INSPECTORS GUIDE

Classified Matter Protection and Control

SSA

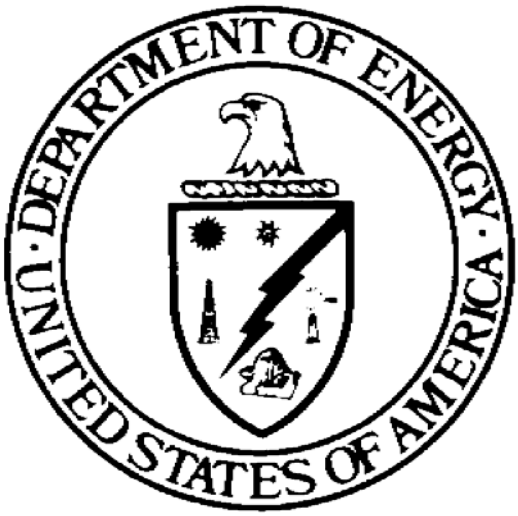
Office of Security and Safety Performance Assurance

Office of Safeguards and Security Evaluations
Office of Independent Oversight and Performance Assurance

September 2005

PROTECTION PROGRAM MANAGEMENT

INSPECTORS GUIDE



February 2006

U.S. Department of Energy
Office of Safeguards and
Security Evaluations
19901 Germantown Road
Germantown, Maryland 20874

Preface

As part of an effort to enhance the appraisal process, the Office of Independent Oversight (SP-40) and the Office of Security Evaluations (SP-41) have prepared a series of documents that collectively provide comprehensive guidance and tools for the evaluation of safeguards and security program effectiveness across the U.S. Department of Energy (DOE) complex. The SP-40 Appraisal Process Protocol describes the philosophy, scope, and general procedures applicable to all independent oversight appraisal activities. The SP-41 Safeguards and Security Appraisal Process Guide describes specific procedures used by SP-41 in planning, conducting, and following up safeguards and security inspections. This Protection Program Management Inspectors Guide, as one in a series of topical inspectors' guides, provides detailed information and tools to assist inspectors assigned to evaluate protection program management in DOE.

Although this inspection guide is designed specifically for the SP-41 inspector, it is made available to the field through the DOE homepage and may be useful to field element and facility contractor personnel who conduct surveys or self-assessments of the protection program management topic.

SP-41 anticipates making periodic revisions to this guide in response to changes in DOE program direction and guidance, insights gained from independent oversight activities, and feedback from customers and constituents. Therefore, users of this process guide are invited to submit comments and recommendations to SP-41.

This page intentionally left blank.

Contents

Contents (Continued)

Acronyms

ACL	Adversary Capabilities List
B&R	Budget and Reporting
BA	Budget Authority
BO	Budget Outlay
CAP	Corrective Action Plan
CD	Critical Decision
CFO	Chief Financial Officer
CMPC	Classified Matter Protection and Control
CPE	Critical Protection Element
COTR	Contracting Officer's Technical Representative
CSO	Cognizant Secretarial Officer
DBT	Design Basis Threat
DOE	U.S. Department of Energy
FV&A	Foreign Visits and Assignments
GPP	General Plant Projects
HRP	Human Reliability Program
ISSM	Integrated Safeguards and Security Management
JCATS	Joint Conflict and Tactical Simulation
JTS	Joint Tactical Simulator
M&O	Management and Operations
MC&A	Material Control and Accountability
NA	Not Applicable
NNSA	National Nuclear Security Administration
OMB	Office of Management and Budget
OPM	Office of Personnel Management
OPSEC	Operations Security
SP-40	Office of Independent Oversight
SP-41	Office of Security Evaluations
PA	Performance Assurance
PPM	Protection Program Management
SNM	Special Nuclear Material
SO	DOE Office of Security
S&S	Safety and Security
SSD	Safeguards and Security Director
SSIMS	Safeguards and Security Information Management System
SSSP	Site Safeguards and Security Plan
TSCM	Technical Surveillance Countermeasures
VA	Vulnerability Assessment
WMD	Weapons of Mass Destruction

This page intentionally left blank.

Section 1

INTRODUCTION

Contents

Purpose

The Classified Matter Protection and Control (CMPC) Inspectors Guide provides guidance, procedures, and inspection tools that enable inspectors to prepare for, conduct, and report the results of an inspection of the CMPC topic. The guide serves to promote consistency and assure thoroughness. Further, it serves to enhance the quality of the inspection process developed by the U.S. Department of Energy (DOE) Office of Independent Oversight and Performance Assurance (OA).

The guide is useful for both the novice and the experienced inspector. For the experienced inspector, the organization of information allows easy reference and serves as a reminder during the conduct of inspection activities. For the novice inspector, the information serves as a valuable training tool. With the aid of an experienced inspector, the novice can use the tools and reference materials for collecting data more efficiently.

Organization

The guide is organized as follows:

- Section 1 – Introduction
- Section 2 – Program Management
- Section 3 – Control of Secret and Confidential Documents
- Section 4 – Control of Top Secret Documents
- Section 5 – Control of Accountable Classified Removable Electronic Media
- Section 6 – Control of Classified Materials
- Section 7 – Special Programs
- Section 8 – Interfaces
- Section 9 – Analyzing Data and Interpreting Results
- Appendix A – Performance Tests
- Appendix B – Forms and Worksheets.

The introductory section (Section 1) provides general guidelines, details on organization of the guide, and explanations of the inspection tools and their use. The section also describes the topic and the methods commonly used for inspecting CMPC. The final part of the section covers the method of identifying and selecting sample sizes and configurations for document reviews and interviews.

Sections 2 through 6 provide detailed guidance for inspecting the CMPC subtopics:

- Section 2, Program Management, includes: Organization and Planning; aspects of the Foreign Ownership, Control, or Influence (FOCI) program, the Security Infraction Program; and the Operations Security (OPSEC) program.

- Section 3, Control of Secret and Confidential Documents, includes: Generation, Review and Use, Accountability, Receipt and Transmittal, Reproduction, Destruction, and Physical Protection and Storage.

- Section 4, Control of Top Secret Documents, includes: Top Secret Classifiers, Top Secret Markings and Forms, Top Secret Control Systems, Receipt and Transmittal, Reproduction, Destruction, and Physical Protection and Storage.

- Section 5, Accountable Classified Removable Electronic Media.

- Section 6, Control of Classified Materials, includes: Marking, Accountability, and Physical Protection and Storage.

- Section 7, Special Programs, includes: Work for Others (WFO), Sensitive Compartmented Information (SCI) and Sensitive Compartmented Information Facilities (SCIFs), Special Access Programs (SAPs), and Communications Security (COMSEC) and Cryptographic (CRYPTO) Materials and Facilities.

- Section 8, Interfaces, contains guidelines for inspectors to aid in coordinating their activities both within the CMPC topic team and with other topic teams. The section provides information on the OA integration process that allows topic team members to align their efforts and benefit from the knowledge and experience of other topic team members. The section provides some of the common areas of interface for the CMPC team and explains how integration contributes to the quality and validity of inspection results.

- Section 9, Analyzing Data and Interpreting Results, contains guidelines on how inspectors organize and analyze information gathered during inspection activities. These guidelines include possible impacts of specific information on other topics or subtopics. They also include experience-based information on the interpretation of potential deficiencies.

- Appendix A, Performance Tests, provides a set of commonly used performance test scenarios, as well as several variations of those scenarios that inspectors may adjust to meet site-specific conditions. Sample performance test plans are also provided.

- Appendix B, Forms and Worksheets, contains forms, lists, and supplemental material frequently useful to inspectors when inspecting the CMPC topic.

General Considerations

The guide contains tools and information that inspectors frequently need. It is designed as a reference manual, for use at the inspector's discretion. Typically, inspectors select the tools that are most useful on an inspection-specific basis. Generally, the guide presents information according to safeguards and security subtopics, so inspectors can easily locate specific subjects. Although the guidelines cover a variety of inspection activities, they do not and cannot address all protection program variations and systems used at DOE facilities. The tools may have to be modified or adapted to meet inspection-specific needs, and sometimes inspectors may have to design new tools or activities to collect information not specifically covered in the guide.

The guide does not repeat word for word the detailed information in DOE orders or manuals. Rather, it is intended to complement the orders and manuals by providing practical guidance for planning the inspection and collecting and analyzing inspection data. One purpose in developing the guide was to capture the collective knowledge of OA's most experienced inspectors. Inspectors should refer to the guide as well as to DOE orders and manuals at all stages of the inspection process.

Every attempt has been made to develop specific guidelines that offer maximum utility to inspectors. In addition to guidelines for collecting information, guidelines are provided for prioritizing and selecting activities, then analyzing and interpreting the results. These guidelines should be viewed as suggestions rather than dogma, and should be interpreted considering inspection-specific and site-specific factors.

Using the Topic-Specific Tools

The CMPC subtopics are further divided into a standard format:

- References
- General Information
- Common Deficiencies/Potential Concerns
- Planning Activities
- Performance Tests
- Data Collection Activities.

References

The references identify DOE orders and sections of DOE manuals that apply to the subtopic. Executive Orders, Site Safeguards and Security Plans (SSSPs), Site Security Plans (SSPs), implementation memoranda, memoranda of agreement, procedural guides, and certain manuals are noted in the References section. Inspectors use the references as the basis for evaluating the inspected program and for assigning findings. It is useful to refer to the applicable orders and manuals during interviews and tours to assure that all relevant information is covered.

General Information

The general information section defines the scope of the subtopic. It includes background information, guidelines, and commonly used terms intended to help inspectors focus on the unique features and problems associated with the subtopic. It identifies the different approaches that a facility might use to accomplish an objective and, when possible, provides typical examples.

Common Deficiencies/ Potential Concerns

This section discusses common deficiencies and concerns that OA has noted on previous inspections. The information in this section is intended to help the inspector further focus inspection activities. By reviewing the list of common deficiencies and potential concerns prior to gathering data, inspectors can be alert for these elements at the inspected facility during interviews, tours, and other data-gathering activities. Also, where appropriate, general guidelines are provided to help the inspector identify site-specific factors that may show whether a particular deficiency is likely to be present.

Planning Activities

This section identifies activities normally conducted during inspection planning. These activities include document reviews and interviews with the facility physical security systems managers. The detailed information in the planning activities section is intended to help ensure systematic data collection, and ensure that critical elements are not overlooked. The thoroughness of planning has a direct impact on the success of the inspection.

Performance Tests

General guidelines are provided to help the inspector identify site-specific factors that may

indicate which performance tests may be particularly important. Appendix A provides a set of commonly used performance test scenarios that may be used directly or modified to address site-specific conditions. The tests may provide information useful in evaluating other CMPC subtopics. For example, during the back check performance tests on accountable documents, inspectors typically gather information relevant to the accountability system, physical protection, document generation, and document reproduction.

Data Collection Activities

This section identifies activities that inspectors may choose to perform during data collection. The information is intended to be reasonably comprehensive, although it is recognized that it will not address every conceivable variation. Typically, these activities are organized by functional element or by the type of system used to provide protection. Activities include tours, interviews, observations, and performance tests.

Inspectors do not normally perform every activity on every inspection. Specific activities and performance tests are normally selected during the inspection planning phase. The activities are those that are most often conducted and reflect as much OA data collection experience and expertise as possible. Also, they are identified by alphabetical letter for easy reference.

Using the Tools in Each Inspection Phase

The inspection tools are intended to be useful during all phases of the inspection, including planning, conduct of the inspection, and closure. The following summarizes the use of the inspection tools at each phase:

In the **planning phase**, inspectors:

- Use the General Information section under each subtopic to characterize the program and focus the review.
- Perform the activities identified under Planning Activities to gather the information necessary to further characterize the program and focus the review.
- Review Common Deficiencies/Potential Concerns to determine whether any of the deficiencies are apparent and to identify site-specific features that may indicate that more emphasis should be placed on selected activities.
- Assign specific tasks to individual inspectors (or small teams of inspectors) by selecting performance tests and specific items from the Data Collection Activities section. The assignments should be made to optimize efficiency and to ensure that all high-priority activities are accomplished.
- Consider the guidelines provided in Section 8 (Interfaces) to ensure that efforts are not duplicated.
- Review Section 9 (Analyzing Data and Interpreting Results) after completing planning activities to aid in evaluation and analysis of the data and to determine whether additional planning data is needed to evaluate the program.
- Prioritize and schedule data collection activities to optimize efficiency and to ensure that high-priority activities are conducted early in the process. A careful prioritization of these activities provides the opportunity to determine whether the available personnel resources and inspection time periods are sufficient to evaluate the inspected topic adequately.
- Review the applicable policy supplements to ensure that they are current with all applicable policy revisions, updates, and clarifications.

In the **conduct phase**, inspectors:

- Use the detailed information in the Data Collection Activities section to guide interviews and tours. Inspectors may choose to make notes directly on photocopies of the applicable sections.

- Review Common Deficiencies/Potential Concerns after completing each data collection activity to determine whether any of the identified deficiencies are apparent at the facility. If so, inspectors should then determine whether subsequent activities should be reprioritized.

- Review Section 9 (Analyzing Data and Interpreting Results) after completing each data collection activity to aid in evaluation and analysis of the data and to determine whether additional data are needed to evaluate the program. If additional activities are needed, inspectors should then determine whether subsequent activities should be re-prioritized.

In the **closure phase**, inspectors:

- Use the Analyzing Data and Interpreting Results section to help analyze the collected data and identify the impacts of identified deficiencies. This will aid in determining the significance of findings, if any, and assist inspectors in writing the analysis section of the inspection report.

Validation

Validation is the process of confirming with site representatives the accuracy of the information that OA inspectors have gathered. Whenever possible, inspectors should confine validation to facts, not conclusions. However, site representatives should also understand the potential impact of the facts that are validated. The OA validation procedure, discussed in detail in the OA Appraisal Process Protocols, includes on-the-spot validations, daily validations, and summary validations. On-the-spot validations confirm data at the time of collection; they are particularly important during performance testing, because several people may be present and they are often difficult to reassemble for the daily and summary validations. Daily validations normally take place at the end of each day during the data collection phase of the inspection. Team members must keep records of the information covered in on-the-spot and daily validations for reference during the summary validation.

Characterization of the Classified Matter Protection and Control Topic

Sensitive information, both tangible and intangible, must be protected from unauthorized disclosure, which might adversely impact national security. The DOE, to fulfill its mission to protect such information, has established formal requirements for the CMPC program in orders and other official communications.

In the past, DOE required strict accountability controls and records for the CMPC program. In February 1991, the Department decided that strict accountability was no longer required for most classified documents. DOE developed a formal process for adopting modified accountability procedures for classified matter. As DOE organizations adopted these procedures, the OA inspection focus for CMPC changed from close attention to accountability records and front check performance tests to emphasis on physical protection of classified matter, access control, and need-to-know. OA's current approach to the CMPC topic retains many aspects of past inspection methodologies for the control of classified documents and material; for example, marking of matter, user and custodian knowledge, FOCI determinations, destruction, reproduction, control of Top Secret documents, and special access programs.

The CMPC topic is made up of several subtopics and special programs. This division facilitates program management and is used by DOE to communicate policy and guidance, and by OA to organize inspection activities. One or more of

these subtopics or special programs are included whenever OA inspects CMPC. The determination as to which subtopics or special programs will be inspected is based on various factors, including: the facility's mission, facility CMPC program documentation, discussions with program managers, and results of previous reviews at the facility.

The CMPC topic team uses five basic methods of data collection: document reviews, observation, interviews, knowledge tests, and performance tests.

Document Reviews

All CMPC programs rely on detailed documentation to ensure that the facility program is properly administered and effective in safeguarding sensitive information. The lack of well-developed and comprehensive policies and procedures is often the first sign of an ineffective CMPC program. Reviewing documentation therefore serves three purposes: 1) it determines whether written policies and procedures are consistent with DOE requirements, 2) it provides inspection team members with a baseline picture of the way the program operates at the site to be inspected, and 3) it may reveal weaknesses in policies or procedures that need to be further explored using other data collection tools and techniques.

All required documents from the site being inspected may not be available during the planning meeting. The team may request that certain information be made available by the site and ready for team use at the beginning of inspection conduct. Reviewing documentation continues throughout the inspection data collection phase. Often, the inspector must request additional documents during the data-gathering phase to develop a complete picture of the facility CMPC program and how it functions. Requests for additional documentation should be made to the facility topic point of contact. If difficulties are encountered in obtaining required information, then a follow-up request should be made by the OA Inspection Chief directly to facility or operations management.

Documents of interest (see Appendix B) usually consist of two categories: 1) policy documents, which provide information on how the CMPC program is supposed to function; and 2) records, which indicate whether the facility program is complying with requirements. Policy documents normally include, but are not limited to, plans, policies, and procedural guides. Records of interest can include such items as administrative records, document control records, classified material (parts) inventory records, records indicating completion of required reviews or actions, training records, security infraction reports, OPSEC assessments, FOCI approvals, and technical surveillance countermeasures (TSCM) equipment records.

Observation

Observation allows inspectors to see how site personnel actually do their jobs, and inspectors can evaluate them under normal, non-staged, non-controlled conditions. This provides the best data on whether they follow established procedures and properly operate the equipment for which they are responsible.

Ideally, observations should be made at as many key points in the CMPC program as practical. Not all observations need be scheduled inspection activities. Observing security personnel at work is an opportunity for adding to the data points being gathered or helping to validate data already collected.

Although observation of personnel actually performing their duties would seem an ideal inspection tool, it is not a simple process:

- First, a conscious decision must be made by topic team members concerning the amount of time that can be allocated for observation: Will an hour spent watching a specific task yield an hour's worth of usable data? In many instances, the answer is "no," since not all

activities associated with the CMPC program occur on any predictable schedule (for example, the receipt of classified documents).

- Second, the mere presence of an inspector may influence behavior and produce erroneous data.

- Third, the results of observations, frequently being subjective, may be hard to validate. This can lead to disagreement between the inspection team and facility personnel on what was actually observed.

For these reasons, observations either are generally confined to certain CMPC duties that occur on a routine basis, or are used to round out the inspection team's overall picture of the site's CMPC program and for evaluating performance in specific areas.

Interviews

Interviews are an excellent way to collect a variety of information. Interviews actually begin during the planning phase, when inspectors ask personnel and points of contact to provide information about all aspects of the CMPC program. Interviews continue during the inspection conduct and provide an important source of information about the program.

