number of blank pages are run after duplicating. c. Determine if blank pages are treated as classified waste. d. Determine if documents are properly controlled while in process. e. Determine if the documenting/marketing of reproduced copies is adequate.
<p>TEST RESULTS: All evaluation criteria must be answered "yes."</p> <ol style="list-style-type: none"> a. Equipment is approved and properly posted. b. The appropriate number of blank pages are run after duplicating. c. The blank pages are treated as classified waste. d. The documents are properly controlled while in process. e. The documenting/marketing of reproduced copies is adequate.
<p>PASS: _____ FAIL: _____ DATE OF TEST: _____</p>
<p>Survey Team Member: _____ Date: _____</p> <p>Team Lead: _____ Date: _____</p> <p>DOE Safety: _____ Date: _____</p> <p>Site Representative: _____ Date: _____</p>

Topic 4.0: Information Protection										
Facility:					Date:			Inspector:		
Subtopic: Classified Matter Protection and Control (CMPC)								Manual Reference: DOE M 470.4-4, Section A		
Verification Elements		Verified By:				Adequacy				Comment
		R	I	O	T	Y	N	NA		
2006 CMPC Self-Assessment Checklist										
TRAINING										
1	Have all employees who have responsibility for classified matter received the appropriate training? If yes, are all certificates of completion on file?									
2	Are custodians aware of where to find the latest version (March 2006) of the Oak Ridge Operations (ORO) CMPC Manual?									
3	Are primary and alternate accountable classified removable electronic media (ACREM) Custodians up to date in their training requirements?									
4	Is ACREM training included in the recurring CMPC training course?									
MARKING REQUIREMENTS										
5	Do individual classified repositories contain only active files, which are referred to frequently in the conduct of current business?									
6	Is the highest overall classification level marked at the top and bottom of the document cover (if any), title page (if any), front of first page of text, and back of last page of document?									
7	Documents dated after 04/01/1996 must be marked in accordance with directives in place at the time of origin or in accordance with the requirements contained in this manual. Active Files: Must meet current marking requirements. Inactive Files: Must contain, at a minimum, the classification level on every page and the category (if Restricted Data [RD] or Formerly Restricted Data [FRD]). The following requirements are also applicable:									
8	For documents containing National Security Information, is every section, part, paragraph, or similar portion marked to indicate the classification level (including Unclassified)?									
9	Is an unclassified title noted with a (U)?									

Topic 4.0: Information Protection										
Facility:				Date:				Inspector:		
Subtopic: 4.5 Classified Matter Protection and Control (CMPC)								Manual Reference: DOE M 470.4-4, Section A		
Verification Elements				Verified By:				Adequacy		Comment
				R	I	O	T	Y	N	
2006 CMPC Self-Assessment Checklist										
CLASSIFIED WORKSHEETS AND DRAFTS										
10	Are the back pages of all classified documents blank, with the classification level marked top and bottom? If not, do they have an appropriate cover sheet affixed?									
ACCOUNTABLE DOCUMENTS										
11	Are all classified documents (e.g., Secret and Confidential as appropriate) listed on the personal inventory accounted for? If not, contact the Central Library in Person .									
12	Do all accountable documents contain the additional marking requirements contained in the ORO CMPC Manual?									
13	Does evidence show that the weekly ACREM inventories are completed and reported as required?									
14	Has the annual Secret inventory been completed?									
15	Are all "Secret" drafts or working papers properly logged on a Secret Worksheet Log?									
16	Has the 180-calendar day maximum time limit expired? Note: If the worksheet or draft has expired, destroy immediately or convert to a permanent document, which has been properly reviewed and signed by an Derivative Classifier (DC).									
17	Is the appropriately color-coded Standard Form (SF) Cover Sheet applied (SF 704 is the Secret cover sheet; and SF 705 is the Confidential cover sheet)?									
18	Does the working paper or draft document list the date created?									
19	Is the highest potential overall classification level of the draft or working paper marked at the top and bottom on the outside of the cover page (if any), on the title page (if any), on the first page, and on the outside of the back cover or last page?									
20	Is each interior page marked at the top and bottom and bottom with the highest classification level of that page (including Unclassified) or the overall classification of the									

Topic 4.0: Information Protection									
Facility:				Date:				Inspector:	
Subtopic: 4.5 Classified Matter Protection and Control (CMPC)								Manual Reference: DOE M 470.4-4, Section A	
Verification Elements		Verified By:				Adequacy			Comment
		R	I	O	T	Y	N	NA	
2006 CMPC Self-Assessment Checklist									
document?									
21	Is the overall category (if RD or FRD) marked on the first page of text?								
22	Is "Working Paper" or "Draft" marked on the first page of text?								
23	Are applicable caveats or special markings annotated on the first page of text?								
STORAGE									
24	Is the information on the SF-700 accurate?								
25	Is the classified matter stored in the security container regularly accessed (i.e., weekly or monthly)? If not, is the repository needed?								
26	Is the U.S. General Services Administration-approved label affixed to the repository?								
27	Is the combination changed when people having it no longer need it due to reassignment, transfer, termination, or if it was found open?								
28	Is the SF-702 used to document the opening and closing of the security container?								
29	Is the top portion of the SF-702 properly completed (i.e., month/year, room#, building, container#)?								
30	Is a separate SF-702 posted on each security container?								
31	Is the SF-702 retained for three months from the date of the last entry?								
32	Is an end-of-day check and double-check performed on all repositories and the surrounding areas?								
33	Do classified repositories contain any prohibited items (money, drugs, or other items susceptible to theft)?								
34	Are there any external repository markings indicating the level and category of information being stored?								
35	Do the custodian and alternates possess the appropriate security clearance for the information stored in the repository?								
36	Have the custodians and individuals possessing the combinations to the repository been appropriately trained?								

Topic 4.0: Information Protection										
Facility:				Date:				Inspector:		
Subtopic: 4.5 Classified Matter Protection and Control (CMPC)								Manual Reference: DOE M 470.4-4, Section A		
Verification Elements				Verified By:				Adequacy		Comment
				R	I	O	T	Y	N	
2006 CMPC Self-Assessment Checklist										
37	Are all ACREM repository combinations marked as accountable and stored properly?									
38	When the Emergency ACREM Custodian must retrieve the combination, is the combination changed?									
REPRODUCTION DEVICES										
39	Are all classified reproduction devices approved for classified processing and have the proper postings, which are signed by the ORO CMPC Operations Manager?									
40	Are proper sanitization procedures followed after reproducing classified information?									
42	Are all reproduced copies of "Secret" documents taken to Central Library to receive a barcode?									
43	Have all unnecessary copies/overruns of classified documents been properly destroyed, in a designated red burn can, in approved cross-cut shredder, or taken to the Central Library?									
DESTRUCTION										
44	If using a shredder for classified destruction, has the shredder been approved and the approval posted on the cross-cut shredder?									
45	Is the Classified Shredder Monthly Check Sheet being completed every month?									
UNCLASSIFIED SENSITIVE										
46	Are all Unclassified Controlled Nuclear Information (UCNI) documents reviewed by an approved UCNI official and marked correctly?									
47	Are Sensitive Unclassified (S-U) documents marked properly?									
48	If stored in the Limited or Exclusion Area, are S-U documents protected from incidental visual access?									
49	If stored in the Property Protection Area, are S-U documents stored in a locked container or in a locked room?									

E. CYBER SECURITY

Subtopical Areas

E-1 CLASSIFIED CYBER SECURITY

- E.1.1 Leadership, Responsibilities, and Authorities
- E.1.2 Certification and Accreditation (C&A), Risk Management, and Planning
- E.1.3 Policy, Guidance, and Procedures
- E.1.4 Technical Implementation
- E.1.5 Performance Evaluation Feedback and Continuous Improvement

E-2 TELECOMMUNICATIONS

E-3 UNCLASSIFIED CYBER SECURITY

- E.3.1 Leadership, Responsibilities, and Authorities
- E.3.2 Certification and Accreditation (C&A), Risk Management, and Planning
- E.3.3 Policy, Guidance, and Procedures
- E.3.4 Technical Implementation
- E.3.5 Performance Evaluation Feedback and Continuous Improvement

Areas of Consideration

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

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

- Have procedures been developed and approved for all aspects of the program?
- Does the Site Safety and Security Plan and other planning documents adequately address Cyber Security?
- Has cyber-specific training been provided to key personnel?
- Are security plans, certification and accreditation letters, site policies, information system (IS) procedures, access authorizations, and internal review and audit reports accurate and up to date?
- Are IS users knowledgeable of site protection requirements and their associated responsibilities?
- Have roles and responsibilities been formally delegated and/or documented?

What ratings were given during past surveys, self-assessments, and inspections?

- Have findings/deficiencies been reviewed for trends?
- Have all elements been reviewed?
- What is the status of open findings and corrective actions?
- Are corrective action plans complete?

E.1 CLASSIFIED CYBER SECURITY

Subtopical Areas to Classified Cyber Security

- E.1.1 Leadership, Responsibilities, and Authorities
- E.1.2 Certification and Accreditation (C&A), Risk Management, and Planning
- E.1.3 Policy, Guidance, and Procedures
- E.1.4 Technical Implementation
- E.1.5 Performance Evaluation Feedback and Continuous Improvement

Current Directives:

The following references apply to Classified Cyber Security:

- DOE M 471.2-2, *Classified Information Systems Security Manual*, 8-3-99
- DOE O 200.1, *Information Management Program*, 9-30-96
- DOE M 470.4-4, *Information Security*, 8-26-05
- DOE P 205.1, *Departmental Cyber Security Management Policy*, 5-8-01
- DOE O 205.1, *Cyber Security Management Program*, 3-21-03
- DOE G 205.1-1, *Cyber Security Architecture Guidelines*, 3-8-01
- DOE M 205.1-1, *Incident Prevention, Warning, and Response (IPWAR) Manual*, 9-30-04
- DOE M 205-1-2, *Clearing, Sanitization, and Destruction of Information System Storage Media, Memory Devices, and Related Hardware Manual*, 6-26-05
- DOE N 205.10, *Cyber Security Requirements for Risk Management*, 2-19-04
- DOE N 205.9, *Certification and Accreditation Process for Information Systems Including National Security Systems*, 2-19-04
- DOE N 205.8, *Cyber Security Requirements for Wireless Devices and Information Systems*, 2-11-04
- DOE N 205.3, *Password Generation, Protection, and Use*, 11-23-99
- DOE G 205.3-1, *Password Guide*, 11-23-99
- DOE N 205.2, *Foreign National Access to DOE Cyber Systems*, 11-1-99
- DOE G 205.2-1, *Guide to Preventing Computer Software Piracy*, 7-12-01

Sample Document List:

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

- Appointment letters for the Designated Approving Authority (DAA), Information Systems Security Operations Manager (ISOM), and Information Systems Security Site Manager (ISSM) letters for the DAA, Classified ISOM, ISSM, and Information Systems Security Officer (ISSOs)
- List of Cyber Security personnel with access authorization level, location, and phone number
- List of all accredited classified information systems (ISs) including accrediting authority and most recent accreditation date for each.
- Copies of the Program Cyber Security Plan and Cyber Security Program Plan applicable to the site
- Copy of the Site-Specific Threat Statement and/or the Site-Specific Cyber Threat Statement
- Any cyber security-related deviations
- Information system security plans (ISSPs) for major systems and networks and a sample of plans for distributed and stand-alone systems, including a master plan, if applicable
- Approval, tests, certification, and accreditation documentation for the systems or networks covered by the requested ISSPs
- Copies of ISSP addenda available for review
- Site Cyber Security policies, procedures, and/or handbooks

- Cyber Security training materials and records
- Procedures for validation/revalidation of users and for prompt notification when a user no longer needs access
- Samples of the written acknowledgments of classified IS users' responsibilities (i.e., Code of Conduct) for the protection of classified information systems and information
- Site IS policies, procedures, or handbooks
- Continuity of operations plans (including contingency planning and disaster recovery planning)
- Procedures for backing up all essential data, utility, and operating system files (including network interface software)
- A summary of Cyber Security incidents involving classified IS, including severity and corrective actions
- Procedures related to the site configuration management program
- Procedures implemented to authorize user access to classified IS resources and need-to-know for specific information
- Previous self-assessments, surveys, and inspection reports, and the status of corrective actions for identified findings
- Qualifications and required training for the ISOM, DAA, ISSM, and/or ISSOs
- Risk assessment documentation and associated acceptance
- Documented risk mitigation strategies
- Integrated Safeguards and Security/Departmental Cyber Security Management policy implementation plans
- Results of the most recent site external and internal vulnerability scans
- Risk assessments and procedures for classified video conferencing

Sample Interview Candidates:

It may be beneficial to conduct interviews with the following individuals:

- The DAA and/or the ISOM, (the DAA is dependent on the protection index of a given system)
- The ISSM
- ISSOs
- System Managers or Administrators for classified information systems
- Owners of major applications, especially mission-essential applications
- System users and operators
- Cyber Security staff members

Sample Interview Questions:

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

- Does the site risk assessment include the Classified Information Systems Security Risk Assessment as its baseline? Are other site-specific threats identified?
- Do the ISSM and ISSOs have the current copies of plans and procedures available?
- What kind of training is provided to the classified IS staff and users? Does it describe their responsibilities? Who receives training? How is training and awareness documented?
- Have all findings and deficiencies been corrected? Are any corrective action plans pending?
- How are passwords receipted? What procedures are in place for the sharing of passwords? What process is used for password generation? Is this process approved by DOE?
- What procedures are in place describing the marking requirements and leaving classified terminals or workstations unattended?