Virtually any person associated with the program is a potential interview candidate. Although interviews can be used to round out the inspector's knowledge, their more important function is to help determine an individual's knowledge and understanding of policies, procedures, and duties.

Both formal and informal interview techniques are employed by OA. Topic teams prepare a series of formal questions based on their initial review of facility documents during the planning phase. These questions are normally organized and presented to the site representatives assigned as points of contact during the planning phase.

Usually the facility points of contact can provide immediate answers to many of the questions during the planning meeting. When a question cannot be answered immediately, the site representative is expected to address the question during the interval between the planning meeting and the beginning of onsite data collection, and to provide answers either during this interval or when the inspection team arrives on site.

Informal questions are those that arise out of the interaction between inspection team members and site personnel. Whether information is obtained through a scheduled interview or an incidental conversation, inspectors should be attentive and follow up on items of interest as they arise. For example, a comment made by a document custodian during the inspection may suggest a lack of understanding or a program weakness. The inspector should be prepared to follow up the comment with additional questions.

Since important issues may arise by chance, inspection team members should be cautious about questioning site personnel in the absence of an assigned point of contact. Information obtained when a point of contact is not present may prove difficult to validate. By the same token, inspectors should be wary of attempts by points of contact to coach or otherwise influence the individuals being interviewed.

Knowledge Tests

Job knowledge is an essential element of any CMPC program. The key to a successful program is how well personnel know and perform their duties. Job knowledge is normally assessed more quickly by interviewing CMPC personnel during the inspection.

There is a certain body of knowledge, some Departmental and some site-specific, that people associated with CMPC must have. Knowledge tests are a means of determining whether personnel possess this knowledge. Inspectors use a variety of tests, including oral, written, or a

combination of the two. OA uses interactive video technology for some topics.

When formal knowledge tests are given, a representative sample of the available test population should be tested. Questions and answers should be carefully validated with representatives of the inspected operations office or facility before the test is administered. Inspectors should understand that knowledge tests indicate only whether a person knows certain policies and methods, not whether he or she can apply that knowledge or perform a related duty.

Performance Tests

Performance testing is one of the most valuable data collection methods used to inspect a CMPC program. Performance testing can determine whether personnel have the skills and abilities to perform their duties, whether procedures work, and whether equipment is functional and appropriate. A performance test is a test in which elements of the program, whether they be personnel, procedures, or equipment, actually perform what is required of them.

Virtually any skill, duty, procedure, or item of equipment can be performance tested. Performance tests may vary in complexity from the simple duplication of a classified document to more complicated and elaborate tests involving the integration of multiple topic interests. The necessity for integrated performance testing has increased since the beginning of modified accountability. Some tests can be conducted under completely normal conditions, where the subject is unaware of the testing. Other tests must be conducted under artificial conditions, although maximum realism is always a primary planning consideration. OA has established formal protocols for planning and conducting certain performance tests, including safety procedures and other requirements.

The actual conduct of each performance test is the most important part of the performance testing process. However, before conducting any performance test, final coordination of all test activities should be made with the site representatives. Test participants should be briefed in detail about the actions that will be expected of them. Topic team members responsible for a given performance test should exercise careful control of all activities for the duration of the test, and test results should be informally validated as soon as possible after the test is concluded.

A performance test plan format has been developed that provides a convenient way to describe proposed tests in planning documents, and also serves as a quick reference for inspectors during the actual conduct of the test. Sample performance test plans are included in Appendix A. The format is flexible and may be adapted to fit test application requirements at varying levels of complexity. The most complex format contains the following sections:

- Objective – Identifies the parts of the CMPC program the test is to measure and briefly describes what the test is designed to accomplish.

- System Description – Provides a succinct description of the system. This helps team members understand system parameters and serves as a quick refresher they can review immediately before beginning the test.

- Sampling Technique – Explains how the sample to be tested will be selected and handled. It also serves as a record of these actions for future reference.

- Scenario – Describes how the performance test will be conducted. The test scenario may include specific points that must be covered to serve as a reminder to personnel performing the test. Frequently, for less complex performance test applications, system descriptions and sampling techniques are discussed under this heading instead of under separate sections.

- Evaluation Criteria – Provides the applicable references used to determine whether the facility is meeting requirements.

- Safety Plan – Requires a detailed safety plan if the performance test has safety implications. Normally CMPC performance tests do not impact safety, and consequently, this requirement would not apply.

Although this format has been provided, it should not be considered mandatory. Inspectors may modify it to meet their requirements. Whatever format is used, it should provide sufficient detail for planning and conducting the test and to serve as an historical record of what was accomplished.

Inspection Goal

The inspection goal is to determine whether the CMPC program is adequately protecting the sensitive information entrusted to DOE and to report the results. To achieve this goal, the topic team must determine the current status of a facility's CMPC program and develop a comprehensive understanding of how the program functions. Such understanding allows a detailed analysis of the system and permits assessment of how well the system can meet protection requirements.

Identifying and Selecting Sample Size and Configuration

Sample size and configuration are important planning elements that must be determined for many data collection activities. It is normally impractical to review every document in an accountability system or interview every custodian. Inspectors must therefore examine a sample of the population applicable to each data collection event and extrapolate the results to form conclusions about the entire population under review. A detailed description of a sampling methodology is included in Appendix B, Forms and Worksheets.

It is important that the samples tested be large enough to provide a reasonable indication of the entire population under review. Similarly, it is just as important that the sample being tested is representative of the total population and of the system involved. The sample to be tested must have qualifications or conditions in common.

Planning for each data collection activity should include a determination of how many items will be tested (reviewed, examined), and how they will be selected. When possible, it is usually best to identify the sample before arrival at the facility, although in certain tests the identity of the samples themselves cannot be provided to the facility in order to maintain objectivity of the performance test. See Appendix B for an expanded discussion of sampling.

Integrated Safeguards and Security Management

The Department is committed to conducting work efficiently and securely. DOE Policy 470.1, *Integrated Safeguards and Security Management (ISSM) Policy*, is designed to formalize a framework that encompasses all levels of activities and documentation related to ISSM.

The framework is made up of seven components to facilitate the orderly development and implementation of ISSM. Included in the components is the objective of ISSM, guiding principles and core functions.

The seven guiding principles of ISSM are:

- Individual responsibility and participation

- Line management responsibility for safeguards and security

- Clear roles and responsibilities

- Competence commensurate with responsibilities

- Balanced priorities

- Identification of safeguards and security standards and requirements

- Tailoring of protection strategies to work being performed.

The five core functions of ISSM are:

- Define the scope of work.
- Analyze the risk.
- Develop and implement security measures.
- Perform work within measures and controls.
- Provide feedback and continuous improvement.

For the purposes of this CMPC Inspectors Guide, OA has established four general categories that encompass the concepts embodied in the guiding principles and core functions of ISSM:

Line Management Responsibility for Safeguards and Security. This category encompasses the corresponding ISSM guiding principles that relate to management responsibilities (i.e., line management responsibility for protection of DOE assets, clear roles and responsibilities, and balanced priorities).

Personnel Competence and Training. This category encompasses the ISSM guiding principle related to competence of personnel (i.e., competence commensurate with responsibilities). It also encompasses DOE requirements related to ensuring that personnel performing safeguards and security duties are properly trained and qualified, and the need for sufficient training/certification requirements and an appropriate skill mix.

Comprehensive Requirements. This category encompasses the corresponding ISSM guiding principles and core functions that relate to policies, requirements, and implementation of requirements (i.e., identifying safeguards and security standards and requirements, tailoring protection measures to security interests and programmatic activities, providing operations authorization, defining work, analyzing vulnerabilities, identifying and implementing controls, and performing work within controls).

Feedback and Improvement. This category encompasses the corresponding ISSM core function (i.e., feedback and improvement) and DOE requirements related to DOE/NNSA line management oversight and contractor self-assessments.

It is important to note that the categories above are only used to organize information in a way that will help inspectors gather data about management performance in a structured and consistent manner. OA has identified general categories of information that would be expected in an integrated ISSM program.

Section 2

PROGRAM MANAGEMENT

Contents

This section addresses elements of program management as they apply to the CMPC program. The organization and planning element encompasses the traditional aspects of management, including developing goals, objectives, and responsibilities; developing and implementing procedures; providing adequate resources to meet program requirements; performing management oversight activities; monitoring the status of programs and policy implementation; and ensuring that corrective actions are implemented in a timely and efficient manner. The FOCI element addresses measures that must be taken to protect against any undue risk that may result when contractors or subcontractors that are controlled or influenced by foreign governments, organizations, or individuals are allowed access to classified information. The Security Infraction Program element encompasses all aspects of security infraction programs, including detecting, investigating, and reporting infractions. All organizations that deal with classified matter in any form are required to have a security infraction program. Lastly, the OPSEC program element addresses the protection of sensitive information. In addition to providing general information, this section discusses the common deficiencies/potential concerns, planning activities, performance tests (if applicable), and data collection activities associated with each element.

This page intentionally left blank.

Section 2.1

Organization and Planning

Contents

References

DOE Order 470.1, Chapters I, II, III and X
DOE Order 471.2A, Chapters I, IV, V, and Attachment 1
DOE Order 430.1B
DOE Manual 471.2-1B
DOE Manual 475.1.1A
DOE Manual 471.2-1C
DOE Manual 452.4-1A
DOE Manual 473.1-1
DOE Manual 471.2-4
DOE Order 473.1

General Information

The organization and planning element of the Program Management subtopic encompasses the traditional aspects of management as they apply to the CMPC program. Successful CMPC programs achieve and maintain full compliance with all aspects of DOE CMPC policy. Management has the responsibility to ensure that this goal is met. In order to meet this responsibility, management performs a number of activities, including:

- Developing plans that include goals, objectives, and responsibilities for every aspect of the CMPC program
- Developing and implementing procedures and policies, considering site-specific conditions, that fulfill DOE requirements
- Providing adequate resources, including personnel (plus training), equipment, and facilities, to meet the requirements contained in the procedures and policies
- Defining organizational and individual responsibilities (including accountability for performance)
- Performing management oversight activities, such as self-assessments, to identify areas that do not meet DOE policy requirements
- Monitoring the status of programs and policy implementation
- Correcting all areas of non-compliance in a timely and efficient manner.

Organization and planning make up one of the most important components of a facility's CMPC program. This is true because organization and planning form the basis for the success or failure of the program. Significant deficiencies in these important areas usually indicate that one or more elements of the CMPC program is deficient.

Usually, OA inspects each major organization that holds classified matter at a site. In some cases, OA reports and rates the results for the local DOE operations office and prime operating contractor separately. If additional prime contractors (for example, the protective force contractor) are present on site, the status of their programs is also reported and rated separately. The program management subtopic is not normally assigned a separate rating, nor is management evaluated as adequate or inadequate. Rather, the results of the review of the facility's CMPC management are considered along with all other CMPC inspection results, and a single rating is assigned to each organization.

The CMPC programs at DOE facilities range from very large to very small. Large programs often have thousands or millions of items of classified matter that are used by hundreds or thousands of individuals. A small program might have only one or two document accounts, very few documents on hand, and very few users. A corresponding variety is found in the management systems. Very small programs typically do not have extensive management documentation (such as written program plans or formal training programs), and the responsibilities for CMPC functions tend to be concentrated in a few individuals. Large CMPC programs generally have more complex management systems. In most moderate to large programs, security responsibilities are decentralized. Frequently, the security department is responsible for issuing security policies and providing technical advice and oversight, and the operating or production departments are responsible for implementing most CMPC functions. In very large programs, the security department frequently has a number of specialists, each with separate areas of responsibility.

The CMPC topic team should dedicate adequate resources to inspect each organization's CMPC management program. A good rule of thumb is that it will take one person one or two days to review management for each program being inspected and rated (the actual time required depends on the size and complexity of the inspected program). The team may want to schedule the review of management for the latter part of the onsite visit so they can focus on the management problems identified during earlier stages of the inspection; for example, Wednesday and Thursday if data is to be gathered during a one-week period.

Interviews with various managers make up one of the most important methods of gathering information about CMPC. Consequently, inspectors can gather much of the information discussed in the data collection activities sections by interviewing key managers. Experience has shown that an efficient way to organize the inspection interviews is to start with the persons who have immediate supervisory authority for the various aspects of the CMPC program. In very large programs with numerous first-line supervisors, it may be necessary to select a representative sample to interview. Inspectors should then interview individuals at successively higher management levels, up to and including the manager with overall responsibility for the safeguards and security program. Managers in the operations and production departments should also be interviewed, since most of the responsibility for implementing classified document control procedures rests with the line organizations. In some cases, based on information learned from interviews and other inspection activities, it may be desirable to interview managers at levels above the overall safeguards and security managers as well. An organized interview schedule, in which the inspectors cover a variety of subjects with each manager, is essential for maximizing the efficiency of the data collection process and minimizing the impact on facility managers.

Common Deficiencies/ Potential Concerns

Line Management Responsibility for Safeguards and Security

Insufficient Management Support or Oversight. Frequently, DOE and facility operations and production managers place a high priority on meeting production or operational goals, and are reluctant to implement security measures that are inconvenient or that would impact production. While such reluctance is understandable, compliance with the minimum requirements of DOE orders must be met, and an appropriate balance between security and operations and production must be maintained. Without the support of senior managers, the security organization may be unable to adequately enforce DOE orders, resulting in a failure to implement required security measures. Additionally, a lack of support may result in security programs that do not have sufficient resources to operate effectively. It is incumbent on senior managers and personnel responsible for oversight activities to assure that a lack of management support does not adversely impact the effectiveness of security programs.

Lack of a Suitable Organizational Structure. Occasionally, inspectors encounter an organizational structure where the person or group responsible for CMPC policy and procedures is not positioned high enough in the organization to ensure compliance. This problem often occurs when one organizational element is responsible for policy, but the document custodians and other persons who actually implement the policy work for different elements. The situation gets worse when the management element common to the two groups is at too high an organizational level to deal with day-to-day issues effectively. Similarly, inspectors may encounter situations where the security organization has little control or influence over the CMPC activities of the operations and production personnel. In such cases, the operations and production managers may place low priority on security issues and, in extreme cases, simply ignore the security organization's policies or procedures.

Responsibilities Not Specifically Assigned. Frequently, facilities fail to document the organizations and persons responsible for various aspects of the CMPC program. Less commonly, they may fail to assign responsibility for some aspects of the program at all. Not documenting responsibility assignments inevitably results in some aspects of the CMPC program "falling through the cracks." Responsibility for every aspect of the program should be specifically assigned in writing first to an organization, and then to a specific position or person within that group.

Headquarters Guidance and Directives Not Distributed to Working Level. DOE Headquarters and NNSA have issued a large number of memos and policy directives clarifying and modifying various aspects of CMPC. This information is sent to the local DOE operations offices, and they are supposed to forward them to the appropriate contractor managers. The contractor managers are required to implement the applicable directives or verify that their programs are in compliance with policies as clarified. For this process to be effective, responsible individuals must distribute the relevant information to the working level in a timely manner. Also, the written procedures must be updated to incorporate the new guidance. Frequently, the flow of information is interrupted at some point before it gets to the working level, so the information may not be implemented and incorporated into written procedures. These interruptions in policy flow are often more frequent when the documents to be protected are compartmented or under special access limitations. This is a common problem at all DOE and contractor organization, regardless of size.

Personnel Competence and Training

Inadequate Training for Classified Matter Custodians and Key Personnel. Many significant CMPC-related deficiencies found in DOE are attributable to inadequate training. Some organizations do not provide any formal training. They rely instead on an unstructured form of on-the-job training. They expect persons with classified matter responsibilities to learn from other, more experienced individuals. Often, however, the experienced individuals themselves lack adequate training, so improper practices continue. In some cases, organizations make attempts at training, but develop and administer it using individuals unfamiliar with proper training techniques. This practice also results in inadequately trained persons performing key duties. Few organizations evaluate the competence of individuals with classified matter responsibilities before allowing them to assume their assigned tasks. Even people who have completed a well-designed training program may not have adequately learned all aspects of their duties. Many facilities rely solely on general awareness training, which frequently is not specific enough or designed to cover details required for classified custodians. If a training program exists, inspectors should focus on reviewing its effectiveness. If no training program exists, inspectors should devote additional attention to activities designed to determine the knowledge level of individuals who perform CMPC functions (for example, interviews or knowledge tests).

Inadequate Staffing. Some facilities simply do not have enough staff to accomplish CMPC functions. A related problem occurs when a facility's CMPC managers cannot effectively manage the program, either because they supervise too many people (excessive span of control), or because they have other duties that deflect their attention from their document protection responsibilities.

Comprehensive Requirements

Inconsistency in CMPC Procedures and Practices. This problem is prevalent in organizations with decentralized responsibility for CMPC, or where the authority of the central CMPC group is weak. Lower-level organizations may develop their own procedures and practices. Even where organization-wide procedures exist, inspectors may find inconsistencies in the way organizational elements implement procedures. Different procedures within an organization are not in themselves a problem but may increase the potential for deficiencies. When inspecting organizations with several lower-level elements that develop separate procedures, inspectors should pay particular attention to determine whether they are consistent and follow DOE policy. This is also true of organizations that do not have a strong central program element to ensure consistent compliance with organization-wide procedures.

Lack of Documented Assessments. Frequently, sites possessing large quantities of classified parts, such as weapons components, will often store these parts in DOE-defined "non-standard" open storage. Open storage is considered non-standard when the storage location (i.e., the storage building) is not fully equipped with both perimeter and interior alarm sensors, and therefore not considered a vault or vault-type room. For such storage to be used, the site must first have implemented compensatory measures that include protective force patrols that are sufficient to prevent adversaries from successfully accessing and removing the parts, and that must be based on documented, approved assessments that consider the time needed to remove the parts, the parts' value, and the consequences to national security of the parts' removal. Most often, such assessments have either not been conducted, have not been conducted for <u>all</u> locations on non-standard storage, or have been completed using inappropriate assumptions, resulting in inadequate protection for the parts.

Feedback and Improvement

Inadequate Self-Assessment Process. Not all facilities have implemented a comprehensive self-assessment program. Others lack the expertise to implement such a program effectively. Therefore, they rely on periodic security surveys to provide data for self-assessment of the local CMPC program. The lack of an effective self-assessment program can result in deficiencies going undetected and uncorrected for extended periods.

Inadequate Corrective Action Plans. This is also a very common and potentially serious deficiency that can result in deficiencies not being corrected. Organizations frequently fail to effectively accomplish one or more of the following actions: (1) analyze (root cause and cost effectiveness) and prioritize deficiencies so that resources can be used to correct the most serious first, (2) establish a corrective action schedule with milestones so progress can be monitored and slippages identified early, (3) assign responsibility for completion to specific organizations and individuals, (4) continually update the plan as known deficiencies are corrected and new ones are identified, and (5) ensure that adequate resources are applied to correcting deficiencies. Frequently, facility managers devote their resources to "putting out brush fires" (that is, correcting the most recently identified deficiency instead of the most serious, and habitually correcting symptoms rather than the root causes of systemic deficiencies).

Incomplete or Inadequate Deficiency Tracking Systems. Tracking system inadequacy is a common and potentially serious deficiency often found in the management area. Problems in the tracking system can result in not correcting deficiencies in a timely manner, or not correcting them at all. The two most common problems found in tracking systems are incompleteness and inaccuracy. Often, the system is incomplete because supervisors or operators fail to list all deficiencies. They are inaccurate when corrective actions are shown as complete when they are not, or the problem has not been dealt with adequately. Occasionally, inappropriate corrective action based on inaccurate tracking data creates new problems.

No Root Cause Analysis of Deficiencies. Another common and potentially serious management deficiency is the failure of organizations to determine the underlying cause of deficiencies. This usually results in the same deficiencies recurring. Many times, the organization corrects the surface problem or symptom rather than identifying and correcting the underlying cause—the root cause. For example, if an inspection or self-assessment identifies widespread and significant marking errors on classified documents, merely instituting a program to re-mark all existing documents would not necessarily solve the problem. If performed correctly, a root cause analysis may reveal that persons generating classified documents are not familiar enough with marking requirements and require training. In this example, a complete corrective action plan would include actions to correct the markings plus provide the necessary training. Unless management accurately determines the root cause of identified deficiencies, it is likely that similar deficiencies will recur.

Planning Activities

During the planning meeting, inspectors interview points of contact and review available documentation (for example, SSSP, CMPC procedures, self-assessments, survey reports, and other pertinent documents) to characterize the program. Inspectors should:

- Determine the CMPC program organizational structure, including whether a central group establishes and monitors compliance with procedures. If not, determine how many separate points of authority for the program exist among the various organizational elements with CMPC interests.

- Review organizational charts and determine the names of all persons with CMPC supervisory and management authority.

- Determine how CMPC policy and procedures are promulgated and distributed.

- Determine how the self-assessment program functions, including the frequency of self-assessments, who has overall authority for the program, and who actually performs the self-assessments. Focus on determining whether the self-assessment program provides independent oversight of all classified matter (including CMPC interests in SCIFs, SAPs and classified WFO programs), or whether it is conducted by the same persons who operate the programs being assessed.

Appendix B contains a list of generic documents that should be reviewed during the planning and conduct phases of the inspection. This list should be tailored to the CMPC program of the site and the DOE field element.

Once inspectors understand the structure of the CMPC management program, they should determine which organizations and program elements will be reviewed in more depth and which individuals will be interviewed. At large facilities, it is not practical to inspect all organizations in the same depth or to interview all individuals who perform document protection duties. In such cases, a representative sample may be selected for evaluation. Typically, inspectors will be covering other CMPC subtopics as well as the program management subtopic for reasons of efficiency. Consequently, a variety of factors should be considered when selecting organizations to review. It is usually advisable to interview first-line managers with responsibility for the same accounts as custodians selected for document accountability performance tests. This ensures that the impact of any deficiencies identified during the reviews can be covered with managers during the management interviews. Frequently, the information gathered during the first few days of the inspection will influence the selection of managers to be interviewed. As program strengths and weaknesses are noted, the inspectors should modify their planned activities appropriately.

Performance Tests

Performance tests are not normally conducted specifically to evaluate the organization and planning element. However, the results of performance tests in other CMPC inspection areas should be considered because strengths and weaknesses in the implementation of the program are often attributable to management issues. The performance test results should serve as a starting point for examining how management handles the CMPC program and for determining, whenever possible, the root causes for identified deficiencies.

Data Collection Activities

Line Management Responsibility for Safeguards and Security

A. Inspectors should review the applicable planning documents that cover the CMPC program (for example, SSSPs or other planning documents). Inspectors should devote particular attention to determining whether the planning documents are current; whether they appropriately identify the goals, objectives, responsibilities, and overall policies for all aspects of their organization's CMPC program; and whether they address all applicable security interests. Any special conditions or unique features of the site that are covered by exceptions or alternative approaches should be reviewed to determine whether the facility has documented the justification for the exceptions.

B. Inspectors should interview security managers, including the CMPC manager and the Special Security Officer (at an SCIF), and review resource plans and budget documents. Elements to cover include:

- Whether goals and objectives are clearly defined

- Whether needs identified in the corrective action plan and strategic plan (if one exists) are reflected in budget documents

- How the CMPC program budgeting process functions

- Whether there is consistency between staffing plans and budget requests.

C. Inspectors should determine whether the organizational structure facilitates efficient communication and positive working relationships between the various organizational elements, and between persons who deal with classified matter. It is important that the functional relationships between the CMPC program group and the various other organizational elements that have classified matter be clearly defined, formally documented, communicated, and understood by all persons who are in a position to work with classified matter, or who manage those that do. One method useful for investigating the adequacy of the communications and interactions between organizational elements is to determine how the CMPC organization interacts with other organizations (for example, protective force and physical security) when facility conditions change (for example, when a new repository is put in use). In this case, inspectors could review records to determine when a repository was put in use, when the physical security group was informed of the possible need for additional alarm sensors, when protective force management was informed of the new repository, and when the protective force supervisors began to implement the required repository checks and patrols.

D. Inspectors should determine whether the persons responsible for the CMPC program are in a position to ensure compliance. This may involve reviewing the facility's policies and procedures to determine whether the safeguards and security manager has the authority to enforce compliance and resolve issues identified during self-assessments or other similar activities. Additionally, managers in the security department and operations and production departments should be interviewed to determine whether the security organization has any problems getting the operations or production personnel to implement required procedures. If initial interviews indicate questions about the operations or production organization's commitment to implementing required security measures, inspectors may elect to conduct more detailed interviews (i.e., with individual managers) and document reviews to determine whether problems exist. This detailed review may involve examining findings identified in self-assessments, surveys, and inspections to determine whether corrective actions were implemented in a timely manner, or whether repeated memoranda from the security organization were necessary before the operations or production personnel took action. Other indicators of problems include a pattern of repeated deficiencies at the same location and "backsliding" (that is, implementing corrective actions after a deficiency is identified, and then discontinuing the corrective measures later, after the "heat is off").

E. Inspectors should determine how management communicates its goals and objectives and stresses the importance of CMPC. Inspectors should determine what incentives are used to encourage good performance and what programs are used to maintain an appropriate level of security awareness.

F. Inspectors may elect to review a sample of position descriptions of specific individuals who have responsibilities for the CMPC program to verify that responsibilities are actually reflected at the individual's level. Inspectors can also review individual position descriptions and performance goals of custodians or other persons in the operations and production departments that use or generate classified documents to determine whether individuals are held accountable for their performance in the CMPC program and whether good performance in CMPC-related areas is included.

G. Inspectors should review actual versus authorized staffing levels for CMPC positions to determine whether the program is operating short-handed. Inspectors must be especially watchful for non-CMPC responsibilities being assigned to key program personnel, detracting from their ability to perform their CMPC duties.

Personnel Competence and Training

H. Training for the personnel who generate, use, and maintain control systems for classified matter is the most important aspect of human resources. Experience has shown that most deficiencies identified during past OA CMPC inspections can be attributed to inadequate or non-existent training programs. Inspectors should interview security managers responsible for the facility's training programs to determine whether the programs are complete and effective. Aspects to cover include whether the training programs are formal, are based on needs and job task analyses, have written lesson plans, and mandate that tests certifying competence be given to custodians and other persons with key roles in working with classified matter. Training for users is equally important. Further, inspectors should examine the site programs for ensuring the appropriate level of general security awareness, as well as CMPC awareness.

I. If a formal program is in place, the inspectors may elect to review a sample of training records or certifications to verify that personnel receive the training. If possible, inspectors should attend a training session to determine whether the training covers relevant information and is appropriately tailored to the needs of the audience.

J. Inspectors should interview selected operations and production managers, custodians, and users to determine their level of satisfaction with the available training programs. Elements to cover include whether the training programs are relevant to the needs of the users and whether enough classes are offered to provide training to persons who require it, or whether there are long waiting lists. Inspectors should determine whether the security organization has been responsive to requests by operations and production managers for more training (or for changes in training programs). If operations and production personnel indicate dissatisfaction with the quality or availability of training, inspectors should follow up those concerns with security managers to gather their views. In some cases, inspectors may find that the security managers are not able to offer more training classes because of lack of resources or qualified training staff.

Comprehensive Requirements

K. Inspectors should review selected procedures for compliance with DOE policy, including whether they incorporate the most current DOE Headquarters guidance memos. Inspectors should check to ensure that procedures are current with the present organizational and site configuration. Where individual organizational elements have their own procedures, inspectors should review procedures of a variety of these elements, paying particular attention to determining whether each element's procedures accurately reflect site policies and DOE orders.

L. Inspectors should interview security managers to determine how the facility updates and distributes procedures to personnel who must implement them. In conjunction with the review of the other CMPC elements (for example, generation and destruction), inspectors should interview selected personnel who perform CMPC functions to determine how procedures are issued to them and how they are informed about revisions and updates. Inspectors should determine whether procedures (including updates and revisions) are being distributed to those who need them. Inspectors should also compare the results of the interviews with security managers to those with the users to determine whether the distribution mechanisms are functioning as intended.

M. Inspectors should determine whether policy updates and directives issued by DOE Headquarters are appropriately distributed.

Feedback and Improvement

N. Most organizations have some type of central, integrated system to identify and follow the status of deficiencies identified during self-assessments, operations office surveys, and inspections. Inspectors should determine what system or systems are being used. Some organizations have a comprehensive system that includes all safeguards and security-related deficiencies. In other organizations, each area, including CMPC, has a separate tracking system.

O. Inspectors should review the self-assessment program in detail. They should determine whether self-assessments are performed at least annually as required by DOE policy and whether they review all aspects of the organization's CMPC program. Selected self-assessment reports should be reviewed to determine whether root causes are identified when deficiencies are found. It is helpful to compare the results of facility self-assessments to inspection findings or other audit results to learn whether the self-assessments are equally effective.

P. Inspectors should determine who actually performs the self-assessments. The DOE field element may be the security survey staff, as they perform the annual survey. If the persons who actually work with classified matter conduct the self-assessments, there should be some form of independent verification or evaluation of the results. Inspectors should determine whether deficiencies identified during self-assessments are entered into a tracking system, and how corrective actions are selected and achieved.

Q. Inspectors should determine whether an organization has a tracking system and how it operates. In conjunction with the survey program topic team, they should determine whether the tracking systems have a means of monitoring the status of all inspections, surveys, self-assessments, and other similar activities. Also, inspectors should determine whether there is a formal system to independently verify that corrective actions have been completed and that the original problem has been effectively resolved. Inspectors may elect to select a sample of CMPC-related deficiencies from several sources and determine whether they were entered into the tracking system. Finally, they can select a sample of CMPC-related deficiencies indicated as closed to verify that they have in fact been adequately corrected.

R. Inspectors should determine whether corrective action plans exist for deficiencies and whether deficiencies are analyzed and prioritized. They should determine whether schedules and milestones have been established and whether specific responsibilities to ensure completion have been assigned down to the individual level. Inspectors should also determine whether root cause analyses are performed. If so, the inspectors should request documentation on root cause analyses for significant deficiencies listed in the tracking system and the rationale for the particular course of corrective actions chosen. As a related activity, inspectors may elect to review how resources required for corrective actions are introduced into the budget process.

S. At contractor facilities, inspectors should review the role of DOE oversight by interviewing selected DOE security or survey managers to determine how DOE implements their responsibilities. Specific items to cover include how DOE reviews the CMPC management program on surveys, how DOE tracks the program status, and how DOE and the facility interact on a day-to-day basis. Additionally, key facility managers should be interviewed to gather their views on the same subjects.

This page intentionally left blank.

Section 2.2

Foreign Ownership, Control, or Influence

Contents

References

DOE Order 470.1, Chapters V, VI, and IX

General Information

DOE has established policies and procedures designed to protect against any undue risk that may result when contractors or subcontractors controlled or influenced by foreign governments, organizations, or individuals are allowed access to classified information. These procedures require that bidders and contractors needing access to classified information for the performance of proposed work submit FOCI information statements or certifications [Department of Energy Acquisition Regulation (DEAR) 952.204-73] to DOE, in accordance with the provisionary clause required to be included in applicable solicitations.

If FOCI certification submittals contain only negative responses, the respective DOE operations office or Headquarters element may make a positive determination based upon the submittal and award the proposed contract. If, however, the FOCI certification contains positive information that FOCI does exist, the certification and supporting FOCI information are required to be submitted to the Headquarters element responsible for FOCI. In coordination with representatives from that element, reviews of the information will be conducted to determine the degree and extent of FOCI in each case. Upon completion of this review, a written response and recommendation is provided to the originating DOE organization. On occasion, Headquarters may recommend that restrictions be placed on the contractor for reasons of FOCI and will suggest that a written plan be submitted by the subject contractor delineating actions the contractor will take to avoid or mitigate the FOCI concern. In these cases, Headquarters reviews the plan of action to determine acceptability. If acceptable, Headquarters normally recommends to the responsible DOE organization that the plan of action be made part of the contract requirements. If unacceptable, Headquarters recommends that the bidder not be considered for contract award or that the affected existing contracts with that contractor be terminated. In some extreme cases, where the particular services of a foreign company cannot be obtained elsewhere, Headquarters may require that a proxy company be established. This company will have a Headquarters-appointed board of U.S. citizens to serve as the company directors and to provide a separate method of controlling the FOCI.

Common Deficiencies/ Potential Concerns

Contracts requiring access to classified information are, at times, awarded without prior receipt of required FOCI certifications from the contractor, without prior receipt of FOCI determinations or recommendations from Headquarters, or without coordination between

the cognizant contracting officer and the Safeguards and Security Director. Any of these conditions could cause the unauthorized placement of classified information or special nuclear material (SNM) within an organization that lacks appropriate DOE approval for the receipt of such information or material, or is owned, controlled, or influenced by foreign interests. The placement of classified information at risk negates much of the assurance that classified matter is properly protected by other aspects of the CMPC program.

Planning Activities

If a large number of site subcontractors or individuals are involved in reviewing FOCI, inspectors may choose to select a representative sample for evaluation. Typically, a selection would include the prime management and operation contractors, as well as a number of subcontractors providing support to those prime contractors.

CMPC inspectors should review the applicable planning documents to gain an understanding of the facility's organizational FOCI responsibilities and the documentation used to record FOCI activities. They should also be prepared to conduct interviews with FOCI points of contact.

Data Collection Activities

Inspectors should interview cognizant DOE security and contracting office personnel and review applicable documentation for the contractor and selected subcontractor organizations. Inspectors should determine whether FOCI certifications or determinations have been executed. Facility approval files should be reviewed to ensure that authorization for access to classified information was granted only after the completion of a FOCI determination. Particular attention should be given to FOCI determinations that have been awaiting approval for an extended period. In these instances, further inquiry is warranted to ensure that the company has not been allowed access to classified information before the determination has been made. If reviews identify concerns relating to the selected organizations, additional contractor FOCI files should be reviewed to determine the status of the overall FOCI program.

Section 2.3

Security Infraction Program

Contents

References

DOE Order 471.4
DOE Order 471.2A, Chapters I, III, and IV
DOE Manual 471.2-1C
DOE Notice 471.3
DOE Manual 452.4-1A
DOE Manual 473.1-1
DOE Manual 471.2-4
DOE Order 473.1

General Information

All organizations that deal with classified matter in any form are required to have a security infraction program. This inspection subject encompasses all aspects of infraction programs, including detecting, investigating, and reporting infractions. It also includes disciplining offenders, analyzing root causes, and initiating comprehensive corrective actions to prevent recurrence.

Responsibility for the security infraction program may be centralized in the group with overall responsibility for the CMPC program, or each suborganization may have an autonomous program. Generally, the more decentralized the incident program responsibilities are, the more likely that deficiencies exist.

Common Deficiencies/ Potential Concerns

No Program To Detect Security Infractions

Occasionally, inspectors encounter organizations that indicate that they have had no security infractions in years. However, closer examination often reveals that the reason is that no one (protective force or staff) routinely checks for the most common problems that result in infractions (for example, classified documents left unsecured, repositories left unlocked). Additionally, many staff are not aware of their responsibility to check their work areas and report infractions if problems are encountered. They mistakenly think that this is solely a protective force responsibility. Such a situation indicates a deficient security awareness and indoctrination program and requires further investigation. The CMPC topic team should coordinate with the protection program management and personnel security topic teams for more data on the inspected organization's training and security awareness programs.

Inadequate Inquiry and Reporting

When examining security infraction reports, inspectors frequently find that some organizations either do not complete infraction report forms as

required, or do not keep them on file. DOE requires that infraction reports be placed in the employee's personnel security file. When reports are available for review, inspectors often find that the required investigation of each security infraction is either not performed, or is performed in a cursory manner.

No Documented Program of Disciplinary Action

Another common problem is that some organizations do not have a documented program of disciplinary action for persons who have committed infractions. There have been cases where persons received multiple infractions in a 12-month period with no action taken by management. One purpose of an infraction program is to hold persons working with classified matter individually accountable for their actions. Without a documented and consistently applied program of disciplinary action, individual accountability cannot be effectively enforced.

No Trend Analysis at Organization or Operations Office Level

Contractors are required to submit infractions to the DOE operations office. The operations office in turn submits infraction reports for themselves and all their contractors to DOE Headquarters. Sometimes these reporting requirements are not met. Even when the reports are submitted, contractors and operations offices rarely do anything more than compile data and forward the reports. They do not analyze the data in the reports to identify trends. An analysis may reveal the need for systemic corrective action, additional policy guidance, or a revision to DOE policy. If trends and systemic deficiencies are not identified, the corrective actions necessary to address root causes will not be taken, and deficiencies are likely to persist.