- How are stand-alone classified IS users informed of their responsibilities and to whom are incidents reported?
- What is the coordination process for cyber security incidents that are reportable under M 470.1-4, Section N and IPWAR 205.1-1
- What is the process for removing unclassified data off the classified IS? Is this process documented and approved by the DAA?
- What kind of training do the classified IS users get?
- Are there security features that block unauthorized users or file access attempts to classified information systems?

E.2 TELECOMMUNICATIONS SECURITY

Subtopical Areas of Telecommunications Security

None

Current Directives:

The following references apply to Telecommunications Security:

- DOE M 470.4-4, *Information Security*, 8-26-05
- DOE M 205.1-3, *Telecommunications Security Manual*, 4-17-06

Sample Document List:

Documentation to be reviewed may include the following:

- List of all Communications Security (COMSEC) custodians and alternates
- Records of appointments and changes of COMSEC Control Officers, COMSEC Custodians, COMSEC Subcustodians, alternates, and any persons having access to COMSEC materials
- List of access authorizations for the individuals listed above
- Results of last physical inventory of COMSEC material
- Last COMSEC survey report completed by DOE-Headquarters (HQ)
- Training records/material for personnel engaged in cryptographic duties
- COMSEC procedures/standard operating procedures
- Incidents of Security Concern involving either a COMSEC facility or material
- Copies of COMSEC material transfer, inventory, and destruction reports as required
- Records of keying and operation of cryptographic-equipment charged to the account
- National Security Agency (NSA) Key Management System records for all STU-III keys
- COMSEC custodian account transfer documentation (Standard Form SF-153)
- Emergency Destruction Plan
- Routine Destruction Plan
- TEMPEST Plan, program files, and incident records, if applicable
- Protected Distribution System records, if applicable
- List of locations where COMSEC material is stored

Sample Interview Candidates:

Interview candidates may include the following:

- COMSEC Control Officer
- COMSEC custodians and alternates
- Persons having access to COMSEC materials

Sample Interview Questions:

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

- What are the duties and responsibilities of the COMSEC Control Officer? What are the training requirements?
- What are the duties and responsibilities of a COMSEC Custodian/alternate? What are the training requirements?
- What are the duties and responsibilities of the users of COMSEC materials? What are the training requirements?
- Does equipment meet TEMPEST requirements?
- What actions are taken in the case of a physical compromise of loss of material?

**COMSEC
MATERIAL ACCOUNTING REQUIREMENTS**

Categories & Examples Accountable COMSEC Material	Accounting to Department COMSEC Custodian		Change of Custodian	Semi- Annual Inventory
	Initial Receipt	Transfer Return		

Cryptographic-marked COMSEC

Material:

Telecommunications Security keytapes, lists, and pads	X	X	X	See 2
---	---	---	---	-------

Non-Cryptographic COMSEC

Material:

Classified:

Telecommunications Security equipment and devices	X	X	X	
Telecommunications Security assemblies and elements	X	X	X	See 1
Telecommunications Security, CE, and E COMSEC Material	X	See 3	See 3	X
Non- Telecommunications Security COMSEC glossary, NSA publications	X	See 4	See 4	See 7

Unclassified:

Cryptographic-ancillary equipment and devices	X	X	X	
Assemblies and elements	X	X	X	
Encryption and decryption devices	X	X	X	
COMSEC publications	X	X	X	
“CE” materials	X	X	See 6	See 6
Controlled Cryptographic Item	X	X	X	See 7

NOTES:

1. Assemblies shall be reported by short title and accounting number. Spare elements shall be reported by short title and quantity unless they are installed in equipment. Spare elements may be removed from the record by reporting the spare elements as being “installed in equipment or assemblies on (date).”
2. Key card book, multi-page key lists, and key pads shall be reported as on hand until all cards, pages, or segments of an edition have been destroyed. In transferring such material, indicate missing cards, pages, segments, if any, on SF-153.
3. Amendments to COMSEC publications are normally inserted into the related publication and the residue destroyed promptly after receipt. Amendments not inserted at the time of a change of Custodian or Semi-annual inventory shall be reported as on hand. (see section 9)
4. Classified cryptographic-related COMSEC material is accountable for logistics purposes
5. Telecommunication nomenclature devices shall be reported.
6. Only those unclassified CE materials specially designated by the Department COMSEC Control Officer shall be included in Semi-annual Inventory reports. Unclassified CE materials should be included in Changes of Custodian reports of logistics purposes
7. CCI material and accountable manuals will be inventoried annually

E.3 UNCLASSIFIED CYBER SECURITY

Subtopical Areas of Unclassified Cyber Security

- E.3.1 Leadership, Responsibilities, and Authorities
- E.3.2 Certification and Accreditation (C&A), Risk Management, and Planning
- E.3.3 Policy, Guidance, and Procedures
- E.3.4 Technical Implementation
- E.3.5 Performance Evaluation Feedback and Continuous Improvement

Current Directives:

The following references apply to Unclassified Cyber Security:

- DOE O 200.1, *Information Management Program*, 9-30-96
- DOE M 200.1-1, *Telecommunications Security Manual*, 3-1-97
- DOE M 470.4-4, *Information Protection*, 8-26-05
- DOE P 205.1, *Departmental Cyber Security Management Policy*, 5-8-01
- DOE O 205.1, *Cyber Security Management Program*, 3-21-03
- DOE G 205.1-1, *Cyber Security Architecture Guidelines*, 3-8-01
- DOE M 205.1-1, *Incident Prevention, Warning, and Response (IPWAR) Manual*, 9-30-04
- DOE M 205.1-2, *Clearing, Sanitization, and Destruction of Information System Storage Media, Memory Devices, and Related Hardware Manual*, 6-26-05
- DOE N 205.2, *Foreign National Access to DOE Cyber Systems*, 11-1-99
- DOE G 205.2-1, *Guide to Preventing Computer Software Piracy*, 7-12-01
- DOE N 205.3, *Password Generation, Protection, and Use*, 11-23-99
- DOE G 205.3-1, *Password Guide*, 11-23-99
- DOE N 205.8, *Cyber Security Requirements for Wireless Devices and Information Systems*, 2-11-04
- DOE N 205.9, *Certification and Accreditation Process for Information Systems Including National Security Systems*, 2-19-04
- DOE N 205.10, *Cyber Security Requirements for Risk Management*, 2-19-04
- DOE N 205.11, *Security Requirements for Remote Access to DOE and Applicable Contractor Information Technology Systems*, 2-19-04
- DOE O 471.3, *Identifying and Protecting Official Use Only Information*, 4-9-03
- DOE M 471.3-1, *Manual for Identifying and Protecting Official Use Only Information*, 4-9-03
- DOE G 471.3-1, *Guide to Identifying Official Use Only Information*, 4-9-03
- DOE O 471.1A, *Identification and Protection of Unclassified Controlled Nuclear Information*, 6-30-00
- DOE M 471.1-1 Chg 1, *Identification and Protection of Unclassified Controlled Nuclear Information Manual*, 10-23-01

Sample Document List:

Documentation to be reviewed may include the following:

- Appointment letters for site Cyber Security personnel
- List of Cyber Security personnel with access authorization level, location, and phone number
- Copies of the Program Cyber Security Plan and Cyber Security Program Plan applicable to the site
- Copy of the Site-Specific Threat Statement and the Site-Specific Cyber Threat Statement
- Deviations related to Cyber Security
- Risk management documentation

- Continuity of operations plans (including contingency planning and disaster recovery planning)
- Internet protocol (IP) addresses for all site computers that include addresses exposed to the Internet, as well as any address ranges on restricted or “yellow” networks
- List of systems within the site address range that are requested to be excluded for safety, security, or other reasons; should include the IP addresses and the reasons for exclusion
- Network topology map containing perimeter devices and IP addresses of those devices, including main border router, other routers that have separate Internet connections, firewalls, gateways, and major subnet routers
- Router access control lists and firewall rules (provided after conclusion of penetration testing)
- List of cyber systems processing Sensitive Unclassified information and the nature of the sensitivity (e.g., Unclassified Controlled Nuclear Information [UCNI], Official Use Only [OUO], Privacy Act)
- List of computer system incident reports for unclassified systems during the review period
- Cyber Security metrics/performance
- Budget prioritization documentation
- Site Cyber Security policies and procedures
- Documents that explain Cyber Security training/briefing/awareness program objectives for users and Cyber Security professionals

Sample Interview Candidates:

Interview candidates may include the following:

- The Designated Approving Authority (DAA) and/or the Information Systems Security Operations Manager, (the DAA is dependent on the protection index of a given system)
- The Information System Security Site Manager (ISSM)
- Information Systems Security Officers (ISSOs)
- System managers or administrators for unclassified information systems
- Owners of major applications, especially mission-essential applications
- System users and operators
- Cyber Security staff members
- Information Management staff

Sample Interview Questions:

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

- Do the ISSM and ISSOs have current copies of plans and procedures available? How are changes handled?
- What kind of training is provided to the IS staff and users? Does it describe their responsibilities?
- Have all findings and deficiencies been corrected? Are any corrective action plans pending?
- How are passwords receipted? What procedures are in place for the sharing of passwords?
- What method of password generation is used? It is approved by DOE?
- How are stand-alone classified IS users informed of their responsibilities and to whom are incidents reported?
- How is the sensitivity of unclassified systems determined?

CYBER SECURITY SAMPLE WORKSHEETS & PERFORMANCE TESTS

The following worksheets and sample performance tests can be utilized during the survey process to evaluate the status of the cyber security topical area.

Sample Performance Test: Classified Cyber Security

<p>FACILITY:</p> <p>TOPICAL AREA: CYBER SECURITY</p> <p>SUBTOPIC: Classified Cyber Security</p>
<p>TEST OBJECTIVE: This test will be used to review multi-user systems, subsystems, or file servers with disk storage space and a user population without a common need to know to determine if disk storage space is cleared before it is reallocated to another user.</p>
<p>REFERENCES: DOE O 200.1, <i>Information Management Program</i>, 9-30-96 DOE O 470.4-4, <i>Information Security</i>, 8-26-05 DOE M 471.2-2, <i>Classified Information Systems Security Manual</i> Classified Cyber Security Site-Specific procedures</p>
<p>TEST PROCEDURES AND CONDITIONS: This test may be conducted from the operator's console in the computer room or from a remote terminal. The Information Systems Security Officer, or authorized designee, will perform the actions listed below under the supervision of the survey team member:</p> <ol style="list-style-type: none"> a. Identify an allocated disk storage space that will be made available to non-privileged users as a temporary workspace during a normal session. Use whatever technique is necessary to identify this space based upon the configuration of the selected computer system. b. Log on as a normal (non-privileged) user with a valid user ID and password. Use the allocated space by executing a prearranged process that will fill the allocated disk space with test data or non-zero characters. The test data must be easily distinguishable from the characters that will be used by the overwrite process. c. Review the file space that contains the test data. Print the contents of the allocated disk workspace if possible. (System privileges may be required to accomplish this step.) d. Invoke the overwrite process either by using some specific command or by logging off the system if the process is invoked automatically at logoff. Terminate the session. e. Access the disk storage space that was allocated to the previous session. Review the contents of the disk workspace to determine if it contains the results of the overwrite process. Print the contents if possible. (System privileges may be required to accomplish this step.)
<p>EVALUATION CRITERIA OR STANDARDS: In order to pass, the overwrite process should have written the expected character(s) into the workspace before that space becomes available to another user. If not, the operating system should preclude a read operation until after the new user has performed a write to that area of memory.</p>
<p>TEST RESULTS: The overwrite process wrote the expected character(s) into the workspace before the space became available to another user. Or, the operating system precluded a read operation until after the new user performed a write to that area of memory.</p>
<p>PASS: _____ FAIL: _____ DATE OF TEST: _____</p>
<p>Survey Team Member: _____ Date: _____</p> <p>Team Lead: _____ Date: _____</p> <p>DOE Safety: _____ Date: _____</p> <p>Site Representative: _____ Date: _____</p>

F. PERSONNEL SECURITY PROGRAM

Subtopical Areas

- F.1 ACCESS AUTHORIZATION (PERSONNEL CLEARANCES)**
- F.2 HUMAN RELIABILITY PROGRAM (HRP)**
- F.3 CONTROL OF CLASSIFIED VISITS**
- F.4 SAFEGUARDS AND SECURITY (S&S) AWARENESS**

Areas of Consideration

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

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

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

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 re-justifications required?
- Are regular reviews conducted of access authorizations for subcontractors/consultants?