Planning Activities

During the planning meeting, inspectors interview points of contact and review documentation—for example, SSSP or site security plan (SSP), CMPC program plan (if one exists), security infraction procedures, and others—to characterize the security incident program. Inspectors should cover the following information:

- Suborganization and the position and person responsible for administering the incident program, and their position within the safeguards and security organization and within the overall organization
- Procedures for security and staff members to report infractions
- Procedures followed when an infraction is reported
- Schedule of disciplinary action
- Procedures for trend analysis of monthly reports.

Performance Tests

The Interior Patrol and Observation tests frequently conducted by the protective force topic team are applicable to providing data relating to the security incident program. These tests will initiate tracking an infraction from identification to filing. Also, the CMPC inspectors may elect to conduct the Repository Check and Storage Area Entry tests described in Appendix A.

Data Collection Activities

Detecting Security Infractions

A. Inspectors should review protective force procedures and post orders (during planning if possible) to determine whether the protective force performs routine checks of classified areas to discover infractions, and, if so, whether all

appropriate areas are covered. Inspectors may be able to verify that the protective force checks an area by reviewing patrol records or logs. These actions may be accomplished through coordination with the protective force topic team.

B. Inspectors should interview operations and production staff to determine whether they are aware of their responsibility to report infractions.

Reporting and Investigating Infractions

C. Inspectors should review a sample of infraction reports to determine:

- Whether the reports contain all the information required by DOE orders, including a description of the incident; date, time, and place; and the name of the individual(s) involved. In addition, inspectors should determine whether the reason or cause given in the infraction report indicates that a thorough analysis was performed to determine the root cause, and whether the corrective action indicates that systemic corrections were considered when appropriate.

- Whether the reports are sent to the person with responsibility for the organization involved and not just the immediate supervisor. The intent is to keep all managers aware of infractions when they occur, as well as first-level supervisors.

Disciplining Offenders

D. Inspectors should determine whether the organization has documented personnel procedures to deal with persons who commit infractions. If conditions warrant, such as an unusual number of infractions by one or more persons, inspectors may also elect to review actual personnel records for such persons to determine whether disciplinary procedures were applied. Usually, this is best accomplished by the personnel security topic team.

Analyzing Root Causes and Instituting Corrective Actions

E. Inspectors should review infraction reports and other documents for evidence of thorough analyses of root causes and appropriate corrective actions. Inspectors should interview persons responsible for conducting investigations and selecting corrective actions to determine how thorough their analyses are and how they select appropriate actions. Inspectors should also determine whether persons performing the investigations and selecting corrective actions are looking beyond the obvious surface causes for the infractions and considering the need for systemic corrections that will preclude recurrence even when individual diligence lapses. An example of this type of corrective action for an infraction where a classified document repository was left open at the end of the work day would be: (1) counsel the employee who left the repository open and take appropriate disciplinary action according to procedures (many infraction programs stop here); (2) implement a procedure whereby all persons who have repositories in their work areas check their individual areas before leaving them unattended, and (3) implement a procedure whereby the last person to leave the floor or building for the day checks all work areas. This type of thorough, systematic approach to corrective action provides multiple levels of backup and prevents single-point failures.

This page intentionally left blank.

Section 2.4

Operations Security Program

Contents

References

DOE Order 471.2A, Chapter II

General Information

An OPSEC program must be in place to help ensure that sensitive information is protected from compromise and secured against unauthorized disclosure. The program must be structured to provide program management with the necessary information required for sound risk management decisions concerning the protection of sensitive information.

Common Deficiencies/ Potential Concerns

Lack of Basic Program Elements

Often encountered are OPSEC programs that lack several of the basic elements needed for the program to function effectively. Fundamental OPSEC plans, procedures, and program files must be maintained; an OPSEC manager must be appointed; and an active working group that is representative of the various site organizations must be established and meet on a regular basis. Additionally, the local OPSEC threat must be defined, and the site must have established site-specific Critical Sensitive Information Lists (CSILs) and attendant Essential Elements of Friendly Information (commonly called Indicators).

Lack of Relevant OPSEC Assessments and Reviews

Pertinent, site-specific OPSEC assessments and reviews are sometimes lacking. While the site may fulfill its obligation to conduct either "programmatic" or "facility" assessments at the required intervals, as described in DOE Order 471.2A, and thereby satisfy minimum OPSEC reporting requirements, the site may not have taken into consideration the most relevant, most sensitive, or highest-value programs or facilities. Moreover, due consideration may not have been given to the site's established CSILs/Indicators when deciding what assessments should be performed.

Likewise, OPSEC reviews may not have been performed for new classified facilities/programs or for facilities/programs that have undergone significant changes relevant to introduction of classified or otherwise sensitive activities. If such facilities or programs go unidentified and are therefore not subject to a review, potential OPSEC concerns involving some of a site's most sensitive assets may remain unaddressed.

Finally, the amount of detail provided in OPSEC assessment or review reports is often limited to "boilerplate" information. This indicates that a program or facility study was lacking in depth

and was not comprehensive and detailed enough to provide management with the information needed to implement appropriate countermeasures.

Planning Activities

Interview the OPSEC Program Manager and/or the OPSEC Working Group Leader relevant to:

- Documentation that can be supplied on program plans and procedures that indicate goals and milestones
- Working group documentation indicating membership, scheduled meetings, topics discussed, and meeting minutes
- The formal OPSEC Plan indicating the threat statement(s) and detailed and relevant CSILs/Indicators
- Copies of all OPSEC assessments and reviews for the past six years
- Documentation on OPSEC awareness training and staff attendance.

Data Collection Activities

Through reviews of the above documentation, interviews with both OPSEC program management and various facility staff, and observations throughout the site, review the following:

- Indications that the OPSEC program staff and the working group have been active in identifying and addressing the site's most valuable/sensitive assets.
- Documentation that assessment and review reports have been timely, relevant to the site-specific threat, and detailed enough to be of use in determining any applicable and necessary countermeasures.
- Evidence that OPSEC awareness training for the ordinary "rank and file" staff has been administered to all staff, has been ongoing every year, and has been timely and comprehensive.
- Indications that the site has conducted initial and/or follow-up OPSEC-related studies to identify all ongoing and planned classified or sensitive unclassified activities for their susceptibility to exploitation.
- Evidence that liaison has occurred between OPSEC staff and various site organizations, particularly those having WFO programs and those involved in counterintelligence, and among other field elements and local agencies, as applicable.
- Observations that a practical, common-sense approach to OPSEC is prevalent throughout the site. Examples would be to preclude sensitive asset identification from public view or from overhead (satellite) imagery, or avoidance of placards/signs to identify buildings/rooms as containing sensitive assets.
- Affirmation that the site's OPSEC program status has been reported annually to the Office of Security and Safety Performance Assurance.

Section 3

CONTROL OF SECRET AND CONFIDENTIAL DOCUMENTS

Contents

References

DOE Order 471.2A, Chapter IV
DOE Manual 471.2-1B, Chapter III
DOE Manual 471.2-1C
DOE Manual 452.4-1A
DOE Manual 473.1-1
DOE Manual 471.2-4
DOE Order 473.1

General Information

One of the most significant policy changes in DOE regarding the CMPC topic has been the reestablishment of document accountability, including that for Top Secret. Accountability applies to:

- Top Secret matter
- Secret matter that is maintained *outside* a Limited or exclusion area
- Any matter that requires accountability by national (National Security Agency [NSA] documents), international, or programmatic requirements, classified computer equipment and media supporting Nuclear Emergency Support Team and Accident Response Group operations, national requirements such as CRYPTO and designated COMSEC, international requirements such as North Atlantic Treaty Organization (NATO) ATOMAL, designated United Kingdom documents, Foreign Government Information designated in international agreements, classified WFO programs, SAPs, and other Federal agency-generated documents
- Weapons data designated as Sigma 14
- Electronic storage media containing Sigmas 1, 2, 14, and 15 or a combination of nuclear weapons design/testing media.

In addition, all classified removable electronic media (CREM) must be protected in accordance with current CREM requirements. (See Section 5.)

During planning for an inspection, documentation from the site should be reviewed to assess the facility's total posture in the area of protection and control of Secret and Confidential matter. The CMPC topic team should take a broad, systematic approach in assessing the protection program afforded to classified matter by evaluating the life cycle of the classified matter. The interfaces discussed in Section 8 will assist inspectors in determining how concerns noted by other inspection teams impact on the CMPC topic.

In the absence of accountability requirements for most classified matter, physical protection and access to classified matter become more critical (see Section 3.7). Special attention should be paid to the physical security systems used to control access to Limited Areas or exclusion areas. The following questions may help the data collection regarding the physical security system used by the CMPC program:

- Do the systems function as intended?
  - Are system tests conducted as required?
  - Who is responsible for conducting the system checks?
  - Who is responsible for maintenance of the physical security systems?
  - Are tests conducted on the "entire" system to measure total system effectiveness, or are systems tested individually (for example, alarms on an internal door as opposed to the entire pathway)?
- Do the physical security systems employed by the site meet DOE requirements?
  - Do the systems in place meet the requirements for a Limited Area?
  - Are the systems used for the Limited Area appropriate?
  - Do the systems in place meet the requirements for an exclusion area?
  - Are the systems in place appropriate for an exclusion area?

Complementing the physical systems that protect classified matter is the human element of protection. With the absence of accountability, access controls are of greater importance. Employees need to exhibit the appropriate level of awareness to ensure that access is controlled:

- Are employees aware of the access control requirements in their functional area?
- Is access controlled in a formalized manner?
- How are access violations investigated, followed up, and validated for closure?

In addition to physical protection and access controls afforded the classified matter, inspectors may evaluate the facility approval system to ensure that the facility is approved for the security interests it maintains. The approval process ensures that all facilities eligible to receive, process, reproduce, store, transmit, or use SNM or classified matter have been granted facility approval. The approval is based on a validated, satisfactory safeguards and security system before permitting classified matter or classified and unclassified SNM on the premises.

Section 3.1

Generation

Contents

References

DOE Order 471.2A, Chapter IV.3.f
DOE Manual 471.2-1C
DOE Manual 452.4-1A
DOE Manual 473.1-1
DOE Manual 471.2-4
DOE Order 473.1

General Information

The Generation subtopic includes the specific requirements pertaining to classified document preparation:

- Pagination
- Marking
- Classification review and classification
- Accountability, when required.

DOE requirements for generating classified documents extend beyond initial document preparation. All classified matter must meet DOE standards for proper marking. Additional requirements are imposed for any holdings remaining in accountability. This includes, but is not limited to, SAPs.

DOE routinely generates a large volume and wide variety of classified documents. Included in the definition of classified documents are all records of information that require protection against unauthorized disclosure, regardless of physical form or characteristics. Classified documents are found in a variety of forms, ranging from handwritten notes to final manuscripts. Many have unique marking or handling requirements, and all types must be strictly controlled in accordance with current orders. The most common forms of classified matter held by DOE are:

- Regular letters and reports
- Files, folders, and groups of documents
- Memoranda and letters of transmittal
- Blueprints and viewgraphs
- Photographic slides, negatives, and prints
- Charts, maps, and drawings
- Material (parts, metals, machinery, chemical compounds, etc.)
- Motion picture film
- Videotapes
- Microfilm reels, negatives, and prints
- Aperture cards
- Punch cards
- Data processing software
- Printouts
- Recordings (magnetic media, e.g., video, audio, computer tapes)
- Disks (floppy and removable hard disks)
- Microfiche
- Containers
- Drafts and worksheets
- Documents pending review

- Messages/cables
- Typewriter and printer ribbons
- Printer cartridges.

Responsibility for the proper preparation of classified documents varies between organizations. Some specifically assign document preparation responsibilities (at least for the most common types of documents), while others leave such responsibilities to subordinate organizations or even the originators.

Common Deficiencies/ Potential Concerns

Lack of Specific Written Procedures Assigning Responsibilities

The lack of local, specific written procedures and responsibilities for all required elements of classified document preparation may indicate a lack of firm control over such preparation. In such cases, inspectors should consider taking a close look at preparation practices and originator knowledge of DOE requirements. Additional information on the significance of a lack of written procedures is provided in Section 2, Program Management.

Draft Documents Not Properly Marked

This is a common concern when documents are in the early stages of preparation, such as handwritten manuscripts, notes, sketches, or computations. Often, such documents are in the custody of the originator, either in the originator's own safe or in the originator's file folder in an organizational safe.

Documents Not Reviewed for Classification

The originators of classified documents are seldom original or derivative classifiers. Consequently, two common problems are encountered. First, the originator may wait until a document is in its final form before having it reviewed and classified by an authorized classifier. Meanwhile, they may incorrectly mark and protect the document on the basis of their own estimate of its classification level, category, and classification duration. The second problem is that once marked by the originator, the document may never be reviewed by a proper classification authority.

Incorrect or Missing Markings

Incorrect and missing markings are commonly encountered on all types of documents. The most frequent errors include:

- Backs of documents are not marked with the classification level (all types of documents, including special documents).
- Required special markings are omitted.
- Document title is not marked with the proper classification.
- Classifier and declassification information are omitted.
- Markings for diskettes and covers are incomplete.

Excessive Number of Document Copies

Often, more copies are generated than required for file and distribution. This can occur with

any type of document, but it is more common with letters, reports, viewgraph transparencies, and photographic prints. Inspectors can easily detect when multiple copies of a particular document are filed together, multiple copies of older documents are on hand, or excessive copies are in storage.

Improper Declassification or Change of Classification Level

This problem is not encountered often, but neither is it rare. It is generally evident in Secret documents changed to Confidential, or Confidential documents changed to Unclassified, with no explanation, date, authority, or other required information. Since inspectors do not normally examine unclassified files, it is only by chance that inspectors encounter documents changed to Unclassified. However, inspectors may encounter declassified documents during the back check performance test.

The review of upgrading notices is more important than declassification notices, especially when a document is being upgraded from an unclassified status. There must be assurance that all unclassified copies are promptly retrieved and upgraded. There should be a record that all copies of the unclassified document were upgraded or a certification that the copies were either destroyed or could not be found.

Files and Folders Improperly Marked

Documents of all kinds are often temporarily or permanently placed in folders. At some facilities, all documents placed in safes are kept in folders. Often these folders are not marked as required, or are not adequately marked. For example, a red or pink folder may be marked (stamped) with red ink, which is not visible or legible without close scrutiny.

Classified Cover Sheets Not Used

Often, cover sheets are not attached to handwritten or other preliminary drafts in the possession of the originator. Documents are not required to have cover sheets while in storage in repositories. If documents within a safe do not have cover sheets, inspectors should expect to find a supply of the appropriate cover sheets in, on, or near the safe.

Typewriter and Printer Ribbons Not Marked or Improperly Stored

This problem is most prevalent for ribbons and cartridges that are occasionally used, or are in use, to produce classified information. Such items often lack proper marking or are improperly stored. This is most likely to occur with typewriters that are occasionally used for classified work; for example, those used to type combinations on form SF 700, Security Container Information.

Planning Activities

During the planning meeting, inspectors interview points of contact and review available documentation (for example, SSSP, CMPC procedures, and other pertinent documents) to characterize the document generation program. Elements to cover include:

- The type of accountability system in operation at the facility
- The types of documents originated at the facility (including all types listed previously in this section)
- Which organizations or individuals create those documents (consider all types listed previously in this section)
- The established procedures and responsibilities for the various elements of document preparation (for example, marking, classification, and accountability)
- Approved exceptions to requirements (for example, marking of special documents and use of cover sheets).

If many organizations or individuals are involved, inspectors should select a representative sample for evaluation. Typically, for efficiency, inspectors cover other CMPC areas in addition to document generation. Consequently, a variety of factors should be considered when selecting individuals and accounts to review. It is usually more efficient to use the same individuals and accounts selected for "document review and use" when looking at document generation, rather than selecting a separate sample. Also, it is usually advisable to select accounts that cover the size and complexity range at the facility (from the largest centralized accounts to small, local accounts). If the facility assigns responsibility for document generation and marking to several different individuals or elements (for example, originators, secretaries, and the central document station), it is advisable to ensure that the accounts selected include these different categories. If the facility generates special documents (for example, photographs or aperture cards), inspectors should review the preparation of those documents, even if other inspection activities do not include those specific items.

Performance Tests

The following standard performance tests yield data applicable to this element:

- Document generation
- Document marking
- Document accountability front check
- Document accountability back check.

Sample scenarios for such performance tests are provided in Appendix A.

In the absence of accountability, performance tests other than front and back checks must be used to ensure that the required control and protection exists. Sites may have procedures that require maintaining logs for handling classified documents by individual custodian or storage area. Inspectors should use such records to conduct performance tests to help determine whether the proper controls are in effect.

Data Collection Activities

Reviews of Individual Accounts

A. Inspectors should interview selected personnel specifically responsible for administering document generation. They should also interview other staff and tour workspaces to determine whether site-specific policies are understood and effectively implemented. Inspectors should determine whether the individuals understand local document preparation procedures and their responsibilities. If specific local procedures have not been published, individuals should be asked to explain all aspects of how they prepare documents. Inspectors should also check for availability of necessary procedures, references, rubber stamps, and cover sheets. Inspectors may choose to ask the custodian or responsible individual to demonstrate the procedures.

B. To supplement information provided by routine document holders, inspectors should interview selected individuals who only occasionally generate, write, or prepare classified documents to determine how well they understand their responsibilities. Such persons can be identified by noting the authors of classified memoranda or reports and identifying individuals with security clearances that work outside the limited area. Typically, inspectors indiscriminately select one to five readily available personnel to interview, rather than expending the effort to obtain a random sample. Inspectors should determine exactly how the procedures are applied and compare the results with DOE and site policies. If local procedures do not exist, inspectors should ask the responsible people to explain all aspects of how they prepare documents and interact with other individuals involved. Inspectors may also elect to ask individuals whether they are currently writing or working on any classified documents. If so, inspectors may ask to see such documents and conduct the activities identified in the following paragraph.

C. A valuable method for determining the adequacy of generation programs is to review documents that facility personnel have prepared or are in the process of preparing. This is often done in conjunction with a document file check, when a wide cross-section of facility documents is examined. This is similar to the back check performance test without attention to accountability records. The partially prepared documents can be checked for markings consistent with the stage of development, and for proper storage practices. If appropriate individuals have documents to prepare, inspectors may wish to observe generation activities and have personnel explain each step as it occurs.

D. Inspectors should interview selected specialists and administrative personnel who routinely or occasionally use special or unique equipment (for example, viewgraph machines or photographic processing equipment) to generate classified documents in order to determine how well they understand their responsibilities. Inspectors should determine exactly how the procedures are applied and compare the results with DOE and site policies.

This page intentionally left blank.

Section 3.2

Review and Use

Contents

References

DOE Order 471.2A, Chapter IV.3.f
DOE Manual 471.2-1B, Chapter III
DOE Manual 471.2-1C
DOE Manual 452.4-1A
DOE Manual 473.1-1
DOE Manual 471.2-4
DOE Order 473.1

General Information

This section addresses two general areas of protection:

- The control and physical protection of classified matter while it is in use or being reviewed

- The steps taken to protect classified information upon the transfer, termination of employment or access authorization, or the death or long-term disability of a person formerly authorized access to such information; these include ensuring that personnel having multiple clearance levels are restricted to classified information commensurate with their clearance level.

The control and physical protection of matter in use includes such requirements as:

- Proper marking
- Accountability (when required)
- Access control
- Enforcement of need-to-know
- Confinement to limited or exclusion areas.

Proper marking and accountability overlap with other elements of the subtopic, and are addressed in detail under "Generation," "Accountability," and "Receipt and Transmittal." This section deals with the remaining areas.

Actions upon transfer, termination, death, or long-term disability deal with:

- Security office notifications
- Return of classified matter
- Recovery of badges and passes
- Combination changes
- Termination of access authorizations
- Execution and disposition of termination statements.

Two major methods are encountered in the physical control of classified matter in use. The most common is a decentralized method. In this method, each asset holder is responsible for ensuring that his or her classified matter is confined to proper security areas, constantly attended or under appropriate control when in

use, and made available only to personnel with the appropriate access authorization and need-to-know. This method places the burden for proper use on the individual and usually provides local procedures for doing so. A second method, becoming increasingly common, involves storage of the classified (or in some cases only accountable classified) matter in one or more central storage facilities or libraries. For classified documents, these places have designated reading areas. Users who check out a document must read it in the designated area. In other cases, users are allowed to check out documents and take them to their offices or other approved areas for use. This method allows centralized control over access and enforcement of need-to-know. It may also provide more restrictive control over use areas and constant attending of the documents, depending upon the checkout and removal policies.

A combination of these methods is sometimes encountered, where some documents are kept by individuals while others are located in central repositories and may be checked out by authorized users.

The central facility is the easiest to inspect. Access control and need-to-know practices are examined at only one or a few locations. Frequently, the areas approved for review and use are also limited. Under such a system, practices are likely to be fairly consistent. However, under the decentralized method, each user is "on his own," with little direct supervision. Therefore, individual practices throughout a facility may vary greatly, and inspectors must visit numerous locations to form an accurate picture of sitewide practices.

The procedures for terminating or transferring personnel, or for those persons who have died or have long-term disabilities, vary greatly from site to site. Specific checkout procedures may be promulgated sitewide or may be left up to subordinate organizations. Enforcement of the procedures often rests with working-level organizations. Usually, comprehensive procedures require action on the part of several organizations, including personnel, personnel security, security, and the person's line organization.

Common Deficiencies/ Potential Concerns

Failure To Enforce Need-to-Know

While most facilities usually take care to ensure that a person has the necessary clearance level (for example, a "Q" clearance) before allowing access, they often do not ensure that the person has a legitimate need-to-know. Often, local classified document handling procedures do not address need-to-know, or address it in a cursory manner, without providing useful guidance. Need-to-know is frequently not a conscious consideration when dealing with classified information. As a result, personnel may gain access to documents, including special category information, for which they have no legitimate need-to-know. Indicators to look for include:

- No specific need-to-know procedures
- No formal method of determining and approving need to know for various types of information
- No access list indicating need-to-know approval
- Multiple users having access to a security repository containing documents belonging to various custodians or pertaining to various projects or subjects.

Failure To Continuously Control Classified Documents

The requirement for appropriately cleared personnel to constantly attend or control classified matter is often violated. This condition can occur in many situations, including:

- Open safes left unattended
- Documents left on desks in unoccupied offices
- Documents left unattended in vehicles during mail or messenger runs.

This problem is more likely to occur at facilities where classified documents are stored and used in workspaces throughout the facility. Work areas that contain "L" cleared or uncleared as well as "Q" cleared personnel should be examined closely.

Inadequate Personnel Checkout Procedures

If organizations do not have comprehensive and specific personnel checkout procedures for transfer, termination, death, or extended employee absence, they are likely to have problems or potential problems with access control, accountability, and control of classified documents. Inadequate checkout procedures can result in failure to:

- Inventory and transfer accountable (and non-accountable) classified documents.
- Change combinations on security repositories.
- Remove names from access lists.
- Provide an audit trail for an accountable document.

Planning Activities

During the planning meeting, inspectors interview points of contact and review available documentation (for example, SSSP, local CMPC procedures, and other pertinent documents) to characterize the review and use policies and procedures in effect at the site. Information to be determined includes:

- Local need-to-know policies and procedures
- Locations of classified repositories, and whether they are in appropriately designated security (limited, exclusion) areas
- Procedures for delivering and receiving classified documents to and from the post office, and for intra-site distribution
- Clearing procedures and requirements in cases of transfer, termination, death, or long-term disability
- Any approved exceptions or deviations (in an approved SSSP or SSP) from policy pertinent to the review and use of classified documents.

If the facility has few storage locations and restrictive policies for review and use of classified documents, inspectors normally inspect all areas. If documents are stored in repositories throughout the facility, and classified documents are reviewed and used throughout, a representative sample may be chosen for evaluation. If a facility has both centralized libraries and reading rooms and decentralized storage, review, and use locations, both types of areas should be included in the sample inspected. The sample can also be used to evaluate other CMPC subtopics and subtopic elements.

Inspectors should also determine the best way to inspect checkout practices. Some aspects of these practices, such as transfer of documents and combination changes, can be examined concurrent with the activities mentioned in the previous paragraph. Other aspects, such as execution and disposition of security termination statements, are usually examined by the Personnel Security topic team.

Performance Tests

The following standard performance tests yield data applicable to review and use:

- Document file check (similar to a traditional back check without attention to accountability records)

- Document front check (used for holdings still requiring accountability).

Sample scenarios for such performance tests are provided in Appendix A.

Inspectors may develop performance tests to evaluate this area. For example, inspectors could recruit a facility employee, who does not have the appropriate clearance or a need-to-know, to attempt to obtain a classified document following normal facility procedures. Inspectors would include the results of such an attempt in evaluating the effectiveness of the facility's systems and procedures in protecting classified documents.

Data Collection Activities

Access Control Procedures

A. Inspectors should interview selected document holders, supervisors, secretaries, and other staff members to determine the procedures used for limiting access, enforcing need-to-know, and attending classified documents outside locked repositories. Also, inspectors should determine whether staff members clearly understand the procedures. If the procedures are in writing, inspectors should determine whether they are available to all staff members. Up-to-date access lists should be available to custodians to help them determine need to know for individuals wanting access to classified documents.

B. Inspectors should observe actual practices to determine whether procedures are followed. Normal practices may become evident during the inspection. The practices may be deficient, especially if no adequate policy exists or if normal practices are habitually sloppy. If procedures require reference to an access list to determine need to know, and custodians indicate they refer to the list before granting access, inspectors should determine whether the list is readily available at the appropriate locations.

C. When checking repositories, inspectors should determine who has access. They should check to ensure that the individuals who have access also have a need to know for all the classified information in the repository.

D. Inspectors should accompany or follow intra-site messengers or post office couriers to determine whether they constantly attend and control the classified matter they pick up and deliver.

Checkout Procedures

E. Inspectors should interview administrative personnel and supervisors to determine what checkout procedures are used. They should determine whether these individuals fully understand the procedures and to what extent the procedures are actually followed. The names of people who have transferred, terminated, or died recently should be obtained to see whether their documents have been transferred, their names removed from access lists, and appropriate combinations changed. The CMPC or the Personnel Security topic team should determine whether security termination statements were completed and properly filed, and whether badges and credentials were recovered.

Section 3.3

Accountability

Contents

References

DOE Order 471.2A, Chapter IV.1.a
DOE Manual 471.2-1C
DOE Order 471.4
DOE Manual 452.4-1A
DOE Manual 473.1-1
DOE Manual 471.2-4
DOE Order 473.1

General Information

Though most DOE elements have eliminated accountability for Secret documents within security areas, accountability is required for Top Secret, Secret matter stored outside a Limited or exclusion area, classified computer equipment and media supporting Nuclear Emergency Support Team and Accident Response Group operations, SAPs, Foreign Government Information, Sigma 14, NATO ATOMAL documents, and designated United Kingdom documents, as well as electronic storage media containing Sigmas 1, 2, 14, and 15 or a combination of nuclear weapons design and/or testing data.

Accountable CREM must be handled in accordance with current requirements. (See Section 5.)

As stated in the overview section of the Control of Secret and Confidential Documents subtopic, the document accountability element covers the specific requirements pertaining to accountability in organizations or programs requiring accountability of classified matter. Elements included in document accountability are:

- Accountability responsibility
- Accountability records
  - originated
  - reproduced
  - received or transmitted
  - destroyed
  - subject to a change of classification
- Unique document numbers
- Documentation of Secret documents
- Inventory of documents
- Unaccounted-for (missing) document procedures.

These requirements apply to all accountable documents. They include the need to maintain a clear audit trail that specifies the current location and custodian for each document. The audit trail covers origination (or first receipt by a DOE entity) to destruction (or transmittal out of DOE). DOE requires that specific accountability documentation be placed on documents and that annual 100 percent inventories be conducted. Various steps and reports are also required when accountable documents are discovered to be missing.

Inspection of the accountability element centers on determining whether accountability records accurately reflect accountable holdings. That is, inspectors should determine whether all documents on the records are present, whether all documents on hand are in the accountability records, and whether the required audit trail for all accountable documents is present. Accountability records include document receipts and destruction records; these are also addressed under "Receipt and Transmittal" and "Destruction."

Although DOE policy specifies what a document accountability system must accomplish, it does not specify how the system must be structured. Consequently, inspectors may encounter several different types of systems that satisfy DOE accountability requirements. The characteristics of an accountability system significantly affect the methods used to inspect the system.

The major difference in accountability systems pertains to the degree of centralization. In centralized systems, all accountable documents are carried in a single accountability system that is controlled and operated by designated personnel. Although documents may be held by individuals who are required to keep an inventory record of documents they possess, the formal accountability records are held centrally. In such systems, all incoming and outgoing accountable documents are processed through the central accountability unit. Also, internal transfers are either routed through or reported to the central unit. In some cases, the central unit is responsible for all destruction of accountable documents.

In a decentralized system, custodians holding documents maintain their own independent accountability system. Such custodians may also receive, transmit, and destroy documents independently. The facility may or may not provide detailed guidelines to custodians regarding the structure of their individual accountability systems.

Other decentralized systems incorporate attributes of both types of systems. Individual accountability systems and records are maintained by the various organizations (department, division, or group), but documents may also be held by individual custodians or subordinate organizations.

Another characteristic of an accountability system that affects inspection activities is its level of automation. Automated systems, which are generally centralized systems, maintain the required accountability information in a database. Although hard copies of document receipts and destruction records are also maintained, the database is frequently considered the accountability record.

Manual systems, on the other hand, include only paper accountability records, usually consisting of locally devised document control cards and copies of receipts and destruction records. Inspectors may also encounter systems undergoing a transition from manual to automated. In these cases, a database may exist, but the paper records are maintained and are still considered the authoritative accountability records.

A final characteristic that affects inspection activities is the number of accountable holdings. The number of holdings inspected typically runs from large systems with tens or hundreds of thousands (or even millions) of documents down to small systems with only a few hundred documents. In decentralized systems, individual custodians with separate accountability systems may have only a few documents.

Facilities with a centralized main accountability system may also have other accountability systems in operation. For example, classified computer media, particularly tapes, may be kept in a tape library under a separate system. Also, documents located in SCIFs or SAPs are frequently held under independent, individual accountability systems. Drafts and worksheets are rarely entered into central accountability

systems and may be accounted for in organizational or individual log book systems. These individual systems will not necessarily follow the same procedures as the main accountability system.

The combination of accountability system characteristics affects inspection planning and data collection. A small, centralized, automated system that includes all accountable documents on site is the easiest system to inspect, since only one sample must be inspected and the automated system can often generate random sample lists. Inspection of decentralized automated systems, while presenting more of a challenge, is generally manageable. In such cases, a sample of systems is usually selected, and then a sample (or the entire population) of documents from each selected system is examined. Efficiently inspecting manual accountability systems, particularly large ones, can be difficult, mainly due to the difficulty in generating random samples. Large, decentralized, manual systems are the most time-consuming for inspectors, since individual samples from a number of accounts must be manually generated and reviewed.

Common Deficiencies/ Potential Concerns

Missing Accountable Documents

It is not unusual for a facility to be unable to locate one or more documents in the sample selected for the document accountability front check. Any documents not found are considered missing documents and the facility should initiate the required actions. Detailed instructions on the specific procedures for handling instances of missing documents are presented in DOE Order 471.4.

Sometimes documents are misfiled or accountability records reflect incorrect locations. The facility should be given every opportunity to locate missing documents during the data collection period. However, searching for documents is the facility's responsibility, and inspectors should not waste time trying to track down documents.

Documents Not in Accountability

On occasion, accountable documents are not found to be listed in their accountability systems.

Although such documents are usually found during document accountability back checks, they may be found during any inspection activity involving document review. The types of documents that are most likely to be out of accountability include:

- Reproduced copies of other documents
- Computer media (diskettes, removable hard drives, etc.)
- Computer printouts
- Viewgraphs and slides
- Photographic prints, negatives
- Drafts and worksheets (although these are not normally in the main accountability system, they should be under some form of listing).

Although isolated deficiencies do occur, inspectors finding documents such as punch cards, viewgraphs, or computer media out of accountability may reasonably conclude that the same problem may exist with similar documents elsewhere on the site. Further investigation may be warranted. It is not unusual for the Cyber Security team to be the first to encounter this problem with computer-related documents.

Inaccurate or Incomplete Accountability Record Data

Inaccurate or incomplete data in accountability records is a common occurrence. Certain elements of information are required to allow the positive identification of documents and to provide a clear audit trail. Errors and omissions

in records can impede these efforts. Although such problems can occur with any type of record, data entry errors are probably more prevalent in automated records. Inspectors should be alert to the significance of the missing or incorrect data elements and should determine whether an adverse trend exists.

Failure To Maintain an Audit Trail

An audit trail for each document requires records indicating the current location or disposition of the document, including receipts for transferred documents and records of destruction for destroyed documents. Sometimes, documents are transferred off site (or "loaned") without proper receipting. Receipts for documents transferred off site may not be returned or may not be kept on file. Similarly, destruction records may not be completed or kept on file. These deficiencies are more likely to be widespread in decentralized systems where many individuals are responsible for their own accountability records.

Failure To Maintain an Accurate List of Accountable Documents

The requirement for each holder of Secret documents to maintain a current list of documents on hand is frequently ignored. In decentralized systems in which each holder has an accountability system, those accountability records would also satisfy this requirement. However, in centralized systems in which individual custodians hold documents, each custodian is required to maintain a current inventory list. Often, custodians do not keep such a list (or receipt file) or the list is not updated to indicate receipts, transmittals, or destructions since the list was last generated. This deficiency is likely to be found when site CMPC procedures do not address the requirement, although it is sometimes found at sites that do.

Failure To Conduct a Proper 100 Percent Inventory

DOE requires an annual 100 percent inventory of accountable matter. Inventory procedures at some locations include only the documents listed in accountability records. Such a procedure misses documents that should be, but are not, in accountability. A proper 100 percent inventory requires that each item listed in the accountability record be visually verified. Facilities with large holdings that have not conducted proper inventories are likely to have significant numbers of documents that are not in accountability.

Not Properly Accounting for Drafts

Improper accountability of working drafts is one of the most common deficiencies found in the CMPC topic. DOE Headquarters has issued guidance in this area, but problems continue to exist. It is common to find Secret drafts more than 180 days old that have not been entered into a formal accountability system. Also, although less common, inspectors find drafts that are not entered into accountability when distributed outside the office in which they originated. In addition, inspectors frequently find drafts that are marked with the classification level, but not the category.

Inadequate Reporting of Unaccounted-for Documents

Organizations often do not follow all requirements when documents cannot be located during inventories or other activities. Organizations must follow Office of Security Policy directives on initial notification of missing or unaccounted for documents (i.e., notification within eight hours to the Headquarters Emergency Operations Center), and must follow

up with a preliminary inquiry and subsequent preliminary and final inquiry reports. Details and timelines for inquiries and reporting requirements are currently found in DOE Order 471.4.

Planning Activities

During the planning meeting, inspectors interview points of contact and review documents (for example, SSSP, CMPC procedures, and other pertinent documents) to characterize the accountability system at the inspected facility. The characterization should include:

- The number of accountability systems at the facility and the specific identity of each
- The number of accountable documents in each system
- Whether each system is centralized or decentralized
- Whether each system is automated or manual
- Who is responsible for the operation (maintenance of accountability records) of each system, including responsibility for receipt, transmittal, and destruction, and the corresponding accountability records
- The number of custodians (holders) in each system
- The storage locations of documents associated with each system
- Any special access requirements for any of the systems.

The scope of the inspection generally involves determining how to sample the systems. If dealing with a small number of systems (one to three), it is practical to inspect each system. When dealing with more systems, it is often necessary to select a sample of systems (two, three, or four) to inspect. The method for selecting systems varies with the circumstances. If there are many similar systems, a random sample may be selected. If there are systems of various sizes, it may be useful to select one system of each size. If there are specialized systems, such as SAPs or tape libraries, they may be specifically included in the sample to be inspected. Information developed during planning interviews and document reviews, such as indications of past accountability problems, may help inspectors decide which specific systems to inspect.