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

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

Is access to facilities adequately controlled?

- Is there an effective Foreign National Visits and Assignments 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 foreign nationals from accessing sensitive information via the local area network?
- Are site-/visit-specific security plans used for visitors from sensitive countries?

F.1 ACCESS AUTHORIZATIONS

Subtopical Areas to Access Authorizations

None

Current Directives:

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*
- DOE M 470.4-5, *Personnel Security*, 8-26-05
- DOE M 470.4-1, *Safeguards and Security Program Planning and Management*, 8-26-05

Sample Document List

Documentation to be reviewed may include the following:

- Access authorization requests to determine if justifications are adequate and include appropriate contract references
- Personnel security files:
 - Has proof of U.S. citizenship been validated using acceptable evidence?
 - Have the appropriate preprocessing checks been completed?
 - 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 special nuclear material (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, Standard Form-86, and fingerprint cards
- Central Personnel Clearance Index records
- List of clearances terminated during the review period
- Case analysis sheets
- List of reinvestigations that are due or past due
- List of individuals on administrative leave
- List of individuals on leave of absence during the period
- List of classified contracts and the access authorizations associated with them
- 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
- Human Reliability Program Adjudicator

Sample Interview Questions:

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

- Is the need for an access authorization determined prior to processing? What constitutes valid need?
- 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)?
- What are the criteria for processing interim access authorizations?
- What procedures are in place to ensure foreign nationals who have been granted access authorizations are not granted access to classified matter such as Top Secret or NATO- or Intelligence-related information?
- 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?

F.2 HUMAN RELIABILITY PROGRAM

Subtopical Areas to Human Reliability Program (HRP)

None

Current Directives:

The following references apply to the Human Reliability Program (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 470.4, *Safeguards and Security Program*, 8-26-05
- DOE M 470.4-1, *Safeguards and Security Program Planning and Management*, 8-26-05
- DOE M 470.4-2, *Physical Protection*, 8-26-05
- DOE M 470.4-3, *Protective Forces*, 8-26-05
- DOE M 470.4-4, *Information Security*, 8-26-05
- DOE M 470.4-5, *Personnel Security*, 8-26-05
- DOE M 470.4-6, *Material Control and Accountability*, 8-26-05

Sample Document Lists:

Documentation to be reviewed may include the following:

- Implementation schedule
- Training records/materials
- Drug testing/handling procedures
- Drug testing records
- Random test procedures
- Site implementation plans, 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 for those with nuclear explosive responsibilities)?
- Review files to ascertain if appropriate records are maintained and properly protected

Sample Interview Candidates:

Interview candidates may include the following:

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

Sample Interview Questions:

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

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

F.3 CONTROL OF CLASSIFIED VISITS

Subtopical Areas to Control of Classified Visits

None

Current Directives:

The following references apply to the Control of Classified Visits:

- DOE M 470.4-1, *Safeguards and Security Program Planning and Management*, 8-26-05
- DOE M 470.4-4, *Information Security*, 8-26-05
- DOE M 470.4-5, *Personnel Security*, 8-26-05
- DOE O 200.1, *Information Management Program*, 9-30-96
- DOE M 475.1-1A, *Identifying Classified Information*, 2-26-01
- DOE O 551.1B, *Official Foreign Travel*, 8-1-03
- DOE M 360.1B-1, *Federal Employee Training Manual*, 10-11-01
- DOE O 142.1, *Classified Visits Involving Foreign Nationals*, 1-13-04
- DOE O 142.3, *Unclassified Foreign Visits and Assignments*, 6-16-04
- DOE O 5610.2, *Control of Weapon Data, Change 1*, 9-2-86

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/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 of the visit?
 - Review procedures for urgent or rush requests
 - Review 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, Formerly Restricted Data, and nuclear weapon data is fully understood. The following people should be considered for interviews:

- Employees responsible for processing and controlling classified visits
- Individuals responsible for processing, controlling, and approving visits of uncleared U.S. citizens
- Staff who routinely host visitors or tours

Sample Interview Questions:

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

- What is the local policy regarding escort-to-visitor ratios?
- Are visitor logs used at Protected Areas? Material Access Areas? Exclusion Areas?
- Have procedures been developed and implemented for classified visits by DOE employees, contractors, and subcontractors?

- Are specific procedures developed for individuals from other government agencies who wish to access classified information?
- Who approves requests for classified visits?
- How are vendors/visitors processed? Is there a difference in the way they are processed?
- When are briefings provided?
- What are the responsibilities of an escort?

F.4 SAFEGUARDS AND SECURITY AWARENESS

Subtopical Areas to Safeguards and Security (S&S) Awareness

None

Current Directives:

The following references apply to S&S Awareness:

- DOE M 475.1-1A, *Identifying Classified Information*, 2-26-01
- DOE M 470.4-1, *Safeguards and Security Program Planning and Management*, 8-26-05
- DOE M 470.4-4, *Information Security*, 8-26-05
- DOE M 470.4-5, *Personnel Security*, 8-26-05
- DOE O 551.1B, *Official Foreign Travel*, 8-1-03
- DOE M 360.1B-1, *Federal Employee Training Manual*, 10-11-01
- DOE O 200.1, *Information Management Program*, 9-30-96
- DOE O 142.1, *Classified Visits Involving Foreign Nationals*, 1-13-04
- DOE O 142.3, *Unclassified Foreign Visits and Assignments*, 6-18-04

Sample Document List:

Documentation to be reviewed may include the following:

- Lesson plans for the initial briefing, comprehensive briefing, refresher briefing, and termination briefing
 - Do the briefings address site-specific needs, S&S interests, and potential threats to the facility/organization? Is the information up to date (last review/update)?
 - Do contents include items outlined in the DOE M 470.4-1 for each briefing?
 - Are briefings given prior to assuming duties or accessing applicable information, as applicable?
- 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 (SFs-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 M 470.4-1?
- Review records. Records must be maintained to provide an audit trail verifying an individual's receipt of the briefings
 - Are completed SF-312 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 M 470 4-1?

Sample Interview Candidates:

Interview candidates may include the following:

- S&S Manager (DOE and Contractor)
- DOE and Contractor Security Awareness Coordinators
- Security Education Training Attendees
- Operations Security Manager
- Site Managers and Supervisors

Sample Interview Questions:

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

- Do awareness briefings/training contain site-specific information and recent threat information?
- Has trending been conducted on security incidents/infractions? If so, have trends been included in awareness material?
- Have training approval programs been implemented to ensure the standardization of S&S training provided onsite?
- Do S&S awareness information and/or briefings address site-specific procedures as well as specific topics such as recent espionage cases, foreign intelligence recruitment techniques, incidents and considerations, and S&S threats and vulnerabilities?
- What types of training records are kept relative to S&S training?
- How are the contents of the Annual Refresher Briefing determined?

PERSONNEL SECURITY SAMPLE WORKSHEETS & PERFORMANCE TESTS

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

**Sample Performance Test
Personnel Security: Safeguards and Security Awareness Program**

<p>FACILITY:</p> <p>TOPICAL AREA: PERSONNEL SECURITY PROGRAM</p> <p>SUBTOPIC: Safeguards And Security (S&S) Awareness Program</p>
<p>TEST OBJECTIVE: To determine the effectiveness of the facility's S&S Awareness Program.</p>
<p>REFERENCES: DOE M 470.4-1, <i>Safeguards and Security Program Planning and Management</i>, 8-26-05</p>
<p>TEST PROCEDURES AND CONDITIONS: Review the security education briefings (initial, comprehensive, and refresher). Select a number of employees who have attended the various briefings. The survey team member will interview these employees with the same questions for the type of briefing they received. (The questions and associated correct answers will be prepared during the survey because they will be site-specific.)</p> <p>The survey team member will complete an evaluation form for each interview (to be prepared during the survey).</p>
<p>EVALUATION CRITERIA OR STANDARDS: 90% of the interview questions must be answered correctly.</p>
<p>TEST RESULTS: To be developed.</p>
<p>PASS: _____ FAIL: _____ DATE OF TEST: _____</p>
<p>Survey Team Member: _____ Date: _____</p> <p>Team Lead: _____ Date: _____</p> <p>DOE Safety: _____ Date: _____</p> <p>Site Representative: _____ Date: _____</p>

G. UNCLASSIFIED VISITS AND ASSIGNMENTS BY FOREIGN NATIONALS

Subtopical Areas

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

Areas of Consideration

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

Is access to facilities adequately controlled?

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

Are security measures in place?

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

G.1 SPONSOR PROGRAM MANAGEMENT AND ADMINISTRATION

Subtopical Areas to Sponsor Program Management and Administration

None

Current Directives:

The following references apply to Sponsor Program Management and Administration:

- DOE M 470.4-1, *Safeguards and Security Program Planning and Management*, 8-26-05
- DOE M 470.4-5, *Personnel Security*, 8-26-05
- DOE M 470.4-4, *Information Security*, 8-26-05
- DOE O 142.3, *Unclassified Foreign Visits and Assignments*, 6-18-04
- DOE M 475.1-1A, *Identifying Classified Information*, 2-26-01
- DOE O 200.1, *Information Management Program*, 9-30-96
- DOE O 471.1A, *Identification and Protection of Unclassified Controlled Nuclear Information*, 06-30-00
- DOE M 471.1-1 Chg 1, *Identification and Protection of Unclassified Controlled Nuclear Information Manual* 10-23-01
- DOE O 551.1B, *Official Foreign Travel*, 08-19-03
- DOE M 360.1B-1, *Federal Employee Training Manual*, 10-11-01

Sample Document List:

The following documentation should be considered for review:

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

Sample Interview Candidates:

The following individuals are candidates for interviews:

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

Sample Interview Questions:

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

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

G.2 COUNTERINTELLIGENCE REQUIREMENTS

Subtopical Areas to Counterintelligence (CI) Requirements

None

Current Directives:

The following references apply to CI Requirements:

- DOE M 470.4-1, *Safeguards and Security Program Planning and Management*, 8-26-05
- DOE M 470.4-5, *Personnel Security*, 8-26-05
- DOE M 470.4-4, *Information Security*, 8-26-05
- DOE O 142.3, *Unclassified Foreign Visits and Assignments*, 6-18-04
- DOE M 475.1-1A, *Identifying Classified Information*, 2-26-01
- DOE O 200.1, *Information Management Program*, 9-30-96
- DOE O 471.1A, *Identification and Protection of Unclassified Controlled Nuclear Information* 06-30-00
- DOE M 471.1-1 Chg 1, *Identification and Protection of Unclassified Controlled Nuclear Information Manual* 10-23-01
- DOE O 551.1B, *Official Foreign Travel*, 08-19-03
- DOE M 360.1B-1, *Federal Employee Training Manual*, 10-11-01

Sample Document List:

The following documentation should be considered for review:

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

Sample Interview Candidates:

The following people should be considered for possible interviews:

- Safeguard and Security Manager (DOE and Contractor)
- CI Program Manager (DOE and Contractor)
- Operations Security (OPSEC) Coordinator and/or OPSEC Working Group members
- Hosts/escorts
- Visit control

Sample Interview Questions:

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

- Which organization maintains the responsibility for indices checks?
- Who has approval authority for all unclassified visits and assignments at the site?
- Who approves the security plans for unclassified Foreign National Visits and Assignments (FNVA) to security areas?
- Is there a process covering the conduct and approval of CI consultations in lieu of indices not returning when return of indices is required?

- Do records indicate indices checks were requested and/or completed as required?
- What is the process for ensuring adequate coordination among security, CI, export control, and foreign intelligence should a foreign national require access to a security area or sensitive subject, or if the individual is visiting the site from a sensitive country?
- How does CI provide review and input to approval authority on FNVA requests?