Once the systems have been identified, the specific sampling methods must be determined and planned. For each system inspected, two types of samples are usually produced. The first is a sample of documents from the accountability records that inspectors review during the document accountability front check performance test. The second is a sample of document custodians or a sample of classified repositories to be used for the document accountability back check performance test. A detailed discussion regarding population identification, sample selection, and statistical analysis is found in Appendix B.

During planning activities, inspectors identify how the samples will be generated. Automated systems can often be programmed to generate samples of specific sizes or percentages of the population. If this is possible, the inspectors will usually specify the sample size and request the site to generate and enumerate five separate samples of that size, one of which will later be used during the inspection. If automatic sample generation is not possible, a more time-consuming method must be employed.

Performance Tests

Most of the data concerning document accountability is developed from two performance tests:

- Document front check
- Document back check.

The primary purpose of these two performance tests is to determine the accuracy of the accountability system and records. However, the topic team may also conduct several other performance tests to collect data on accountability practices:

- Document generation
- Receipt and transmittal
- Document reproduction
- Document destruction.

Sample scenarios for all these performance tests are provided in Appendix A.

Data Collection Activities

Accountability Systems and Procedures

A. Inspectors should interview accountability system managers and staff as well as selected custodians to determine whether site-specific accountability procedures are understood and are effectively implemented. Inspectors also should determine whether responsible personnel fully understand and are correctly maintaining the document accountability records.

Accountability Records

B. Inspectors should review accountability records and backup documents to determine whether records contain all required information and are properly maintained. In large automated systems, particularly mainframe-based systems, it may be useful to interview appropriate data processing personnel to learn the system's capabilities, weaknesses, and potential vulnerabilities. Inspectors should pay particular attention to determining whether the software allows the users to delete records. If so, inspectors should determine whether the facility has implemented any measures to prevent or detect misuse (for example, a user covering up the loss of a document by deleting the accountability record entry).

Section 3.4

Receipt and Transmittal

Contents

References

DOE Order 471.2A, Chapter IV
DOE Manual 471.2-1C
DOE Manual 452.4-1A
DOE Manual 473.1-1
DOE Manual 471.2-4
DOE Order 473.1

General Information

This element of the subtopic deals with receipt and transmittal of Secret and Confidential documents. Activities include:

- Receipt of documents from off site
- Transmittal of documents off site
- Intra-site transfer of documents
- Hand-carrying documents.

The responsibility for receipt and transmittal of Secret and Confidential documents is normally assigned to a central facility or individual. Centralized systems usually involve the facility mailroom or classified document control station taking procedural responsibility for receiving, accounting, storage or dispatch to users, wrapping, and transmission. Only in rare cases are individual custodians personally responsible for all actions associated with receipt and transmittal. Inspectors should determine the completeness of procedures and the knowledge of the individuals who carry out receipt and transmittal responsibilities.

Receipt of Documents From Off Site

Classified documents received from off site are normally either picked up from the U.S. Postal Service (USPS) facility by site couriers or delivered to the site by USPS delivery personnel. Additionally, there are provisions for the use of express services, such as Federal Express. Inspection interest normally begins at the point when the mail is transferred and continues through its processing by DOE or DOE contractors.

Receipt procedures normally include the physical transfer of incoming mail to the facility mailroom or other location, x-ray check or safety and security screening, and transfer to the intended recipient or document accountability station. The mail is then usually checked for any evidence of tampering, and required receipts are checked against the documents to ensure that descriptions are accurate. If descriptions match materials received, the receipts are usually signed and returned to the sender, and the documents themselves are processed for delivery to the intended recipient. If the documents are not as described, have been missent, were tampered with, or are improperly packaged, the sender's

security office should be contacted immediately or other appropriate action taken.

When required, classified documents must also be entered into formal accountability upon receipt, either during receipt processing or on delivery to the intended custodian (see Section 3.3, "Accountability"). Incoming documents must also be reviewed to ensure that markings meet DOE standards. Any deficiencies must be corrected (see Section 3.1, "Generation").

If the receipt process takes a long time (for example, if delivery to the intended recipient is not possible), the receipt process may also include storage of the incoming documents. When such storage is a possibility, it should also be included in the scope of inspection activities.

Transmittal of Documents Off Site

Offsite transmittal of classified documents is basically the reverse of the receipt process. For accountable classified documents, the process normally begins with accountability record adjustment. Receipts describing the documents in detail are always required and must be prepared according to DOE guidance. One copy of the receipt is maintained in a suspense file until a signed copy is received from the recipient. The remaining copies of the receipt accompany the classified documents in transit.

Next, the documents are double wrapped for shipment. DOE requires the inner wrapping to be marked with the classification of the contents and the recipient's classified mailing address. The outer wrapping also shows the recipient's mailing address, but is not marked to indicate that the package contains classified information. The recipient's address is a classified mailing address approved for the receipt of classified documents. If a facility permits the use of briefcases, the local procedures must fully explain all pertinent requirements. Finally, the package must be sent using approved channels. Normally, Secret information is sent by registered mail, and Confidential is sent by certified mail. DOE has also authorized other methods, such as Federal Express, for use in certain circumstances.

Intra-site Transfer of Documents

Although recommended, receipts are not required for intra-site transfer of non-accountable classified matter. However, when accountability systems are used, the intra-site transfer of classified documents generally follows procedures similar to those used for offsite transmittal and receipt; facilities normally modify the procedures to meet site-specific needs. Inspectors should determine whether local procedures have been developed and promulgated in appropriate security directives.

Inspectors should check a number of key points. It is important that documents are properly wrapped if taken out of a security area, classified information is appropriately protected during transport, packages are inspected by the recipient, storage transport procedures meet DOE requirements, and accountability requirements are met, when required.

Hand-carrying Documents

Under certain circumstances, hand-carrying classified documents is permitted. Normally, this is restricted to emergency situations when classified documents cannot be transferred in time to meet urgent requirements and must be approved by the applicable Departmental entity. Authorization to hand-carry to and from foreign countries must be approved by DOE Headquarters and the person selected to hand-carry the documents must be thoroughly instructed on the procedures to be followed. Hand-carry procedures employed by a facility should be reviewed carefully to ensure that they meet the DOE order requirements and local instructions. Key points include ensuring that personnel are thoroughly briefed on procedures and responsibilities, and that classified information is never exposed to unnecessary risk of loss or compromise. Under no circumstances is classified information to be taken to

unauthorized locations, such as residences or motels.

Common Deficiencies/ Potential Concerns

Documents Not Properly Protected

Review of transmittal procedures at some facilities has shown that classified documents do not receive the required physical protection. Typical problems have ranged from documents being left unattended in vehicles while couriers make deliveries, to classified documents being left in distribution bins while mailrooms are unattended. This can also occur when classified documents are sent directly to the recipient without following procedures or processing through a central receipt station. It also seems to be a common problem when recipients hand-carry documents back from meetings.

Documents Not Properly Marked or Documented

Documents received from off site, especially those from other agencies, are often mismarked. Each document being received must be reviewed for proper marking and brought up to DOE standards as necessary. Two common examples are the lack of downgrading instructions and documentation on Secret matter received from outside agencies. Seldom is sufficient information included to meet DOE standards. Consequently, either the sender must be contacted for additional information, or the receiving facility must apply the proper markings. This can also occur when classified documents are sent directly to the recipient and when recipients hand-carry documents back from meetings. The problem is also addressed in Section 3.1, "Generation."

Transmittal Accountability Receipts Not Returned

This problem is usually reflected in overdue suspense slips being held by the sending facility. Although the problem is caused by sites not returning receipts promptly, the opportunity seldom arises when inspectors can check the offending facility. Rather, it is more common for the inspection to focus on prompt and aggressive follow-up on overdue suspense by the sending facility.

Misaddressed Classified Documents

This problem manifests itself in two ways. First, facilities may not check the current lists of approved classified mailing addresses located in the Safeguards and Security Information Management System (SSIMS) and may therefore send documents to unauthorized facilities and uncleared recipients. Second, facilities receiving missent classified documents may not report the problem to the sender's security office as required by DOE. The missending of classified documents is often reflected in accountability problems.

Improper Wrapping

Single (rather than double) wrapping of classified documents and failure to mark inner packages with required information are typical problems. Improper wrapping is more common at facilities where individual custodians, rather than a central facility, are responsible for transmittal. Sites with widely dispersed security areas also experience more problems with wrapping because custodians may overlook requirements when transferring documents within the same facility.

Improper Transmittal Methods

The most common problem associated with actual transmittal of documents is the choice of incorrect methods. Some facilities regularly fail to use registered mail for Secret and certified mail for Confidential. Additionally, some facilities seem to routinely rely on express services, rather than reserving this method for urgent or emergency situations.

Authorization To Receive Mail Not Current

Facilities often fail to update lists of personnel authorized to receive USPS registered and certified mail. Failure to update lists and to ensure that superseded authorizations are removed from USPS files creates a situation where terminated or uncleared individuals could actually be given classified documents at the servicing post office.

Improper Hand-carrying of Classified Documents

Failure to follow established procedures is a common problem with classified document hand-carry programs. Individuals continue to take classified documents to residences and motels, although such actions are clearly prohibited by DOE orders and local site directives. Early flights, late arrivals, and a lack of attention to proper procedures all seem to contribute to the problem.

Planning Activities

Inspectors interview points of contact and review available documentation (for example, CMPC procedural guide and any specialized transfer procedures) during the planning phase to characterize the classified document receipt and transmittal procedures. Key elements include:

- Procedures used by the facility to receive and send classified documents off site (responsibilities of individuals and central facilities)
- Methods used to ensure that facility recipients are authorized to receive incoming classified documents addressed to them
- Methods used to verify classified mailing addresses before documents are sent off site
- When required, accountability procedures used to ensure that an uninterrupted audit trail is maintained for all classified documents (including preparation of receipts and suspense systems)
- Location of facility security areas and how documents are transferred between security areas
- Specific instructions governing the transfer of classified documents to other government agencies and to outside entities
- Details of the facility's hand-carry program, including the number of individuals authorized to hand-carry documents and how often hand-carrying occurs.

Inspectors should determine which elements of the program are critical to the effective transfer and physical protection of documents, and which will be inspected. Activities that should be considered include:

- Transfer procedures to and from USPS
- Receipt procedures
- Accountability procedures, when required
- Internal distribution procedures
- Dispatch procedures
- Interim storage and physical protection procedures
- Hand-carrying procedures.

Many receipt and transmittal elements can be inspected in conjunction with other inspection topics. However, if circumstances permit, inspectors should plan to observe the actual receipt, transfer, and dispatch of classified documents and discuss procedures with responsible employees as they perform their duties.

Performance Tests

The inspection team can employ the following standard performance tests to yield data applicable to this subtopic:

- Document receipt
- Document transmittal.

Sample scenarios for such performance tests are provided in Appendix A.

Other performance tests may be developed and used to test aspects of the receipt and transmittal process. For example, appropriate personnel could be required to store a "simulated" classified document to determine whether all required procedures are followed.

Data Collection Activities

Receipt of Documents from Off Site

A. It is usually best for inspectors to begin by actually observing the transfer of classified documents to site personnel. This will usually occur at either the U.S. Post Office or the site mail facility. USPS access documents should be checked to ensure that they are current and that only properly cleared employees may receive registered and certified mail for the site. Actual transfer procedures should also be reviewed to ensure that DOE representatives closely check materials they sign for, especially the registered and certified mail accountability documents.

B. If mail is picked up from the post office, the actual procedures used to transfer it to the site should be closely observed. Especially important are stops along the way where mail is left unattended, presence of adequate communications, and provisions for emergency support.

C. Once the mail is received in the facility mailroom or central document station, inspectors should observe whether adequate receipt procedures are used. Is the mail transferred by signature? Is it carefully inspected for evidence of tampering? Has it been sent to the proper classified mailing address and properly packaged? Was the method of transmission appropriate for the contents? Inspectors should interview assigned personnel to determine whether they know what to do if tampering has occurred or if other problems are detected. If assigned personnel appear unsure of DOE requirements or local procedures, specialized performance tests can be quickly developed and used to assess their level of knowledge.

D. Receipt procedures should also be observed to determine whether incoming documents are reviewed for proper marking and documentation. Any deficiencies should be corrected or noted for further action. Procedures should also be checked to ensure that accountable Secret documents are brought into accountability at the appropriate time.

E. Inspectors should observe internal distribution to ensure that documents are properly protected while en route to their intended recipients or storage location. If documents are temporarily stored, those procedures should also be checked to ensure compliance with DOE requirements.

Transmittal of Documents Off Site

F. Frequently, review of incoming procedures and discussions with employees are sufficient to determine the adequacy of transmittal actions. However, at a minimum, inspectors should review the adjustment of accountability records, preparation and suspense of receipts, packaging, verification of the classified mailing addresses,

physical protection, and dispatch of the classified document.

G. Inspectors should determine whether receipts are prepared to formally transfer the documents, a copy of each receipt is retained in a suspense file, and records are annotated to show which accountable documents are being transferred. This is also a good time for inspectors to look at the facility suspense file to determine whether proper and timely follow-up is accomplished for documents that have already been transferred. If no documents are currently in suspense, inspectors can view older (cleared) receipts normally available, in conjunction with interviews, to get an indication of program effectiveness.

H. Packaging procedures should be reviewed to ensure that they comply with DOE requirements. Inspectors should check for secure double wrapping, proper marking of the inside package, and proper addressing of the package. The classified mailing address should be verified and the dispatch of the documents should be reviewed. During the entire process, inspectors should carefully observe the physical protection afforded classified matter to ensure that it meets DOE requirements.

Intra-site Transfer of Documents

I. As discussed earlier, the transfer of classified documents within a DOE facility may incorporate many of the elements found in offsite receipt and transfers. If necessary, inspectors should modify their inspection activities once the system in use at the site is understood. They should review the method of physical transfer, accountability adjustment and tracking procedures, packaging (required if classified documents are transferred between security areas), and the physical security afforded the documents.

J. The best way to determine how the process is conducted is for inspectors to observe the actual transfer of classified documents. Inspectors should interview individuals assigned transfer duties to obtain information and explanations of any variations. If no classified matter is transferred during the inspection, a document transfer performance test can be conducted using simulated classified matter, or appropriate individuals may be asked to transfer an actual document so inspectors can observe the process.

Hand-carrying Documents

K. Methods used to inspect this area depend largely on how the site has established its hand-carry program. Many sites prohibit hand-carrying and thus have no formal program designed to regulate the process and to prepare personnel for hand-carrying responsibilities. At such sites, inspectors should interview those individuals responsible for exceptions, if any.

L. On the other hand, some facilities permit hand-carrying regularly. Usually, these facilities have established a full, formalized program. Although it is impractical to observe actual hand-carrying, inspectors should assess the program by reviewing the training, instructions, and records of personnel authorized to carry classified matter. To get an accurate indication of how the program works, inspectors may attend a training session and talk with people who have been given authorization to hand-carry. Also, inspectors can ask to review security infraction records to determine how well authorized personnel comply with program requirements.

Section 3.5

Reproduction

Contents

References

DOE Order 471.2A, Chapter IV
DOE Manual 471.2-1C
DOE Manual 452.4-1A
DOE Manual 473.1-1
DOE Manual 471.2-4
DOE Order 473.1

General Information

Reproduction of Secret and Confidential documents includes the requirements that directly pertain to the specifics of reproduction as well as other related elements, including:

- Physical protection
- Marking
- Documentation
- Accountability.

DOE requires that classified information be protected continuously during reproduction. This requires strict controls over both the material involved and the equipment used. Additionally, reproduced matter must be properly marked to reflect required information, including the classification level and category. Requirements also exist when reproducing accountable matter to enter the reproduced documents into accountability.

Reproduction of classified documents within DOE can be divided into two categories: copying and printing. Copying, or local duplication, is normally associated with the reproduction of classified matter on common office equipment by document custodians or administrative staff. Printing, or centralized duplication, is usually a much more complicated and formal process. It is normally conducted in facilities designed for that purpose, using specialized equipment. Examples include use of office duplicating equipment (as used in copying, but done in a central facility), blueprint machines, photographic equipment, aperture cards, microfilm, microfiche, and photo-offset presses.

Whatever methods the facility uses, inspectors must clearly understand how the reproduction of classified matter is accomplished, who is responsible for each facet, and any local procedures governing the process.

Generally, the copying process is straightforward and easy to inspect. Most facilities limit the number of copying machines authorized for classified reproduction. Consequently, in some cases the inspection may be as simple as looking at one photocopy machine and discussing procedures with assigned personnel. This can often be done while visiting custodians as part of the document accountability front and back checks. A brief conversation is usually all that is

necessary to determine whether responsible individuals know DOE and local requirements.

Sites with printing plants or centralized reproduction facilities are usually more difficult to inspect. Technical knowledge of a variety of processes may be required to adequately analyze procedures and to determine whether DOE requirements are met. Additionally, the complexity of many such systems requires inspectors to be familiar with diverse elements of classified document control, including receipt and transmittal, generation, accountability, and physical protection. The more complex the central facility, the more time inspectors may need to adequately review procedures and determine program compliance. A comprehend-sive review of a large facility could require several days and several inspectors, although such time and personnel are seldom available. In this case, extensive planning is necessary. Fortunately, most facilities have limited programs that can be adequately evaluated in a reasonable amount of time.

Common Deficiencies/ Potential Concerns

Adequate Procedures Not Available

Depending on the complexity of the reproduction system, local procedures may be required to adequately govern the process. Although DOE orders may provide sufficient guidance for simple copying programs, centralized printing programs normally require detailed procedures. Unfortunately, many sites have not developed adequate local procedures that specify how they will comply with DOE physical protection, marking, documentation, accountability, and transmittal requirements. The need for local procedures, and their adequacy when they exist, should be carefully reviewed.

Photocopy Machine Procedures

DOE requires that copying machines that are routinely used to reproduce classified documents be in security areas and that restrictions and requirements for reproducing classified documents be posted. Special procedures must also be employed to ensure that trapped waste and residual images are cleared, and that uncleared personnel are not present during reproduction. Inadequate procedures, lack of adherence to local instructions, instructions not posted, machines located in non-security areas and, on occasion, the inability to identify the locations of *all* machines authorized for classified, are common problems found by inspectors.