G.3 EXPORT CONTROLS/TECHNOLOGY TRANSFER REQUIREMENTS

Subtopical Areas to Export Controls/Technology Transfer Requirements

None

Current Directives:

The following references apply to Export Controls/Technology Transfer requirements:

- DOE M 470.4-1, *Safeguards and Security Program Planning and Management*, 8-26-05
- DOE M 470.4-5, *Personnel Security*, 8-26-05
- DOE M 470.4-4, *Information Security*, 8-26-05
- DOE O 142.3, *Unclassified Foreign Visits and Assignments*, 6-18-04
- DOE M 475.1-1A, *Identifying Classified Information*, 2-26-01
- DOE O 200.1, *Information Management Program*, 9-30-96
- DOE O 471.1A, *Identification and Protection of Unclassified Controlled Nuclear Information*, 06-30-00
- DOE M 471.1-1 Chg 1, *Identification and Protection of Unclassified Controlled Nuclear Information Manual* 10-23-01
- DOE O 551.1B, *Official Foreign Travel*, 08-19-03
- DOE M 360.1B-1, *Federal Employee Training Manual*, 10-11-01

Sample Document List:

The following documentation should be considered for review:

- Sensitive countries listing
- Documentation identifying sensitive topics
- Visit-specific security plans
- Notification of approval documentation
- 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:

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

Sample Interview Questions:

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

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

G.4 SECURITY REQUIREMENTS

Subtopical Areas to Security Requirements

None

Current Directives:

The following references apply to Security Requirements:

- DOE M 470.4-1, *Safeguards and Security Program Planning and Management*, 8-26-05
- DOE M 470.4-5, *Personnel Security*, 8-26-05
- DOE M 470.4-4, *Information Security*, 8-26-05
- DOE O 142.3, *Unclassified Foreign Visits and Assignments*, 6-18-04
- DOE M 475.1-1A, *Identifying Classified Information*, 2-26-01
- DOE O 200.1, *Information Management Program*, 9-30-96
- DOE O 471.1A, *Identification and Protection of Unclassified Controlled Nuclear Information*, 06-30-00
- DOE M 471.1-1 Chg 1, *Identification and Protection of Unclassified Controlled Nuclear Information Manual* 10-23-01
- DOE O 551.1B, *Official Foreign Travel*, 08-19-03
- DOE M 360.1B-1, *Federal Employee Training Manual*, 10-11-01

Sample Document List:

The following documentation should be considered for review:

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

Sample Interview Candidates:

The following people should be interviewed regarding the export control and tech transfer programs:

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

Sample Interview Questions:

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

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

G.5 APPROVALS AND REPORTING

Subtopical Areas to Approvals and Reporting

None

Current Directives:

The following references apply to the approval and reporting process used for Unclassified Visits and Assignments by Foreign Nationals:

- DOE M 470.4-1, *Safeguards and Security Program Planning and Management*, 8-26-05
- DOE M 470.4-5, *Personnel Security*, 8-26-05
- DOE M 470.4-4, *Information Security*, 8-26-05
- DOE O 142.3, *Unclassified Foreign Visits and Assignments*, 6-18-04
- DOE M 475.1-1A, *Identifying Classified Information*, 2-26-01
- DOE O 200.1, *Information Management Program*, 9-30-96
- DOE O 471.1A, *Identification and Protection of Unclassified Controlled Nuclear Information*, 06-30-00
- DOE M 471.1-1 Chg 1, *Identification and Protection of Unclassified Controlled Nuclear Information Manual* 10-23-01
- DOE O 551.1B, *Official Foreign Travel*, 08-19-03
- DOE M 360.1B-1, *Federal Employee Training Manual*, 10-11-01

Sample Document List:

The following documentation should be considered for review:

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

Sample Interview Candidates:

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

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

Sample Interview Questions:

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

- Which organization maintains the responsibility for indices checks?
- Who has approval authority for all unclassified visits and assignments at the site?
- Who approves the security plans for unclassified FNVA to security areas?

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

UNCLASSIFIED VISITS & ASSIGNMENTS BY FOREIGN NATIONALS SAMPLE WORKSHEETS & PERFORMANCE TESTS

The following worksheets and sample performance tests can be utilized during the survey 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 foreign nationals?
- 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 counterintelligence, 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 foreign nationals from terrorist countries approved by the U.S. Secretary of Energy? This can be verified through sample record review. Sample should include only those terrorist country visits and assignments since 08/99.
- Are all visits/assignments being added to the DOE Foreign Access Central Tracking System (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 foreign nationals 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 foreign national 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 foreign nationals? Has the plan been reviewed and approved by the DOE cognizant security authority?
- 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 cognizant security authority?
- Do the areas identified as security areas in the standard or specific security plans match the current list of security areas of the facility? Check with the Physical Security Inspector for verification or list of areas.

- 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 responsibility? Does anyone discuss prohibited articles, badging, areas access is limited to, etc., with the visitor?
- Are the foreign nationals issued a unique badge that identifies them as a non-U.S. citizen?
- Do badging and visitor control procedures address what approvals must be in place before a foreign national is issued a visitor or permanent badge?
- Are foreign national 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 foreign national requirements, as they relate to Cyber Security, with the inspector evaluating Unclassified Cyber Security.

Sample Performance Test
Unclassified Visits and Assignments by Foreign Nationals: Sponsor Program Management and Administration

<p>FACILITY:</p> <p>TOPICAL AREA: UNCLASSIFIED VISITS & ASSIGNMENTS BY FOREIGN NATIONALS</p> <p>SUBTOPIC: Sponsor Program Management and Administration</p>
<p>TEST OBJECTIVE:</p> <p>This test will be used to determine that a system/process is implemented to ensure DOE requirements are met regarding a visit by a foreign national from a non-sensitive country.</p>
<p>REFERENCES:</p> <p>DOE O 142.3, <i>Unclassified Foreign National Visits and Assignments</i>, 6-18-04</p>
<p>TEST PROCEDURES AND CONDITIONS:</p> <p><u>Procedures:</u></p> <ol style="list-style-type: none"> a. The survey team member will prepare a request for an unclassified visit to the facility by a foreign national from a non-sensitive country. b. The survey team member will review the facility procedures for implementation and then coordinate with a facility representative to submit the request to the visitor control staff. c. The survey team member will observe the visitor control staff in the processing of the visit request from start to finish, noting if correct forms and plans are used. <p><u>Conditions:</u></p> <p>Normal work conditions.</p>
<p>EVALUATION CRITERIA OR STANDARDS:</p> <p>Facility implementation procedures are followed.</p>
<p>TEST RESULTS:</p> <p>Facility implementation procedures are followed. A written evaluation may be prepared to document the implementation procedures.</p>
<p>PASS: _____ FAIL: _____ DATE OF TEST: _____</p>
<p>Survey Team Member: _____ Date: _____</p> <p>Team Lead: _____ Date: _____</p> <p>DOE Safety: _____ Date: _____</p> <p>Site Representative: _____ Date: _____</p>

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

Subtopical Areas

H.1 PROGRAM ADMINISTRATION

H.2 MATERIAL ACCOUNTABILITY

H.3 MATERIAL CONTROL

Areas of Consideration

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

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

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

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

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

Has management established an effective and efficient organization structure?

- Is the MC&A function sufficiently independent from production operations to ensure that there are no conflicts of interest that might be detrimental to the protection of nuclear materials?
- Are there indications of frequent change in the organizational structure?
- Where are roles, responsibilities, and authorities defined and documented?
- Are lines of communication, accountability, and authority clear?
- Is the organization at a level to achieve effective program implementation?
- Is there a documented program that ensures personnel performing MC&A functions are trained and qualified?

Has the facility properly categorized its nuclear material?

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

Do the Site Safeguards and Security Plans (SSSP)/Vulnerability Assessment documents adequately address MC&A elements?

- Do MC&A personnel participate actively in the SSSP development?
- Was the full threat spectrum used and were multiple scenarios evaluated and documented?
- Were single, abrupt, and protracted theft and diversion scenarios documented?
- Is the documentation consistent with the MC&A plan, procedural directives, and security-related documentation, and does it accurately correlate with conditions at the facility?

H.1 PROGRAM ADMINISTRATION

Subtopical Areas to Program Administration

None

Current Directives:

The following references apply to Program Administration:

- DOE M 470.4-6, *Nuclear Material Control and Accountability*, 8-26-05
- DOE O 470.4, *Safeguards and Security Program*, 8-26-05
- DOE M 232.1-1A, *Occurrence Reporting and Processing of Operations Information*, 7-21-97

Sample Document List:

Documentation to be reviewed may include the following:

- Material Control and Accountability (MC&A) plans and procedures
- Site Safeguards and Security Plan (SSSP) and Vulnerability Assessments (VAs)
- Deviations and exceptions
- Organization charts
- Training records, lesson plans
- MC&A assessment program plans
- Internal assessments and corrective action plans
- 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
- Material Balance Area Custodians/alternate custodians
- Emergency management personnel
- Operations personnel
- Personnel responsible for developing SSSP/VA documents
- Personnel responsible for MC&A internal reviews and assessments

Sample Interview Questions:

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

- Has a nuclear MC&A program that meets the requirements of DOE O 470.4 and DOE M 470.4-6 for all special, source, and other nuclear materials on inventory under a three-letter reporting identification symbol been implemented?
- Is the MC&A management official organizationally independent from responsibilities of other programs?
- Is the MC&A program documented in an approved MC&A plan and procedure?
- Is the MC&A program implemented on the basis of the graded safeguards concept?
- Has a program to periodically review and assess the integrity and quality of the MC&A program and practices been implemented?
- Has a documented program to ensure that personnel performing MC&A function are trained and qualified been implemented?

- Has a loss-detection evaluation been performed and documented for each Category I facility including facilities for which a credible scenario for rollup of Category II to a Category I quantity of special nuclear materials has been identified?
- Have performance requirements for MC&A system elements been documented and a performance testing program implemented?
- Have MC&A loss-detection elements been included in documented procedures for reporting Incidents of Security Concern?
- Are procedures developed and documented for characterizing nuclear materials on inventory to determine categories and attractiveness for implementation of the graded safeguards concept?

H.2 MATERIAL ACCOUNTABILITY

Subtopical Areas to Material Accountability

None

Current Directives:

The following references apply to Material Accountability:

- DOE M 470.4-6, *Nuclear Material Control and Accountability*, 8-26-05
- DOE O 470.4, *Safeguards and Security Program*, 8-26-05
- DOE M 470.4-1, *Safeguards and Security Program Planning and Management*, 8-26-05
- DOE M 232.1-1A, *Occurrence Reporting and Processing of Operations Information*, 7-21-97

Sample Document List:

Documentation to be reviewed may include the following:

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

Sample Interview Candidates:

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 Interview Questions:

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

- Does the accounting structure assist in the determination of the category and attractiveness level of each MBA?
- Who determines the MBA and account structure? Who can change it? How is it changed?
- What role does the accounting system play in determining categories of MBAs?
- What role does the accounting system play during inventory?
- What records does the system require to be input? Are data transcribed? How are laboratory data input?

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

H.3 MATERIAL CONTROL

Subtopical Areas to Material Control

None

Current Directives:

The following references apply to Material Control:

- DOE M 470.4-6, *Nuclear Material Control and Accountability*, 8-26-05
- DOE O 470.4, *Safeguards and Security Program*, 8-26-05
- DOE M 232.1-1A, *Occurrence Reporting and Processing of Operations Information*, 7-21-97
- DOE M 470.4-3, *Protective Force*, 8-26-05
- DOE M 470.4-2, *Physical Protection*, 8-26-05

Sample Document List:

Documentation to be reviewed may include the following:

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

Sample Interview Candidates:

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 Interview Questions:

Suggested interview questions may include the following:

- How are keys and combinations to Special Nuclear Materials (SNM) areas controlled?
- Does the facility have a documented program to provide controls of nuclear material operations relative to Material Access Areas (MAAs)?
- Are there approved procedures governing MBA-to-MBA and MAA-to-MAA material transfers?
- What training is provided to MBA custodians? Frequency?
- What transfer controls are in place?

- Are documented controls covering nuclear material being used or stored in processing areas?
- How is access to SNM use and storage locations approved?
- How is the two-person rule implemented at the facility?
- Are material custodians prohibited from hands-on SNM functions?
- Are searches conducted of all persons exiting an MAA?
- Is a daily administrative check program implemented at the facility?
- How is the TID program documented and approved?
- Does the TID program include sample testing of new TIDs to ensure compliance with requirements?
- Who is responsible for testing and calibrating portal monitors? Are problems corrected in a timely manner?

MATERIAL CONTROL AND ACCOUNTABILITY SAMPLE WORKSHEETS & PERFORMANCE TESTS

The following worksheets and sample performance tests can be utilized during the survey process to evaluate the status of the material control and accountability topical area.

**Sample Performance Test
Material Accounting: Document Sampling**

<p>FACILITY:</p> <p>TOPICAL AREA: NUCLEAR MATERIAL CONTROL & ACCOUNTABILITY</p> <p>SUBTOPIC: MATERIAL ACCOUNTABILITY: Document Sampling</p>
<p>TEST OBJECTIVE: This test will determine whether the accounting system is in compliance with all reporting requirements.</p>
<p>REFERENCES: DOE M 470.4-6, <i>Nuclear Material Control and Accountability</i>, 8-26-05 DOE M 470.4-1, <i>Safeguards and Security Program Planning and Management</i>, 8-26-05 Local procedures</p>
<p>TEST PROCEDURES AND CONDITIONS: Randomly select a sample of accounting documents to verify accuracy and completeness and then use this sample to physically locate material. (May be used with the tests for accountability, data traceability, and item location.)</p>
<p>EVALUATION CRITERIA OR STANDARDS: <u>Evaluation Criteria:</u></p> <ol style="list-style-type: none"> Were all records complete, accurate, and submitted in a timely manner? If discrepancies exist, are they a systemic problem or isolated cases? Does the information in the records agree with the physical inventory
<p>TEST RESULTS:</p> <ol style="list-style-type: none"> All records were complete, accurate, and submitted in a timely manner. If discrepancies exist, they were due to a systemic problem or were an isolated case. The information in the records agrees with the physical inventory.
<p>PASS: _____ FAIL: _____ DATE OF TEST: _____</p>
<p>Survey Team Member: _____ Date: _____</p> <p>Team Lead: _____ Date: _____</p> <p>DOE Safety: _____ Date: _____</p> <p>Site Representative: _____ Date: _____</p>

**Sample Performance Test
Material Accounting: Accounting System**

FACILITY:

TOPICAL AREA: NUCLEAR MATERIAL CONTROL & ACCOUNTABILITY

SUBTOPIC: MATERIAL ACCOUNTABILITY: Accounting System

TEST 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.

REFERENCES:

DOE M 470.4-6, *Nuclear Material Control and Accountability*, 8-26-05
DOE M 470.4-1, *Safeguards and Security Program Planning and Management*, 8-26-05
Local procedures

TEST PROCEDURES AND CONDITIONS:

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 OR STANDARDS:

Evaluation Criteria:

- a. Were operations successfully restarted?
- b. Was there resolution of all items, operations, and measurements affected while the system was down?
- c. Was the system successfully restarted from backup data or systems?

TEST RESULTS:

- a. Operations were successfully restarted.
- b. There was resolution of all items, operations, and measurements affected while the system was down.
- c. The system was successfully restarted from backup data or systems.

PASS: _____ **FAIL:** _____ **DATE OF TEST:** _____

Survey Team Member: _____ **Date:** _____

Team Lead: _____ **Date:** _____

DOE Safety: _____ **Date:** _____

Site Representative: _____ **Date:** _____

Sample Performance Test

Material Accounting: Material Transfer Checks for Material Balance Area (MBA) Categorization

FACILITY:

TOPICAL AREA: NUCLEAR MATERIAL CONTROL & ACCOUNTABILITY

SUBTOPIC: MATERIAL ACCOUNTABILITY: Material Transfer Checks for MBA Categorization

TEST 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.

REFERENCES:

DOE M 470.4-6, *Nuclear Material Control and Accountability*, 8-26-05

DOE M 470.4-1, *Safeguards and Security Program Planning and Management*, 8-26-05

Local procedures

TEST PROCEDURES AND CONDITIONS:

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 OR STANDARDS:

- a. Do procedures exist to prohibit the increase in category level for MBAs?
- b. Was the attempted transfer detected?
- c. Was the facility response to the attempted transfer appropriate?

TEST RESULTS:

- a. Procedures exist to prohibit the increase in category level for MBAs.
- b. The attempted transfer was detected.
- c. The facility response to the attempted transfer was appropriate.

PASS: _____ **FAIL:** _____ **DATE OF TEST:** _____

Survey Team Member: _____ **Date:** _____

Team Lead: _____ **Date:** _____

DOE Safety: _____ **Date:** _____

Site Representative: _____ **Date:** _____

Sample Performance Test
Material Accounting: Item Identification Front and Back Checks

<p>FACILITY:</p> <p>TOPICAL AREA: NUCLEAR MATERIAL CONTROL & ACCOUNTABILITY</p> <p>SUBTOPIC: MATERIAL ACCOUNTABILITY: Item Identification Front and Back Checks</p>
<p>TEST OBJECTIVE: This test will determine whether the facility records accurately reflect the identity, value, and location of inventory items.</p>
<p>REFERENCES: DOE M 470.4-6, <i>Nuclear Material Control and Accountability</i>, 8-26-05 DOE M 470.4-1, <i>Safeguards and Security Program Planning and Management</i>, 8-26-05 Local procedures</p>
<p>TEST PROCEDURES AND CONDITIONS: Select a sample of items from either the inventory listing or during the field inspections. Record the item ID, location, plutonium weight, and tamper indicating device (TID). Verify the items in the field or the sample taken from the field to the accountability system records.</p>
<p>EVALUATION CRITERIA OR STANDARDS: Were items in the field successfully reconciled to the nuclear material accounting system records?</p>
<p>TEST RESULTS: The items in the field were successfully reconciled to the nuclear material accounting system records.</p>
<p>PASS: _____ FAIL: _____ DATE OF TEST: _____</p>
<p>Survey Team Member: _____ Date: _____</p> <p>Team Lead: _____ Date: _____</p> <p>DOE Safety: _____ Date: _____</p> <p>Site Representative: _____ Date: _____</p>

**Sample Performance Test
Material Accounting: Accounting System Forms**

<p>FACILITY:</p> <p>TOPICAL AREA: NUCLEAR MATERIAL CONTROL & ACCOUNTABILITY</p> <p>SUBTOPIC: MATERIAL ACCOUNTABILITY: Accounting System Forms</p>
<p>TEST OBJECTIVE:</p> <p>This test will determine the effectiveness of the system utilized for filing controlled accountability forms used in the Material Balance Area (MBA). Check key information on documents reviewed, including form used for transfers of special nuclear material (SNM).</p>
<p>REFERENCES:</p> <p>DOE M 470.4-6, <i>Nuclear Material Control and Accountability</i>, 8-26-05</p> <p>DOE M 470.4-1, <i>Safeguards and Security Program Planning and Management</i>, 8-26-05</p> <p>Local procedures</p>
<p>TEST PROCEDURES AND CONDITIONS:</p> <p>For each type of control and accountability record, randomly select 10% (or a minimum of 1) of the forms used in the MBA during the review period. Locate these specific records and check key entries for completeness.</p>
<p>EVALUATION CRITERIA OR STANDARDS:</p> <p><u>Evaluation Criteria:</u></p> <ol style="list-style-type: none"> a. Could all forms be located during the field investigation portion of the review? b. Were all corrections or lineouts initialed by the custodian done in accordance with requirements? c. Did all of the forms contain the required information?
<p>TEST RESULTS:</p> <ol style="list-style-type: none"> a. All MBA transactions were properly documented using the applicable controlled accountability form. b. All transaction documents were completed according to applicable procedures.
<p>PASS: _____ FAIL: _____ DATE OF TEST: _____</p>
<p>Survey Team Member: _____ Date: _____</p> <p>Team Lead: _____ Date: _____</p> <p>DOE Safety: _____ Date: _____</p> <p>Site Representative: _____ Date: _____</p>

**Sample Performance Test
Material Control: Tamper Indicating Device (TID) System**

<p>FACILITY:</p> <p>TOPICAL AREA: NUCLEAR MATERIAL CONTROL & ACCOUNTABILITY</p> <p>SUBTOPIC: MATERIAL CONTROL: TID System</p>
<p>TEST OBJECTIVE: This test will determine whether TID discrepancies are detected and if proper resolution is achieved. May be included as a test of daily administrative checks and physical inventories.</p>
<p>REFERENCES: DOE M 470.4-6, <i>Nuclear Material Control and Accountability</i>, 8-26-05 DOE M 470.4-1, <i>Safeguards and Security Program Planning and Management</i>, 8-26-05 Local procedures</p>
<p>TEST PROCEDURES AND CONDITIONS: Replace a TID with another TID without initiating changes in accounting records; OR make a change in the TID number in the accounting records.</p>
<p>EVALUATION CRITERIA OR STANDARDS: <u>Evaluation Criteria:</u></p> <ol style="list-style-type: none"> a. Was the different number detected? b. Were records checked to verify which TID should be on the item? c. Was the item remeasured to verify the special nuclear material (SNM) content?
<p>TEST RESULTS: The answer to all questions must be “yes” to pass.</p> <ol style="list-style-type: none"> a. Was an investigation initiated to locate the TID recorded but not present? b. Were procedures for application and removal of TIDs reviewed? c. Were operations successfully restarted?
<p>PASS: _____ FAIL: _____ DATE OF TEST: _____</p>
<p>Survey Team Member: _____ Date: _____</p> <p>Team Lead: _____ Date: _____</p> <p>DOE Safety: _____ Date: _____</p> <p>Site Representative: _____ Date: _____</p>

**Sample Performance Test
Material Control: Material Surveillance – Two-Person Rule**

<p>FACILITY:</p> <p>TOPICAL AREA: NUCLEAR MATERIAL CONTROL & ACCOUNTABILITY</p> <p>SUBTOPIC: MATERIAL CONTROL: Material Surveillance – Two-person rule</p>
<p>TEST OBJECTIVE: This test will determine if the two-person rule can be compromised.</p>
<p>REFERENCES: DOE M 470.4-6, <i>Nuclear Material Control and Accountability</i>, 8-26-05 DOE M 470.4-1, <i>Safeguards and Security Program Planning and Management</i>, 8-26-05 Local procedures</p>
<p>TEST PROCEDURES AND CONDITIONS: 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, Tamper Indicating Device (TID) applications, etc.</p>
<p>EVALUATION CRITERIA OR STANDARDS: <u>Evaluation Criteria:</u> a. Did the person leave the area? b. Was a second authorized person called to provide two-person coverage?</p>
<p>TEST RESULTS: The answer to all questions must be “yes” to pass. a. Was the two-person rule compromised at any time during the operation? b. Do procedures cover situations for replacing one of the two-person team if that person must leave?</p>
<p>PASS: _____ FAIL: _____ DATE OF TEST: _____</p>
<p>Survey Team Member: _____ Date: _____</p> <p>Team Lead: _____ Date: _____</p> <p>DOE Safety: _____ Date: _____</p> <p>Site Representative: _____ Date: _____</p>

Sample Performance Test
Material Accounting: Measurements and Measurements Control – Scales and Balances

<p>FACILITY:</p> <p>TOPICAL AREA: NUCLEAR MATERIAL CONTROL & ACCOUNTABILITY (MC&A)</p> <p>SUBTOPIC: MATERIAL ACCOUNTING: Measurements and Measurements Control – Scales and Balances</p>
<p>TEST OBJECTIVE: This test will determine whether the Scales and Balances program provides data of the quality required for MC&A records.</p>
<p>REFERENCES: DOE M 470.4-6, <i>Nuclear Material Control and Accountability</i>, 8-26-05 DOE M 470.4-1, <i>Safeguards and Security Program Planning and Management</i>, 8-26-05 Local procedures</p>
<p>TEST PROCEDURES AND CONDITIONS: Select a sample of accountability weighing instruments from the MC&A organization records and verify the frequency and currency of the calibration and the performance of daily linearity checks. Check the performance of the instrument against standards normally used or against independent weight standards that are in the normal weighing range of the instrument.</p>
<p>EVALUATION CRITERIA OR STANDARDS: <u>Evaluation Criteria:</u></p> <ol style="list-style-type: none"> a. Was instrument calibration current? b. Are appropriate standards being used? c. Are daily checks being made? d. Were personnel familiar with the operation and MC&A procedures? e. Did the instruments perform to the stated specification?
<p>TEST RESULTS: The answer to all questions must be “yes” to pass.</p> <ol style="list-style-type: none"> a. Were all requirements documented by the facility for the Scales and Balance program? b. Were personnel performing measurements trained in or knowledgeable of the program requirements? c. Was weighing performed in accordance with applicable procedures?
<p>PASS: _____ FAIL: _____ DATE OF TEST: _____</p>
<p>Survey Team Member: _____ Date: _____</p> <p>Team Lead: _____ Date: _____</p> <p>DOE Safety: _____ Date: _____</p> <p>Site Representative: _____ Date: _____</p>

5.0 **POST-SURVEY TOOLS**

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

- 5.1 Sample Report Format
- 5.2 Sample Termination Survey Report
- 5.3 Report Writing Guide
- 5.4 Sample Slides for the Exit Briefing
- 5.5 Transmittal Memorandum
- 5.6 DOE F 470.8, Survey/Inspection Report Form
- 5.7 Sample Corrective Action Plans
- 5.8 Sample Root Cause Analysis Form
- 5.9 Sample Request for Finding Closure/Validation

5.1 Sample 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 description of the protection program), conclusions, synopsis of findings, and appendices.