Incorrect or Missing Documentation

Special documentation requirements should exist for reproduced copies and masters. One common problem occurs when custodians photocopy accountable material without changing the documentation. This results in identical copies that cannot be distinguished from each other, and may result in the loss of the required audit trail for accountability purposes.

Documents Not in Accountability

Accountability problems associated with reproduction generally involve master copies, reproduced documents, and overruns. Small-scale copying operations seem to have the most accountability problems. Problems with masters and overruns are generally associated with larger, centralized printing activities.

A fine line exists between overruns and "scrap/ waste." For accountable documents, overruns (complete, extra copies) must be brought into accountability. However, accountability is not required for waste or scrap, which can be returned to the "customer" or destroyed. Experience has shown that problems often exist in this area, and few facilities have adequate procedures in place.

Planning Activities

Inspectors interview points of contact and review available documentation (for example, SSSP,

CMPC procedures, and any specialized procedures) during the planning meeting to characterize the classified document reproduction program. Key elements include:

- Authorized procedures for copying classified documents, including the number and location of reproduction machines, personnel who are authorized to reproduce classified documents, and any special procedures in use.

- Central facilities used for printing classified information (including photographic, blueprint, microfilm, and aperture card facilities). It is important for inspectors to know their location, the types of equipment used, names and phone numbers of supervisors, volume of classified documents handled, and the frequency of reproduction.

- Any approved exceptions to requirements.

Normally, inspectors can review copying programs in conjunction with other inspection subtopics. Checking machines, discussing procedures with responsible individuals, and reviewing duplicated documents often accompany other inspection activities. This is an efficient approach, because interviews with individual document holders normally require inspectors to visit areas where copying occurs. If a large number of copy machines are approved for reproduction, the inspection team might consider some form of sampling technique.

In contrast, inspectors will usually review printing and centralized reproduction facilities as a separate inspection effort and prepare for the review much the same as for accountability checks, destruction, and other similar classified document inspection activities. Since resources are normally limited, inspectors should carefully select the facilities and review potential weaknesses. Once determined, inspectors can develop detailed inspection activities and schedules. Inspectors must also determine whether specialized technical expertise is required to inspect large-scale reproduction facilities.

Performance Tests

The inspection team may consider using performance tests to establish a clear picture of local procedures and the competence of individuals normally assigned to reproduce classified matter. Observation of actual procedures or performance testing may be the only way to adequately evaluate document transfer and physical protection practices.

The following standard performance tests yield data applicable to this subtopic:

- Document front check
- Document back check
- Reproduction.

Other performance tests may be developed and used to more fully test the reproduction of classified matter. For example, appropriate personnel could be required to reproduce a "simulated" classified document using a particular piece of equipment to determine whether they follow all required procedures.

Data Collection Activities

A. For normal copying and duplication programs, inspectors should concentrate on whether copy machines are located in security areas, conspicuously marked with the procedures for classified duplication, and used properly. Inspectors may be able to observe the classified reproduction process. Otherwise, those responsible for duplicating should be interviewed to determine whether they understand requirements and follow approved procedures. If questions arise about procedures or their adequacy, performance tests can be developed to establish a clear picture of local procedures and the competence of individuals involved in reproducing classified matter.

B. Printing or centralized reproduction facilities may require a more thorough review. Normally, inspectors tour the facility and interview assigned personnel. Once reproduction procedures are understood, inspectors can identify key areas and functions and determine whether the process complies with DOE and local requirements. Again, if classified reproduction is taking place during the inspection, inspectors should observe the process. If not, inspectors should interview facility personnel to determine whether procedures are followed, or ask them to reproduce an imitation classified document.

Section 3.6

Destruction

Contents

References

DOE Order 471.2A, Chapter IV
DOE Manual 471.2-1C
DOE Manual 452.4-1A
DOE Manual 473.1-1
DOE Manual 471.2-4
DOE Order 473.1

General Information

The destruction element of the subtopic includes all policies, procedures, and practices for destroying all types of media containing Secret and Confidential information, with the exception of classified materials. Inspection procedures for classified materials are contained in Section 6.

Destruction systems used in DOE can be categorized as either centralized or decentralized. A facility may use either type or a combination of both. Typically, centralized systems have one location on site where all classified media are destroyed. Equipment at these facilities usually consists of high volume shredders or pulverizers. Classified documents and other media are collected at various locations and taken to the facility for destruction, either on a scheduled basis or when a sufficient quantity has accumulated. Frequently, documents and other media are collected and stored for a period of time before being destroyed. Central destruction facilities are normally operated by designated operators, not by individual document holders.

Decentralized systems are becoming increasingly common because they avoid the logistical, accountability, and storage problems associated with large central destruction facilities. Decentralized systems range from small shredders placed in every location where classified documents are stored, to larger shredders serving an entire department or building. The feature they usually have in common is that the machine is operated by individuals who use the classified matter, rather than by designated operators.

The General Services Administration (GSA) Federal Supply Schedule includes a list of document shredders that meet DOE requirements. In addition, Annex B of the NSA Telecommunications System Security Instruction 4004 has a list of approved shredders, pulpers, and disintegrators.

Some non-paper media cannot be adequately destroyed by shredding or pulverizing. Some examples are: computer diskettes, removable hard disks and tapes, microfilm and microfiche, typewriter and printer ribbons, and laser printer cartridges. For these media, DOE policy requires different destruction procedures. Incineration and chemical decomposition are commonly used for destroying classified computer disks and other

media. Degaussing with NSA-approved equipment is another method of destroying classified information on magnetic computer media. The Information Systems Security Products and Services Catalogue published by NSA includes a preferred product list of NSA-approved degaussing equipment. It is important that the DOE operations office issue specific written approval of destruction methods and procedures for these types of classified media, excluding paper documents. Destruction facilities for other than paper documents are almost always centralized and are not necessarily located near the central shredder or pulverizer.

Common Deficiencies/ Potential Concerns

Non-approved or Inadequate Destruction Equipment

Occasionally, destruction equipment (e.g., shredders, pulverizers, degaussers) not approved by the NSA is in use. Inspectors should check the equipment manufacturer and model number against the most current preferred product list. Additionally, approved equipment is occasionally found to be improperly installed. Finally, approved equipment that is properly installed can malfunction, causing problems such as residue that does not meet the maximum size requirements.

Use of Shredders for Non-paper Media

Sometimes shredders are used to destroy classified media such as microfiche, microfilm, and diskettes. This is not in compliance with DOE policy. Because of the density of information on this kind of media, particles can meet the DOE maximum size requirements and still contain recoverable amounts of classified information. These types of classified media must be destroyed by other means, such as incineration, chemical decomposition, or degaussing (for magnetic media). The operations office specifically approves means of destruction for all classified media other than paper documents.

Improper Use of Degaussing Equipment

Facilities sometimes attempt to degauss magnetic computer media without the proper equipment (for example, using a common magnet). NSA approves each piece of degaussing equipment for specific applications. A piece of equipment approved for one magnetic medium may not be approved for another.

Improper Storage

Facilities sometimes store materials awaiting destruction in containers that do not meet DOE requirements. Additionally, documents are sometimes left unattended while awaiting destruction. Such deficiencies are more prevalent at centralized destruction facilities and at facilities where documents are deposited in satellite containers for later pickup and transfer to a central destruction area.

Audit Trail Not Maintained Through Physical Destruction

A common deficiency is the failure to maintain a written audit trail for accountable documents up through the time when they are physically destroyed. This problem is mainly found at facilities with a centralized destruction system. Frequently, document custodians remove documents from the accountability system by completing and signing the record of destruction. This often is done when the document is taken to the central collection point, if centralized destruction systems are used, or when the document is placed in a storage container awaiting destruction. When this happens, the documents are not accounted for from the time the record of destruction is signed until the documents are actually destroyed. DOE policy requires that certain classified documents be continuously accounted for "from cradle to grave." The destruction can be performed by any

appropriately cleared and authorized person as long as the audit trail for each document is maintained until actual, physical destruction.

If this deficiency is found, it is especially important that inspectors determine whether the physical protection of classified documents awaiting destruction meets DOE policy requirements. Documents awaiting destruction must meet all DOE policy requirements for the storage of classified documents. The potential for theft or compromise is much greater when documents are out of accountability as well as improperly stored.

Planning Activities

During the planning meeting, inspectors interview points of contact and review available documentation (for example, SSSP, CMPC procedures, and other pertinent documents) to characterize the document destruction program. Policies and procedures for destroying classified matter other than paper documents should be determined. Elements to cover include:

- All types of equipment used to destroy classified documents and other media at the facility
- Which organizations possess and operate destruction equipment (including shredders, degaussers, incinerators, and all other mechanical, chemical, or thermal means)
- The established procedures and responsi-bilities for document destruction (including whether the operations office has issued procedures or approved the facility procedures)
- Approved exceptions to requirements, including whether the exceptions have been formally approved by DOE Headquarters.

In addition, copies of any written operations office approvals of destruction methods for any kind of classified matter should be requested.

If a large number of organizations or stations are involved, inspectors may select a representative sample for evaluation. Typically, for reasons of efficiency, inspectors cover other elements along with the destruction element of the subtopic. Consequently, a variety of factors should be considered when selecting organizations and stations to review. If the facility relies primarily on decentralized document shredder stations, it is generally more efficient to use the same accounts and custodians selected for "document review and use" interviews, rather than selecting a separate sample of document shredder stations. In the case of a centralized operation, it is advisable to review most, if not all, centralized destruction stations.

Performance Tests

Other than verifying that equipment is operable and that residue is within allowable specifications, opportunities for collecting information through performance tests are limited in this area. Most information can be gathered from reviewing documents and interviews. In some circumstances, it may be useful to have one or more document custodians demonstrate the entire process they normally follow (using a "dummy document"), including physical destruction. Inspectors may also conduct variations on such tests (for example, including dummy classified microfiche in a set of documents to be destroyed in a shredder, and observing whether the person tested recognizes that microfiche should not be shredded but should be destroyed by other means).

Data Collection Activities

Documentation

A. Inspectors should review records of destruction to determine whether procedures are implemented as intended and whether records are maintained as required. Typically, inspectors determine where records are stored and randomly select a credible sample for review (generally 10 to 100). The forms should be checked for completeness, correct dates, document numbers and series, and signatures of persons who destroy the documents, consistent with site and DOE requirements. Other factors to consider are:

- Type of records maintained (for example, is DOE Form 5635.9, Record of Destruction, or a form similar in content, used to record the destruction of accountable documents?)
- Retention period for records of destruction
- Procedure for filling out the form (for example, at what point in the destruction process is the record of destruction completed and signed?)
- The minimum number of persons or witnesses present during the actual destruction of the documents.

Audit Trails

B. Inspectors should interview points of contact, custodians, or specialists to determine whether required audit trails are maintained where traditional accountability systems are still employed. Inspectors should review the procedures for transferring responsibility for control of documents at each stage of the destruction process (for example, does an audit trail exist indicating who had possession of each accountable document until the document was physically destroyed?).

C. It is sometimes advisable to trace a small sample of indiscriminately selected destruction records back through the system to verify that the destruction records are consistent with other site records. This can be accomplished by noting the document series and copy number on recent records of destruction and then following the transfer records back through the system. By examining the dates on the destruction and transfer records, inspectors can determine whether records are accurately maintained and can sometimes identify potential gaps in the accountability record. **Note:** Inspectors should not waste time attempting to trace records back through the morass of paperwork. It is generally sufficient to trace back one or two steps in the accountability records and to focus on recently created documents, which may have readily available records. An indiscriminately selected sample of about 10 records is generally sufficient to indicate whether systemic deficiencies exist. Additional records should be reviewed if evidence of deficiencies is discovered in the initial sample.

Centralized Destruction Stations

D. Inspectors should interview the custodians, administrative staff, or other personnel responsible for operating a centralized destruction station (high-volume shredder, incinerator, or degaussing station) and tour the station to determine whether operations comply with site and DOE requirements. Specific items to determine are:

- The location where documents to be destroyed are stored before removal to the collection point; maximum and typical duration of storage before destruction; protection measures in place at the storage location
- The methods for transferring the documents to the collection point; physical protection during transfer (are the documents left unattended?);

methods for transferring accountability for each document (including determining who accepts responsibility for and signs for the documents at the receiving or collection point)

- The storage location for the documents after they are collected; physical protection measures in place at the collection and storage area; duration of storage.

E. Inspectors should observe the actual facilities for storing and destroying documents and other forms of classified matter to determine whether they comply with DOE orders. Shredder and degaussing equipment should be compared against the lists of NSA-approved equipment contained in the preferred products list. The residue of the destruction process should be examined to determine whether classified information can be recovered. Inspectors should thoroughly check out the area around shredders and pulverizers to determine whether residue in excess of DOE requirements is being discharged. Any of these deficiencies can result in classified matter being left in a form from which classified information could be recovered by unauthorized persons. Inspectors should also check to determine the specific types of magnetic media that are degaussed to determine whether the operations are consistent with the site policy and whether approved and suitable equipment is being used.

Decentralized Destruction Stations

F. Inspectors should interview document holders, administrative staff, or other personnel responsible for operating decentralized destruction stations (most frequently shredders) and tour selected stations to determine whether operations comply with site and DOE requirements. Specific items to determine are:

- Storage practices for documents awaiting destruction; maximum and typical duration of storage before destruction

- Physical protection at the shredder location (does the area meet DOE requirements to review classified documents?)

- Personnel authorized to operate the shredders.

G. Inspectors should observe operations at the shredder location to determine whether personnel correctly destroy documents and protect against unauthorized disclosure during the destruction process.

This page intentionally left blank.

Section 3.7

Physical Protection and Storage

Contents

References

DOE Order 471.2A, Chapter IV
DOE Manual 471.2-1B, Chapter III.1.2
DOE Manual 471.2-1C
DOE Manual 452.4-1A
DOE Manual 473.1-1
DOE Manual 471.2-4
DOE Order 473.1

General Information

DOE orders require that Secret and Confidential matter be adequately protected while in use, storage, or transit. The effectiveness of systems utilized to provide the required protection are even more critical in the absence of accountability. The physical protection and storage element of the subtopic includes all hardware and procedural measures that protect classified documents, including:

- Review and use areas
- Repositories and storage areas
- Security areas
- Access controls
- Locks and barriers
- Intrusion detection systems
- Protective force patrols
- Security shipments and escorts
- Badge and passes.

The inspection of these areas is normally a coordinated effort involving the Physical Security Systems, Protective Force, Personnel Security, and CMPC topic teams, as well as the cyber security team. (See Section 7, Interfaces, for a more detailed discussion of how responsibilities are divided.)

Section 3.2, "Review and Use," contains additional information about physical protection of Secret and Confidential matter in use. Section 3.4, "Receipt and Transmittal," contains additional information about protection of Secret and Confidential documents in transit. SCIFs and communication centers are subject to special requirements, which are discussed further in Section 7.

Physical protection requirements apply to all forms of documents at the facility (for example, blueprints, viewgraphs, photographs, microfiche), as well as to all material items (e.g., weapons components). When planning inspection activities, it is important that inspectors consider all forms of classified matter at the inspected facility.

DOE orders permit the use of either alarm systems or protective force patrols to protect Secret or Confidential matter in storage. Protective force patrols do not provide continuous protection and are generally considered less reliable than intrusion sensors. Frequently,

protective force patrols only check 25 percent of the site's repositories during a 24-hour period. The CMPC inspectors should devote additional attention to physical protection at facilities that rely primarily on protective force patrols to detect unauthorized intrusion or access to classified matter.

Most frequently, Secret and Confidential matter at a facility is stored either in centralized repositories (for example, vaults, vault-type rooms, or open storage areas protected by patrols or alarm systems when unattended) controlled by a custodian, or in individual repositories (for example, safes and filing cabinets). Many facilities use a combination of these measures (for example, individual custodians have safes in their offices, while large, centralized storage areas are used to store matter that is used infrequently). Areas designated for review and use of classified matter during normal working hours are often used as storage areas during non-working hours.

DOE has adopted the standard forms recommended by GSA. These are:

- SF-700, Security Container Information
- SF-701, Activity Security Checklist
- SF-702, Security Container Checksheet.

These forms are to be used by all DOE facilities to record information about security-related activities.

Common Deficiencies/ Potential Concerns

Security Areas Not Established

The requirement to establish Limited or exclusion areas to protect classified matter is frequently misunderstood and incorrectly implemented. Security areas must be established when the nature, size, revealing characteristics, sensitivity, or importance of the classified matter is such that access cannot be controlled by other internal measures. Facilities with limited scope and volume of work do not normally require security areas to be established if adequate security can be established using other measures. The critical factor when determining whether security measures for classified matter located outside a security area provide a level of protection equal to that of a security area is how well unauthorized access to classified information is precluded.

Persons inspecting areas where classified matter is used or stored outside a security area should pay particular attention to whether persons without the required clearance level have access to the area and, if so, how their access to the classified information is precluded. Inspectors may wish to evaluate security system effectiveness in this area through specialized performance tests, such as having an uncleared or "L" cleared person attempt to gain access to the area or to classified information. Tests of this type should incorporate control measures to ensure that classified information is not disclosed to persons who do not have the appropriate clearance level.

Security Containers Not Meeting Requirements

Vaults, vault-type rooms, safes, and security cabinets must meet established specifications (for example, security cabinets must be GSA-approved). Some facilities use containers that do not meet the standards and do not provide equivalent protection by alternative measures (for example, alarm sensors).

Locks Not Meeting Requirements

DOE orders require that built-in combination locks used to protect classified matter meet X-0 electronic lock standards, and that combination padlocks meet applicable Federal specifications. Many facilities use locks that do not meet these requirements and do not have the appropriate approvals or exceptions. Frequently, facilities use locks that meet Group I (but not Group I-R) standards for operational convenience (Group I-R locks are not as durable). Use of Group I locks instead of Group I-R has only a minor impact on

security effectiveness if complementary protection measures (for example, patrols or alarm sensors) are in place, since the only difference is the relative susceptibility of Group I locks to using x-ray techniques to determine the combination. The use of built-in locks that do not meet Group I standards or padlocks that do not meet the applicable specifications is a more significant concern.