In addition to the completed DOE F 470.8, Survey/Inspection Report for the report must include:

- a. 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.
- b. Report Content.
 - (1) Initial/Periodic Survey Reports and Self-Assessment Reports. Reports must contain the following items.
 - (a) A completed DOE F 470.8 (or equivalent for self-assessments).
 - (b) An executive summary containing:
 - 1 The scope, methodology, period of coverage, duration, date of the exit briefing to management;
 - 2 A brief overview of the facility, function, scope of operations, and contractual information (e.g., contract number, award and expiration dates, contract type, identification of security clauses, identification of the security and overall scores assigned to the most recent contract appraisal);
 - 3 A brief synopsis of major strengths and weaknesses that impact the effectiveness of the facility's overall S&S program, including identification of any topical areas rated less than satisfactory;
 - 4 The overall composite facility rating with supporting rationale; and
 - 5 A reference to a list of findings identified during the survey or self-assessment.
 - (c) An introduction containing:
 - 1 The scope, methodology, period of coverage, duration, date of the exit briefing to management; and
 - 2 A description of the facility, its function and scope of operations, security interests, and contractual information (e.g., contract number, award and expiration dates, contract type, identification of security clauses, identification of the security and overall scores assigned to the most recent contract appraisal).
 - (d) Narrative for all rated topical and subtopical areas that includes:
 - 1 A description of the site's implementation of the program element;
 - 2 The scope of the evaluation;
 - 3 A description of activities conducted;
 - 4 The evaluation results and associated issues (including other Department elements or OGA review or inspection results related to this topic/subtopic that were included in the survey);

- 5 The identification of all findings, including new and previously identified open findings, regardless of source (e.g., HS-60, IG, GAO, and their current corrective action status; and
- 6 An analysis that provides a justification and rationale of the factors responsible for the rating.

(e) Attachments, including:

- 1 A copy of the current DOE F 470.2, “Facility Data and Approval Record” (FDAR);
- 2 A listing of all active DOE F 470.1, “Contract Security Classification Specification” (CSCS), or DD F 254, “Contract Security Classification Specification;”
- 3 A listing of all new findings resulting from the survey/self-assessment;
- 4 A listing of all previous findings that are open, to include the current status of corrective action;
- 5 A listing of team members including names, employer, and their assigned area(s) of evaluation; and
- 6 A listing of all source documentation used to support the survey/self-assessment conduct and results (e.g., GAO, IG, Office of Independent Oversight (HS-60), and similar assessment documents).

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

The report should reflect the compliance and performance segments of the survey. 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 inspected, and what was found. A summary of content requirements appears below.

- The status (e.g., approved, pending) of any required planning documents (e.g., Site Safeguard and Security Plan [SSSP], Material Control and Accountability [MC&A], Information System Security [ISS]).
- All new findings, with Safeguards and Security Information Management System-compatible finding numbers, should be identified. Open findings from the previous survey should be identified in the narrative portion of the survey 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 survey.
- A description of the facility's strengths and weaknesses should correlate to the results from the compliance and performance survey segments, and discuss the bases for the ratings. The survey

report should reflect validated and defensible ratings. Assigned performance ratings should be based upon 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 survey 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 survey scope, scope of operations, corrective actions or findings, discussion of significant impact, and analysis of each topical area.

5.2 Sample Termination Survey Report

SCOPE

This report documents the results of the Safeguards and Security (S&S) termination survey of the XXX Site facilities Safeguards and Security Division (SSD) which was conducted by personnel from XXX Site Office. This report contains the results of the termination survey conducted February 28 – March 4, 2005.

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

FACILITY OPERATIONS

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

VERIFICATION ACTIVITIES

RESOLUTION OF FINDINGS

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

CLASSIFIED MATTER

All classified matter, including accountable matter has either been destroyed or transferred to NSO.

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

SSD has executed a Certificate of Non-possession for activities at Building XXX; a copy is included as **Appendix 1**.

Communications Security (COMSEC)

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

Security Officer.

NUCLEAR MATERIAL CONTROL AND ACCOUNTABILITY

SSD did not possess nuclear and other hazardous material presenting a potential radiological or toxicological sabotage threat as explained above.

PERSONNEL SECURITY

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

FACILITY CLEARANCE

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

CONCLUSION

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

5.3 Report Writing Guide

Introduction

This Report Writing Guide describes the philosophy, scope, and general procedures for documenting the activities associated with the conduct of S&S surveys or self-assessments. It addresses the requirements specified in DOE M 470.4-1, Section G, as it pertains to the writing of survey reports. However, it is also important to note that this Guide goes further by offering suggestions beyond those identified in the DOE directive. This Guide is directed at fundamentals; it does not address writing styles, sentence structure, grammar, or punctuation. It is designed to give the user specific direction on what level of content is expected within the survey report, along with some general information on how to present this information in a more clear and direct manner.

The second section of this Guide focuses on report writing mechanics. It describes the basic elements of the survey report (narrative, findings). The purposes of each of these elements are described along with some examples of how they may be written. This chapter also addresses the appropriate use and documentation of other assessment reports used to augment the survey report. Lastly, this chapter addresses the most critical aspect of the survey report, the end product of analyzing all collected data, and the resulting conclusion about the effectiveness of the S&S program.

The third section focuses exclusively on survey content. Each section of the survey report will be addressed including the Executive Summary, each Topical Area and, to a lesser extent, the types of information to be included for each subtopical area.

The final section addresses all other types of survey reports. These include special surveys, termination surveys, surveys for non-possessing (NP) facilities, and excluded parent organizations. The chapter also discusses the importance of self-assessments and the applicability of this Guide to that process.

Report Writing Mechanics

This section of the S&S Report Writing Guide is applicable to all types of survey reports, regardless of the objectives of the report (i.e., Initial, Periodic, Termination). The S&S Survey 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 of the potential audiences reading it can understand it with equal clarity. One of the great errors of many organizations responsible for writing survey reports is the failure to recognize the many different audiences that may encounter the report. Certainly it will be used internally at the site, but copies of the report are sent to DOE-Headquarters elements, other DOE elements that have an interest in the facility, potentially other government agencies, and ultimately to the highest levels of the Executive and Legislative branches of U.S. government.

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 the understanding of the detached third-party reader, such as a member of Congress. Keep in mind that the ultimate goal of the survey report is the documentation of the status of the S&S program and its capability to protect target assets. To be an acceptable report, it 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

Survey reports must describe the conduct, evaluation activities, and results of the evaluation of the S&S program. The report must contain certain minimum requirements. Initial and periodic survey reports are divided into essentially four main parts: the Executive Summary, the Introduction, the body of the report, and finally the attachments. Other types of survey reports will be addressed separately. 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 survey report read. It is therefore critical, that this section capture all the important “big-picture” details associated with the survey. The Executive Summary is normally one to three pages in length and contains, at a minimum, the following information:

- A statement reflecting survey 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 the survey. Usually the period of coverage is 12 months (or from the end of the last survey to the beginning of this one).
- The survey methodologies/techniques used (e.g., document reviews, observations interviews, performance tests). Keep in mind these are simply a broad list of the inspection methods and techniques used during the survey. It is not intended to address the inspection activities associated with each subtopical area.
- A brief overview of the facility, function, and scope of operations. Brief is the key word here. The Executive Summary is usually one to three pages, so detailed descriptions would be inappropriate. This overview should provide the reader with enough information to understand what type of facility was surveyed, why that 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 composite rating, as well as the ratings for the topical areas.
- 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 with supporting rationale. The supporting rationale may be explained in conjunction with the syntheses of major strengths and weaknesses or it 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 survey report. The Introduction provides a place for this information and sets the tone of the survey. Information that should be included in the Introduction section of the report includes:

- The period of coverage for the survey. Although mentioned in the Executive Summary, it is important to include that information in the body of the survey report as well. In addition, if the survey happened to have been extended (i.e., skipped one survey cycle in accordance with the provisions of DOE O 470.4-1, Section G), then the coverage should reflect the 24 months since the last survey. If long-standing issues are being evaluated (e.g., resolution of past findings, status of line-item budget upgrade) activities occurring outside of the 12 or 24 month window may be subject to evaluation. This should be specified in the Introduction.
- Composition of survey team members and the areas evaluated. This serves as a record for management if questions should arise in the future or as a resource in assisting with the validation of corrective actions.
- Description of the facility, its function, and its scope of operations. Without question this has been one of the more controversial items to be contained in the survey report. The controversy surrounds the level of detail necessary to adequately describe the facility, its function, and its scope of operations. The report should contain enough information to allow the reader to have a basic understanding of what types of operations are occurring at the facility, and a brief description of the physical layout of the facility itself. However, detailed information about the operations of particular programs should not be addressed. This information should provide a description of the function and scope of operations and the 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 SSSP or Site Security Plan. This issue will again be addressed during the discussion of the Narrative section of the report.

- **Report Body**

- **Narrative**

The Narrative section of the report is where the “story” of the survey is actually told. The narrative explains what actually occurred during the inspection and how the protection measures were evaluated. There are actually two parts to the narrative. The first part serves as an introduction to the topical/subtopical area being evaluated. This 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.
- The status of corrective actions for all open findings and status of all open and closed findings from the previous survey 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.

The other part of the narrative describes the survey process. Much work and effort goes into the planning and conduct of an S&S survey. Unfortunately, the extent of this effort is lost due to a failure to adequately document the survey activities in the report. Because the narrative tells a story, then all parts of the story must be included. The following information should be contained at a minimum in the report narrative.

Scope of subtopical area evaluation. The report should describe what activities were evaluated within the subtopical area. For example, the subtopical area of Intrusion Detection and Assessment Systems was evaluated, and the scope of the evaluation would include the 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 surveyed.

Description of survey activities. The report should explain what was evaluated and how the evaluation was performed. This would include information such as how many personnel or items were sampled and the basis of the evaluation (i.e., What was the purpose of evaluation? What was the inspector attempting to validate or verify?).

Specific numbers (e.g., 125 records evaluated out of 1,000) or detailed information (number of hours observed at which types of locations) should be provided to give the reader a perspective of the extent of the survey activities. If a deficiency is noted, the narrative will describe how the deficiency was identified, the characteristics of the deficiency (isolated or systemic), and its implications.

Description of evaluation results and associated issues. This portion of the narrative documents what all of the survey activities mean. This portion of the narrative should document the 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 survey 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 survey 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 that 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 of that evaluation (i.e., that 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 the 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/program implementing procedure or the failure to meet a performance standard) that requires the implementation and tracking of corrective actions sufficient to prevent recurrence. Findings can be written for deficiencies that are isolated single-point failures or are systemic and capable of impacting other facilities or sites. However, the real art is in the ability to write a “good” finding.

There are two key things that should be remembered about findings. First, no finding should ever be written that, by its existence (and ultimate correction), would not improve the overall effectiveness of 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 the implementation of appropriate corrective action 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 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 develop corrective actions in response is not worth the costs involved because the end result will not positively impact S&S program effectiveness. A “good” finding is one that is firmly based in DOE policy, clearly communicates what is deficient, and improves the S&S program when corrected.

There are several requirements associated with findings that are explained in detail in the S&S Survey and Self-Assessment Guide (e.g., number of characters, specific method of numbering) This Guide focuses on the construction of the finding and the formula for writing a “good” finding. First, it is important to note that a finding is only as good as its supporting narrative. As discussed in the section above, the narrative tells the story. The narrative explains what is deficient, how the deficiency was validated, and the significance of that deficiency. Because findings are restricted to only 500 characters (including punctuation and spaces between words), an in-depth description of the circumstances surrounding the deficiency is not possible. 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 directives or meet documented performance standards. This may be reflected simply as:

Condition at the facility + DOE directives/requirements = Finding

Example: During the data collection phase of a survey, you have taken a representative sample of the 300 Security Police Officer (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 make-up training was never provided. DOE M 470.4-3. Section B, 4.b. (1) 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% deficiency rate, further sampling is not deemed necessary not only due to this rate, but also due to the limitation of time resources.

The finding for this deficiency would be written as follows:

FINDING: 20% 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 the above 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.

The following is a third approach to documenting the deficiency discussed above. This 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 make-up 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 make-up 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 (nor resolved) if the finding is focused on the reasoning rather than the situation.

However, if the survey 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.

A few other requirements associated with findings that must be remembered follow:

- Each finding and subsequent corrective action should be required to have a stand-alone security classification (i.e., be portion-marked).
- Findings will be documented in each survey report and listed separately at the end of the report. Each report will include an attachment, summary, or other section in which all the findings for the survey should be collected and 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 directive reference number.
- Each finding will have alpha/numeric references to the DOE orders, manuals, or other documents that identify the requirement(s) not being met.
- Each finding identified in the survey report should have a unique identification number assigned which can be used throughout the reporting and tracking process.

▪ **Attachments**

The report must also contain certain forms and other documentation that can be collectively defined as attachments. A list of this documentation follows:

- A completed DOE F 470.8
- A copy of the current DOE F 470.2 Facility Data and Approval Record (FDAR)
- A copy of each active DOE F 470.1 Contract Security Classification Specification (CSCS) or DD 254

- Any other items, as necessary, to provide supportive documentation regarding the scope of the evaluation or associated results.

Analysis and Conclusions

Each survey team member invests much effort in the planning and research for a survey. The team member spends extensive time (day and night) looking around, asking questions, and conducting performance tests. This portion of the narrative allows for the explanation of what all this effort means. What do the results of the survey efforts tell 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 the resulting rating. If there is inconsistency here, the validity of the entire survey effort may be called into question.

Use of Other Assessment Reports

Reviews or inspections, conducted by Departmental elements other than the Surveying Office, may be used to meet survey requirements. All topical and subtopical areas, as specified on DOE F 470.8, must be inspected. The Surveying Office can use the inspection of a topical or subtopical area if that area was inspected as part of an external review.

When using reviews to meet the requirements of the survey, the following guidelines must be followed:

- The review/inspection must have been conducted within the survey period.
- Applicable portions of the review/inspection must be attached to the survey report.
- Portions of topical and subtopical areas not covered by the review/inspection must be surveyed.
- If ratings were not assigned during the review/inspection, the Surveying Office must analyze the impact of any deficiencies and assign ratings.

Types of Survey Reports

There are a number of different types of surveys performed to accomplish very different objectives. For example, a survey may be performed to allow a facility to possess certain DOE security interests or to verify that all security interests have been removed once work requirements have ceased for the facility. The following briefly addresses some considerations for each type of survey report.

- **Initial Survey Reports**

Initial surveys must be conducted at facilities where there will be a clearance established for a facility with an importance rating of: A, B, C, or PP (see Section I, Chapter II of DOE M 470.1-1). Survey activities must be comprehensive and result in a satisfactory composite rating prior to a facility clearance being granted.

- **Periodic Survey Reports**

Periodic surveys are conducted for all facilities and must cover all applicable topics to ensure survey program objectives are met. The periodic survey may be composed of multiple special survey reports, provided all the requirements of this section of the Guide are met. Integration of internal and external reports including quality assurance, property appraisals, performance assurance, and other evaluation reports may be used to augment the requirement for a periodic survey. A DOE federal facility (e.g., site office) conducting a periodic survey is required to perform self-assessments as noted in Section (1)(e)6, below.

- Facilities with importance ratings of A, B, or C must be surveyed once every 12 months (with the exception of Category IV SNM-only facilities – see (1)(c) below).

- Facilities with an importance rating of PP must be surveyed once every 24 months.
- For facilities with Category IV SNM and nuclear material, including source material, the nuclear MC&A topical area must be surveyed at least once every 24 months.

Facilities with importance ratings of D, NP, or E do not require surveys but do require periodic reviews (see (1)(d)5, below).

- **Special Surveys**

Special surveys may be conducted at facilities for specific limited purposes. Examples include extended survey activities, technical security activities, “for cause” reviews, line management direction, shipment of nuclear and/or classified information or matter, or a change in the contractor operating a government-owned facility.

- **Termination Surveys**

Termination surveys must be conducted to verify the termination of Departmental activities and appropriate disposition of S&S interests. Examples of survey activities include: the appropriate disposition, destruction, or return of classified information or matter, SNM, hazardous material, property, security badge retrieval, debriefings, and subsequent verification of the termination or transfer of DOE access authorizations.

- Onsite termination surveys must be conducted at facilities possessing Top Secret matter, Sensitive Compartmented Information/Special Access Program information or matter, or SNM.
- Onsite or correspondence termination surveys must be accomplished for all other possessing facilities.

- **Review of Non-Possessing Facilities**

A documented review of entities (D, NP, and E facilities) such as subcontractors, consultants, and common carriers must be performed by the DOE cognizant security authority at least every five years. Reports for non-possessing facilities must include:

- A completed DOE F 470.8
- A copy of the DOE F 470.2 FDAR
- A list of each active DOE F 470.1 CSCS or DD F 254
- An evaluation of the Foreign Ownership, Control, or Influence status
- A determination that employees and subcontractors possess appropriate access authorizations
- A review to ensure that individuals no longer employed on the contract have had their access authorizations terminated and their security badges have been accounted for
- Other topical/subtopical areas identified on DOE F 470.8 as required by the DOE cognizant security authority.

Self-Assessments

Self-assessments must be conducted between the periodic surveys conducted by the cognizant security authority and include all applicable facility S&S program elements. Federal facilities may use the self-assessment to substitute for the periodic survey requirement. Non-possessing facilities are not required to conduct self-assessments. However, sponsoring organizations (federal or contractor) must include in their self-assessments a thorough review of their registration program for non-possessing facilities that may result in a program review of identified subcontractors.

Self-assessment reports must contain the following items:

- (1) Initial/Periodic Survey Reports and Self-Assessment Reports. Reports must contain the following items.
 - (a) A completed DOE F 470.8 (or equivalent for self-assessments).
 - (b) An executive summary containing:
 - 1 The scope, methodology, period of coverage, duration, date of the exit briefing to management;
 - 2 A brief overview of the facility, function, scope of operations, and contractual information (e.g., contract number, award and expiration dates, contract type, identification of security clauses, identification of the security and overall scores assigned to the most recent contract appraisal);
 - 3 A brief synopsis of major strengths and weaknesses that impact the effectiveness of the facility's overall S&S program, including identification of any topical areas rated less than satisfactory;
 - 4 The overall composite facility rating with supporting rationale; and
 - 5 A reference to a list of findings identified during the survey or self-assessment.
 - (c) An introduction containing:
 - 1 The scope, methodology, period of coverage, duration, date of the exit briefing to management; and
 - 2 A description of the facility, its function and scope of operations, security interests, and contractual information (e.g., contract number, award and expiration dates, contract type, identification of security clauses, identification of the security and overall scores assigned to the most recent contract appraisal).
 - (d) Narrative for all rated topical and subtopical areas that includes:
 - 1 A description of the site's implementation of the program element;
 - 2 The scope of the evaluation;
 - 3 A description of activities conducted;
 - 4 The evaluation results and associated issues (including other Department elements or OGA review or inspection results related to this topic/subtopic that were included in the survey);
 - 5 The identification of all findings, including new and previously identified open findings, regardless of source (e.g., HS-60, IG, GAO, and their current corrective action status; and
 - 6 An analysis that provides a justification and rationale of the factors responsible for the rating.

- (e) Attachments, including:
- 1 A copy of the current DOE F 470.2, “Facility Data and Approval Record” (FDAR);
 - 2 A listing of all active DOE F 470.1, “Contract Security Classification Specification” (CSCS), or DD F 254, “Contract Security Classification Specification;”
 - 3 A listing of all new findings resulting from the survey/self-assessment;
 - 4 A listing of all previous findings that are open, to include the current status of corrective action;
 - 5 A listing of team members including names, employer, and their assigned area(s) of evaluation; and
 - 6 A listing of all source documentation used to support the survey/self-assessment conduct and results (e.g., GAO, IG, HS-60, and similar assessment documents).

The following are some guidelines that should be followed to ensure the integrity of the report. First, 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 in the conduct of the assessment. If not, the self-assessment program has no integrity and management cannot trust the results of the self-assessment effort. Second, the self-assessment should be performed in an integrated fashion, such 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 that the results of the evaluation are examined in light of the results of all other evaluations. Third, 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 block,” 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 documented in a way that helps management effectively direct the program, then nothing has been gained.

Conclusion

The most effective program evaluation is of little value if it is not adequately documented. Those who have performed surveys in the past realize that the first document requested in planning for a survey is the most recent survey report. In addition to aiding management in the present, the survey report is the basis for future survey activity as well. Hopefully, this guide will be of assistance in documenting future survey activities.

5.4 Sample Exit Briefing

Classification

SAFEGUARDS AND SECURITY PERIODIC SURVEY

Name of Facility Surveyed
Facility Code

Dates of Survey

Conducted by
Surveying Office



Surveying Office

Classification

Classification

Topical and Sub-topical Ratings

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

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



Surveying Office

Classification

Classification

Protection Program Management

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

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

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

Continue for each sub-topical area.



Surveying Office

Classification

Classification

Composite Rating

A composite rating is based upon

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

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



Surveying Office

Classification

5.5 Sample Transmittal Memorandum

DATE: Within 60 working days after final closeout of the survey

REPLY TO
ATTN OF:

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

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

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

The composite rating assigned to [organization being surveyed] is [rating]. The assignment of this rating dictates that corrective action plans be developed within [number] working days. The [Organization, Office] will verify the adequacy and completeness of these action plans in accordance with DOE M 470.4-1, *Safeguards and Security Program Planning and Management*.

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

Include classification information as appropriate.