Lock Combinations Not Changed as Required

DOE requires that combinations be changed if a person who has the combination is terminated, transferred outside the area, or no longer needs access to the repository. The facility must use a system to positively control combinations. Frequently, facilities do not strictly adhere to these requirements.

Classified Matter Not Protected from Visual Access

In some cases, areas used for reviewing or processing classified matter do not have adequate barriers to prevent unauthorized visual access. For example, facilities often designate rooms that may be used to review/use classified matter but fail to take measures to cover windows with opaque material when classified matter is exposed. Such deficiencies are particularly significant if uncleared personnel could be present in an area from which classified information may be visible.

Protective Force Patrols Not Performed Consistently

DOE orders permit the use of protective force patrols to protect Secret or Confidential documents in storage. If this is the primary protection method, it is particularly important that the patrols be consistently performed since protective force patrols do not provide continuous protection. In a few cases, the required patrols are not performed. More frequently, the patrols are not performed consistently. For example, patrols may be missed on holidays or when the protective force is operating short-handed.

Repository Checks Not Performed Consistently

Many facilities require the custodians or users to maintain a log of entries and closures of repositories, or checks at the end of the day to verify that the repositories have been closed before personnel leave for the day. Frequently, the checks are not performed as required in site-specific procedures. For example, daily checks may be missed when the document holder is not on duty (for example, on vacation or ill). Also, operating and production personnel often do not devote enough attention to security if the security organization does not establish clear procedures and enforce them consistently.

Inoperable or Blocked Intrusion Sensors

Facilities that use electronic alarm systems do not always assure that they are effective. A particularly frequent problem is encountered in alarmed storage areas when persons place objects such as shelves or boxes in locations that block the “line of sight” coverage of motion detection sensors, rendering them ineffective. Another common problem involves failure to perform corrective maintenance in a timely manner at classified storage areas, which are frequently regarded as a low priority.

Undefined or Inadequate Search Procedures

DOE orders require that all items hand-carried by uncleared personnel be inspected or searched upon entering or exiting a limited area. Additionally, each facility’s SSSP or SSP must specify frequencies for searching vehicles and items carried by cleared personnel. Not all facilities implement these requirements. In some cases, there are no provisions for searching items carried by uncleared persons. In other cases, no

searches are performed on vehicles or on items hand-carried by cleared persons.

Planning Activities

During the planning meeting, inspectors interview points of contact and review relevant documents (for example, SSSP, CMPC procedures) to characterize the physical protection program. Elements to cover include:

- Identification of all Limited and exclusion areas, including a general description of the size and location of each area
- A general description of the scope and nature of the classified interests in each area (for example, the number of repositories in each area, the type and level of matter being protected, the number of employees assigned to each area). This information need not be precise as long as it is sufficient to give the CMPC inspection team a general idea of the scope and nature of the security area for planning purposes.
- General search policies and procedures at each limited and exclusion area, including the frequency of random searches at the security area portals
- The general methods for controlling employee access (for example, badge checks, card readers, Mardix/CAIN booths) to each limited and exclusion area
- The general methods for controlling visitor access (for example, badges, escort policies) within each limited and exclusion area
- The location of all centralized document storage areas, including vaults, vault-type rooms, and open storage areas
- The extent (if any) of alarm system coverage at both centralized storage areas and individual repositories
- The types of repositories used by individual custodians or small groups (for example, safes, previously GSA-approved filing cabinets, and locked rooms)
- The general procedures for protecting individual repositories (for example, repository logs, protective force patrols, alarm protection, or combinations of alarms and patrols)
- The general policies and procedures for controlling combinations to locks that protect classified matter, including the minimum intervals for changing the combinations
- The general policies and procedures for protecting classified matter in transit
- Identification of all means of intra-site and intersite transit authorized at the facility (hand-carrying, rail, plane, or registered mail) and a general idea of the frequency of use of each mode (for example, the average number of shipments per month by rail, plane, truck, registered mail, and hand-carried)
- Approved exceptions to requirements (for example, use of locks or cabinets that do not meet standards).

At large facilities, it is not practical to inspect all organizations or all individual security areas and repositories. In such cases, a representative sample may be selected upon which to base the evaluation. Typically, for reasons of efficiency, inspectors will be covering other CMPC elements and subtopics as well as the "physical protection and storage" element. It is usually more efficient to inspect the same accounts and custodians selected for interviews concerning destruction or reproduction, rather than selecting a separate sample of accounts that store documents. It is generally advisable to select areas and repositories that cover the different sizes and complexities at the facility (from the largest centralized storage areas to an individual custodian's safe and office). If the facility uses a

variety of means to transport documents, it is also advisable to assure that a representative sample is reviewed.

Performance Tests

All the tests in Appendix A provide data applicable to this subtopic. The physical protection provided to classified documents should be observed during any tests conducted. The following standard performance tests yield data specifically applicable to this subtopic:

- User awareness
- Repository checks
- Storage area entry
- Emergency and special procedures
- Search procedures.

Other performance tests may be developed (e.g., in coordination with the physical security topic) and used to more fully test this area. Additional guidance for conducting performance tests is included in the OA Physical Security Systems and Protective Force Inspectors Guides.

The document user awareness test may be particularly applicable at facilities that have areas dedicated to reviewing classified documents (for example, designated rooms within a Limited Area) that are used by a relatively large number of people. Repository check tests may be particularly applicable at facilities that do not use electronic alarm systems and rely primarily on protective force patrols to detect security container violations or unauthorized entry.

The CMPC topic team would not normally perform the last three of the listed tests unless there are indications of problems in those areas. If performed, those tests would normally be performed as joint efforts of CMPC and Physical Security Systems or Protective Force topic team.

The information presented in this and the following section includes activities that the CMPC team would normally perform as part of its review, along with activities that other teams usually perform but that the CMPC topic team might occasionally perform or participate in. The planning activities section covers a wide spectrum of physical protection topics so that the CMPC team will develop a broad-based understanding of the physical protection program before finalizing its list of inspection activities.

Data Collection Activities

Review and Use Areas

A. Inspectors should interview selected security managers, individuals, and other personnel responsible for establishing and controlling areas where classified information is reviewed and used. They should also tour the areas to determine whether site-specific policies are understood and effectively implemented. Inspectors should determine whether the responsible individuals understand the local policies and procedures that pertain to physical protection and individual responsibilities. If there are no published local procedures, individuals should be asked to explain all aspects of their physical protection duties. At large centralized areas, inspectors should focus on access controls, the means used to verify the authorization of an individual granted access to the area, and the procedures for establishing need-to-know. At small areas used by an individual or a small number of individuals, inspectors should focus on how the individuals control access to the area. Inspectors should also check the physical arrangement of selected areas to determine whether adequate barriers are in place. Items to check include: (1) whether there is uncontrolled (that is, unlocked and unmonitored) entry to the area that could allow unauthorized access to the area without observation, and (2) whether clear windows, open doors, or incomplete barriers could allow an individual to observe classified information from outside the area.

Repositories and Storage Areas

B. Inspectors should interview selected security managers and other personnel responsible for establishing and controlling centralized repositories and storage areas, and tour selected centralized repositories and storage areas to determine whether DOE order requirements and site-specific policies are understood and effectively implemented. Inspectors should:

- Determine the means of controlling access when the area is not secured (that is, locked, alarmed, or both).

- Review the procedures for opening the area and placing the alarm system in access mode (if applicable). If the procedures require the person opening the storage area to contact the Central Alarm Station (CAS), note whether the CAS has a means of verifying the identity of the person or verifying that the person requesting that the alarms be put in access mode has the authority to do so.

- Review the procedures for securing the area and placing the alarm system in secure mode (if applicable). Note whether the procedures include provisions for checking that the area is secure (for example, by having a second person verify that doors are locked and sign a log sheet).

- Determine the general condition of the barriers (that is, walls, floors, ceilings, doors, windows) and whether any obvious unprotected penetrations are apparent (for example, walls that do not extend to the ceiling).

- Verify that combination locks are used on doors and determine when the combination was last changed (a sticker is usually placed near the lock or inside the door to indicate the date the combination was changed). Inspectors can often determine whether the built-in combination locks meet Group I-R standards by looking at the back cover of the lock.

- If the repository is a vault, verify that the walls, ceilings, and floor are of substantial construction (that is, equivalent to an 8-inch-thick reinforced concrete wall); a Class 5 vault door is used (look for an engraved statement inside the door that indicates the door class); and an alarm sensor is mounted to detect the door opening (usually a balanced magnetic switch on the door or a motion sensor directed at the doorway).

- Verify that automated or manual entry and exit logs are maintained.

- If the storage areas are not within Limited or exclusion areas, pay particular attention to access controls and verify that the required alarm systems and protective force patrols are implemented.

C. At storage areas protected by alarm systems or vault-type rooms, inspectors may elect to determine whether alarms are operable and whether sensor coverage is adequate. The CMPC team would review alarm sensors only if the physical security systems topic team is not planning to conduct tests of alarm sensors in the classified storage areas of interest to the CMPC team. In such cases, the CMPC team would normally review the operability and coverage of sensors but would not generally address the technical aspects of alarm systems or testing and maintenance programs. A review of sufficient depth for the CMPC team purposes can be accomplished by:

- Observing sensor coverage and verifying that the sensor detection capability is not blocked. Particular attention should be devoted to determining whether sensors adequately cover all viable entrances to the area (for example, doors and windows).

- Verifying that sensors are operable. This generally involves asking the custodian to place the sensor in the secure mode, and then walking around in the area to verify that an

alarm is generated in the CAS. If the team has appropriate expertise, inspectors may also conduct walk tests of the sensors to verify sensor sensitivity and coverage. Such tests, which are discussed in more detail in the OA Physical Security Systems Inspectors Guide, involve walking from an entrance (door or window) at a slow speed (approximately one foot per second) toward a safe, cabinet, or shelf where classified documents are stored to determine whether an alarm is generated.

Note: Inspectors should ensure that all potential safety issues (including protective force response) have been addressed before conducting any activity that would result in an alarm at the CAS.

D. Inspectors should conduct a detailed review of custodian logs, records of protective force patrols, and other required logs to determine whether the logs and records are consistently and accurately maintained. Typically, this would involve selecting a sample of records and verifying that signatures or initials and other information (for example, time or date) are entered as required by site procedures. Experience has shown that a sample representing two to six weeks of records (not necessarily consecutive weeks) provides a credible sample, although the sample size may vary depending on the site procedures. At storage areas protected by protective force patrols, inspectors should verify that the records demonstrate that patrols are conducted at the required intervals (four or eight hours, depending on the type of matter and whether the matter is in a security area). If custodian records are being reviewed, inspectors should consider selecting some sample records from time periods when the primary custodian was not available (which can usually be determined by asking the primary custodian when he or she last took a vacation).

Security Areas

E. Inspectors should interview selected security managers and other personnel responsible for establishing security areas. They should tour selected security areas to determine whether DOE order requirements and site-specific policies are understood and effectively implemented. Specific items include:

- Verifying information gained during the planning meeting, including the size and location of each area and the general description the scope and nature of the classified interests in each area (for example, the number of repositories in each area, the type and level of documents being protected, the number of employees assigned to each area).

- Verifying that the search policies and procedures at Limited and exclusion areas are implemented as required by DOE orders and site-specific policies. In particular, note the frequency of random searches at the security area portals and the means of selecting personnel for searches.

- Observing the methods for controlling employee access (for example, badge checks, card readers, Mardix booths) to each Limited and exclusion area portal.

- Observing the implementation of methods for controlling visitor access (for example, badges, escort policies) within each Limited and exclusion area.

- Observing the condition of the barriers (for example, walls, doors, windows, fences, or gates) and whether any obvious unprotected penetrations are apparent (for example, unmonitored vehicle gates).

- Verifying that any entry and exit logs required by site-specific policy are maintained.

F. Inspectors should interview selected security police officers (SPOs) at portals to determine whether DOE order requirements and site-specific policies are understood and effectively implemented. Specific items to check include the

SPO's understanding of the search policies and procedures at each portal, the frequency of random searches at the security area portals, the means of selecting personnel for searches, the implementation of methods for controlling visitor access (for example, badges and escort policies), and the requirements for maintaining entry and exit logs. By comparing the responses of a small sample of SPOs (typically three to five interviews is sufficient), the CMPC team can usually determine whether there are any significant disconnects between the site-specific policies and the implementation of those policies by SPOs.

Security Shipments

G. Physical protection of Secret and Confidential matter during intrasite transit should be reviewed concurrent with the review of other aspects of transmittal and receipt. The inspectors should devote particular attention to:

- Verifying that the procedures require the matter to be continuously protected (for example, continuously attended or in a securely locked configuration)
- Comparing the physical hardware used to protect classified matter (for example, locks used on delivery vans) to DOE order and site-specific requirements
- Verifying that individuals transporting the matter follow applicable procedures and do not leave the matter unattended.

H. It is generally not practical to observe the physical protection afforded offsite shipments. However, the adequacy of physical protection of offsite shipments can be determined by:

- Observing the physical security at the point of transmittal, noting in particular the means of protecting the matter while awaiting pickup by the courier
- Observing the physical security at the point of receipt, noting in particular the means of protecting the matter while awaiting pickup by the recipient
- Reviewing the procedures used by employees who transport the matter and interviewing such persons to verify that those procedures are understood and followed
- Reviewing the contracts, memoranda of understanding, and procedures that govern the transport of classified matter by commercial carrier (including rail, air, or road transport).

Section 4

CONTROL OF TOP SECRET DOCUMENTS

Contents

Many of the basic control and handling requirements that apply to Secret documents also apply to Top Secret documents. Therefore, the basic guidance regarding inspection activities provided in Section 3 remains valid when inspecting Top Secret holdings and is referred to in this section. Additionally, accountability for Top Secret matter is required for National Security Information, Restricted Data, and Formerly Restricted Data, and strict accountability is still required for all Top Secret Sigma 14 and Foreign Government documents. The control and protection of SCI Top Secret documents is prescribed in DOE Order 5639.8A and Director of Central Intelligence Directive (DCID) 6/9, which provides guidance on the inspection of SCI matter. Therefore, the inspection of Top Secret documents focuses heavily on access control and physical protection and storage of Top Secret documents.

This page intentionally left blank.

Section 4.1

Top Secret Classifiers

Contents

References

DOE Manual 471.2-1C
DOE Manual 475.1-1A, Chapter VI
DOE Notice 471.3
DOE Manual 452.4-1A
DOE Manual 473.1-1
DOE Manual 471.2-4
DOE Order 473.1

General Information

The Top Secret classifiers element of the control of Top Secret documents subtopic includes various requirements and responsibilities. Elements included are:

- The formal appointment of Top Secret classifiers
- Classification of Top Secret documents, including drafts and worksheets
- Downgrading and declassification of Top Secret documents.

The general and specific responsibilities assigned to Top Secret classifiers are fairly limited in scope and are delineated in detail in DOE Manual 475.1-1A.

Top Secret accounts are not found at all DOE facilities, and where they do exist, Top Secret holdings are typically much smaller than Secret holdings. Therefore, the number of Top Secret classifiers (and alternates) is normally very small. The largest concentrations of Top Secret documents are frequently found in SCIFs. Special considerations for inspecting SCIFs are addressed in Section 7.

Common Deficiencies/ Potential Concerns

Failure to Conduct Annual Review of Top Secret Documents

In the past, one of the duties of the Top Secret classifier was to review Top Secret documents annually to determine whether they should be destroyed or returned, or whether their classification should change. Currently the Top Secret classifier is no longer required to complete this duty; however, an annual inventory of accountable matter is still required. Each item listed in an accountability record must be visually verified. All sites must develop procedures to ensure that all accountable matter has been entered into the accountability system. A report of unresolved discrepancies shall be submitted in accordance with DOE Order 471.4. Since the requirement for Top Secret classifiers to conduct the annual review has been dropped and no report of the annual review is required, sometimes the review does not take place. While this omission does not immediately affect the protection of the documents, it can, in the long run, result in an unnecessary accumulation of Top Secret information.

Planning Activities

During the planning meeting, inspectors interview points of contact and review available documents (for example, SSSP and CMPC procedures) to identify:

- The number and identities of Top Secret classifiers
- The volume of Top Secret documents originated at or received by the facility annually
- The comprehensiveness of local procedures in addressing Top Secret classifiers
- The current protection strategy
- The design basis threat, or local threat statement if available.

Once this information has been compiled, inspectors determine which of the Top Secret classifiers (and their programs) will be inspected. Usually, there are so few Top Secret classifiers that they can all be inspected. If that is not the case, a sample of Top Secret classifiers can be selected for inspection.

Performance Tests

As explained more comprehensively in Section 4.3, the following standard performance tests yield data applicable to Top Secret classifiers:

- Document accountability front check
- Document accountability back check.

During these performance tests, inspectors will observe all markings to ascertain whether certified classifiers have properly reviewed the documents. Sample scenarios for these performance tests are provided in Appendix A.

Data Collection Activities

During the onsite inspection, Top Secret classifiers should be interviewed to determine whether their Top Secret classification authority is current and to determine the frequency of their classification reviews, as well as how well they know their responsibilities and how they fulfill those responsibilities. Inspectors should also review program records and Top Secret documents to determine whether the Top Secret classifiers are correctly performing their various duties.

Section 4.2

Top Secret Markings and Forms

Contents

References

DOE Manual 471.2-1C
DOE Manual 452.4-1A

General Information

This element deals with the markings and cover sheets required on Top Secret documents and folders, and with the forms required for processing and using Top Secret documents. These forms include:

- Standard Form (SF)-703, Top Secret Cover Sheet
- DOE Form 5635.3, Classified Document Receipt
- DOE Form 1540.2, Courier Receipt
- DOE Form 5635.9, Destruction Record
- DOE Form 5639.2, Reporting Unaccounted-for Documents.

General requirements for marking classified documents also apply to Top Secret documents; however, some additional requirements apply to Top Secret. As with other classified documents, DOE requires the DOE holder to ensure that all Top Secret documents possessed are properly marked. This requirement applies whether the documents are originated by the holder's organization or received from another source. With some exceptions, primarily SCIFs, most DOE Top Secret accounts do not originate or receive a large number of documents.

Common Deficiencies/ Potential Concerns

Top Secret marking requirements and common problems are basically the same as those for other classification levels. These are discussed in detail in Section 3.

Required Forms Not Available or Not Used

A number of forms specific to