5.6 Survey / Inspection Report Form

DOE F 470.8

U.S. Department of Energy

SURVEY / INSPECTION REPORT FORM

1. Survey Type: <input type="checkbox"/> Initial <input type="checkbox"/> Periodic <input type="checkbox"/> Special <input type="checkbox"/> Termination <input type="checkbox"/> EPR <input type="checkbox"/> NPR <input type="checkbox"/> OA		3. Report #:		
3. Facility Name:		4. a. Facility Code: b. RIS Code:		
5. Survey Date(s):	6. a. Findings: <input type="checkbox"/> Yes <input type="checkbox"/> No b. Findings Against Other Facilities:	7. Composite Rating:		
8. Previous Survey Date(s):	9. Unresolved Findings: <input type="checkbox"/> Yes <input type="checkbox"/> No	10. Previous Rating:		
11a. Surveying Office:	11b. Cognizant Security Office:	11c. Other Offices with Interests:		
12. Ratings:				
<table style="width:100%; border:none;"> <tr> <td style="width:50%; vertical-align: top;"> <p>a) PROGRAM MANAGEMENT AND SUPPORT</p> <p>PROTECTION PROGRAM MANAGEMENT _____</p> <p>Program Management and Administration _____</p> <p>Resources and Budgeting _____</p> <p>Personnel Development and Training _____</p> <p>S&S PLANNING AND PROCEDURES _____</p> <p>MANAGEMENT CONTROL _____</p> <p>Surveys and Self Assessment Programs _____</p> <p>Performance Assurance Program _____</p> <p>Resolution of Findings _____</p> <p>Incident Reporting and Management _____</p> <p>PROGRAM WIDE SUPPORT _____</p> <p>Facility Approval and Registration of Activities _____</p> <p>Foreign Ownership, Control or Influence _____</p> <p>Security Management in Contracting _____</p> <p style="text-align: right;">OVERALL RATING _____</p> <p>b) PROTECTIVE FORCE</p> <p>MANAGEMENT _____</p> <p>TRAINING _____</p> <p>DUTIES _____</p> <p>FACILITIES AND EQUIPMENT _____</p> <p style="text-align: right;">OVERALL RATING _____</p> <p>c) PHYSICAL SECURITY</p> <p>ACCESS CONTROLS _____</p> <p>INTRUSION DETECTION & ASSESSMENT SYSTEMS _____</p> <p>BARRIERS AND DELAY MECHANISMS _____</p> <p>TESTING AND MAINTENANCE _____</p> <p>COMMUNICATIONS _____</p> <p style="text-align: right;">OVERALL RATING _____</p> <p>d) INFORMATION PROTECTION</p> <p>BASIC REQUIREMENTS _____</p> <p>TECHNICAL SURVEILLANCE COUNTERMEASURES _____</p> <p>OPERATIONS SECURITY _____</p> <p>CLASSIFICATION GUIDANCE _____</p> <p>CLASSIFIED MATTER PROTECTION & CONTROL _____</p> <p>Control of Classified Matter _____</p> <p>Special Access Programs and Intelligence Information _____</p> <p style="text-align: right;">OVERALL RATING _____</p> </td> <td style="width:50%; vertical-align: top;"> <p>e) CYBER SECURITY</p> <p>CLASSIFIED CYBER SECURITY _____</p> <p>Leadership, Responsibilities and Authorities _____</p> <p>C&A, Risk Management & Planning _____</p> <p>Policy, Guidance and Procedures _____</p> <p>Technical Implementation _____</p> <p>Performance Eval Feedback & Continuous Improvement _____</p> <p>TELECOMMUNICATIONS SECURITY _____</p> <p>UNCLASSIFIED CYBER SECURITY _____</p> <p>Leadership, Responsibilities and Authorities _____</p> <p>C&A Risk Management and Planning _____</p> <p>Policy, Guidance and Procedures _____</p> <p>Technical Implementation _____</p> <p>Performance Eval Feedback & Continuous Improvement _____</p> <p style="text-align: right;">OVERALL RATING _____</p> <p>f) PERSONNEL SECURITY PROGRAM</p> <p>ACCESS AUTHORIZATIONS _____</p> <p>HUMAN RELIABILITY PROGRAM _____</p> <p>CONTROL OF CLASSIFIED VISITS _____</p> <p>SAFEGUARDS AND SECURITY AWARENESS _____</p> <p style="text-align: right;">OVERALL RATING _____</p> <p>g) UNCLASSIFIED VISITS & ASSIGNMENTS BY FOREIGN NATIONALS</p> <p>SPONSOR PROGRAM MANAGEMENT & ADMIN _____</p> <p>COUNTERINTELLIGENCE REQUIREMENTS _____</p> <p>EXPORT CONTROLS/TECH TRANSFER REQUIREMENTS _____</p> <p>SECURITY REQUIREMENTS _____</p> <p>APPROVALS AND REPORTING _____</p> <p style="text-align: right;">OVERALL RATING _____</p> <p>h) NUCLEAR MATERIALS CONTROL & ACCOUNTABILITY</p> <p>PROGRAM ADMINISTRATION _____</p> <p>MATERIAL ACCOUNTABILITY _____</p> <p>MATERIALS CONTROL _____</p> <p style="text-align: right;">OVERALL RATING _____</p> </td> </tr> </table>			<p>a) PROGRAM MANAGEMENT AND SUPPORT</p> <p>PROTECTION PROGRAM MANAGEMENT _____</p> <p>Program Management and Administration _____</p> <p>Resources and Budgeting _____</p> <p>Personnel Development and Training _____</p> <p>S&S PLANNING AND PROCEDURES _____</p> <p>MANAGEMENT CONTROL _____</p> <p>Surveys and Self Assessment Programs _____</p> <p>Performance Assurance Program _____</p> <p>Resolution of Findings _____</p> <p>Incident Reporting and Management _____</p> <p>PROGRAM WIDE SUPPORT _____</p> <p>Facility Approval and Registration of Activities _____</p> <p>Foreign Ownership, Control or Influence _____</p> <p>Security Management in Contracting _____</p> <p style="text-align: right;">OVERALL RATING _____</p> <p>b) PROTECTIVE FORCE</p> <p>MANAGEMENT _____</p> <p>TRAINING _____</p> <p>DUTIES _____</p> <p>FACILITIES AND EQUIPMENT _____</p> <p style="text-align: right;">OVERALL RATING _____</p> <p>c) PHYSICAL SECURITY</p> <p>ACCESS CONTROLS _____</p> <p>INTRUSION DETECTION & ASSESSMENT SYSTEMS _____</p> <p>BARRIERS AND DELAY MECHANISMS _____</p> <p>TESTING AND MAINTENANCE _____</p> <p>COMMUNICATIONS _____</p> <p style="text-align: right;">OVERALL RATING _____</p> <p>d) INFORMATION PROTECTION</p> <p>BASIC REQUIREMENTS _____</p> <p>TECHNICAL SURVEILLANCE COUNTERMEASURES _____</p> <p>OPERATIONS SECURITY _____</p> <p>CLASSIFICATION GUIDANCE _____</p> <p>CLASSIFIED MATTER PROTECTION & CONTROL _____</p> <p>Control of Classified Matter _____</p> <p>Special Access Programs and Intelligence Information _____</p> <p style="text-align: right;">OVERALL RATING _____</p>	<p>e) CYBER SECURITY</p> <p>CLASSIFIED CYBER SECURITY _____</p> <p>Leadership, Responsibilities and Authorities _____</p> <p>C&A, Risk Management & Planning _____</p> <p>Policy, Guidance and Procedures _____</p> <p>Technical Implementation _____</p> <p>Performance Eval Feedback & Continuous Improvement _____</p> <p>TELECOMMUNICATIONS SECURITY _____</p> <p>UNCLASSIFIED CYBER SECURITY _____</p> <p>Leadership, Responsibilities and Authorities _____</p> <p>C&A Risk Management and Planning _____</p> <p>Policy, Guidance and Procedures _____</p> <p>Technical Implementation _____</p> <p>Performance Eval Feedback & Continuous Improvement _____</p> <p style="text-align: right;">OVERALL RATING _____</p> <p>f) PERSONNEL SECURITY PROGRAM</p> <p>ACCESS AUTHORIZATIONS _____</p> <p>HUMAN RELIABILITY PROGRAM _____</p> <p>CONTROL OF CLASSIFIED VISITS _____</p> <p>SAFEGUARDS AND SECURITY AWARENESS _____</p> <p style="text-align: right;">OVERALL RATING _____</p> <p>g) UNCLASSIFIED VISITS & ASSIGNMENTS BY FOREIGN NATIONALS</p> <p>SPONSOR PROGRAM MANAGEMENT & ADMIN _____</p> <p>COUNTERINTELLIGENCE REQUIREMENTS _____</p> <p>EXPORT CONTROLS/TECH TRANSFER REQUIREMENTS _____</p> <p>SECURITY REQUIREMENTS _____</p> <p>APPROVALS AND REPORTING _____</p> <p style="text-align: right;">OVERALL RATING _____</p> <p>h) NUCLEAR MATERIALS CONTROL & ACCOUNTABILITY</p> <p>PROGRAM ADMINISTRATION _____</p> <p>MATERIAL ACCOUNTABILITY _____</p> <p>MATERIALS CONTROL _____</p> <p style="text-align: right;">OVERALL RATING _____</p>
<p>a) PROGRAM MANAGEMENT AND SUPPORT</p> <p>PROTECTION PROGRAM MANAGEMENT _____</p> <p>Program Management and Administration _____</p> <p>Resources and Budgeting _____</p> <p>Personnel Development and Training _____</p> <p>S&S PLANNING AND PROCEDURES _____</p> <p>MANAGEMENT CONTROL _____</p> <p>Surveys and Self Assessment Programs _____</p> <p>Performance Assurance Program _____</p> <p>Resolution of Findings _____</p> <p>Incident Reporting and Management _____</p> <p>PROGRAM WIDE SUPPORT _____</p> <p>Facility Approval and Registration of Activities _____</p> <p>Foreign Ownership, Control or Influence _____</p> <p>Security Management in Contracting _____</p> <p style="text-align: right;">OVERALL RATING _____</p> <p>b) PROTECTIVE FORCE</p> <p>MANAGEMENT _____</p> <p>TRAINING _____</p> <p>DUTIES _____</p> <p>FACILITIES AND EQUIPMENT _____</p> <p style="text-align: right;">OVERALL RATING _____</p> <p>c) PHYSICAL SECURITY</p> <p>ACCESS CONTROLS _____</p> <p>INTRUSION DETECTION & ASSESSMENT SYSTEMS _____</p> <p>BARRIERS AND DELAY MECHANISMS _____</p> <p>TESTING AND MAINTENANCE _____</p> <p>COMMUNICATIONS _____</p> <p style="text-align: right;">OVERALL RATING _____</p> <p>d) INFORMATION PROTECTION</p> <p>BASIC REQUIREMENTS _____</p> <p>TECHNICAL SURVEILLANCE COUNTERMEASURES _____</p> <p>OPERATIONS SECURITY _____</p> <p>CLASSIFICATION GUIDANCE _____</p> <p>CLASSIFIED MATTER PROTECTION & CONTROL _____</p> <p>Control of Classified Matter _____</p> <p>Special Access Programs and Intelligence Information _____</p> <p style="text-align: right;">OVERALL RATING _____</p>	<p>e) CYBER SECURITY</p> <p>CLASSIFIED CYBER SECURITY _____</p> <p>Leadership, Responsibilities and Authorities _____</p> <p>C&A, Risk Management & Planning _____</p> <p>Policy, Guidance and Procedures _____</p> <p>Technical Implementation _____</p> <p>Performance Eval Feedback & Continuous Improvement _____</p> <p>TELECOMMUNICATIONS SECURITY _____</p> <p>UNCLASSIFIED CYBER SECURITY _____</p> <p>Leadership, Responsibilities and Authorities _____</p> <p>C&A Risk Management and Planning _____</p> <p>Policy, Guidance and Procedures _____</p> <p>Technical Implementation _____</p> <p>Performance Eval Feedback & Continuous Improvement _____</p> <p style="text-align: right;">OVERALL RATING _____</p> <p>f) PERSONNEL SECURITY PROGRAM</p> <p>ACCESS AUTHORIZATIONS _____</p> <p>HUMAN RELIABILITY PROGRAM _____</p> <p>CONTROL OF CLASSIFIED VISITS _____</p> <p>SAFEGUARDS AND SECURITY AWARENESS _____</p> <p style="text-align: right;">OVERALL RATING _____</p> <p>g) UNCLASSIFIED VISITS & ASSIGNMENTS BY FOREIGN NATIONALS</p> <p>SPONSOR PROGRAM MANAGEMENT & ADMIN _____</p> <p>COUNTERINTELLIGENCE REQUIREMENTS _____</p> <p>EXPORT CONTROLS/TECH TRANSFER REQUIREMENTS _____</p> <p>SECURITY REQUIREMENTS _____</p> <p>APPROVALS AND REPORTING _____</p> <p style="text-align: right;">OVERALL RATING _____</p> <p>h) NUCLEAR MATERIALS CONTROL & ACCOUNTABILITY</p> <p>PROGRAM ADMINISTRATION _____</p> <p>MATERIAL ACCOUNTABILITY _____</p> <p>MATERIALS CONTROL _____</p> <p style="text-align: right;">OVERALL RATING _____</p>			
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

5.7 Sample Corrective Action Plan

Finding No: Copied directly from the final inspection report.

Finding: Copied directly from final inspection report.

Root Cause Lead Organization (LO) Subject Matter Experts (SMEs) complete the Root Cause Worksheet (attached) and provide documentation to Facility Security Officer (FSO).

Lead Person: Point-of-contact (POC) provided by LO (usually a member of management from the LO).

Lead Organization: Assigned by FSO (in conjunction with the organization) based on DOE's final report.

Man-Hours Costs (labor, contracts, materials, equipment, etc.): _____
 POC to provide feedback on costs estimated for Closure/Validation of Finding (labor, contracts, materials, equipment, etc).

Summary: LO 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
	<p>The LO (and secondary organizations, if applicable) determines corrective actions, which <i>must</i> address the results of the root cause analysis.</p> <p><i>NOTE: FSO is available to advise the LO's POC/SMEs in composing the milestones and projected completion dates.</i></p> <p>Reasonable projected completion dates are determined based on coordination with all affected organizations.</p>		

SECURITY ANALYSIS CORRECTIVE ACTION PLAN				
Report Number		Title		Finding Number
Finding:				
SA Project Manager Concurrence:				Date:
NSRC Review	N/A	NTS	Non-NTS	Date:
Corrective Action Plan:				
Estimated Completion Date		Date CAP Approved		Date CAP Completed
Responsible Manager's Signature/Date		Auditor's Signature		Verified By/Date

5.8 Sample Root Cause Analysis Form

Finding Number and Description:	Copied directly from DOE final inspection report.
Participants:	Names, titles, organizations.
Date(s):	
Methodology:	How was root cause analysis conducted? What methodology was used?
Results:	<p>Root cause to include contributing factors. Break down in sufficient detail to describe how you came to the root cause.</p> <p>Contributing causes:</p> <p>Root cause:</p>
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).

5.9 Sample Request for Finding Closure/Validation

Audit Title: _____

Finding Number: _____

Finding Narrative: _____

Response Narrative: _____

Status: _____

Compliance Verified By:

DOE Facility Security Officer or SME

Date

Validated By:

DOE S&S Staff

Date

Validation Actions Completed:

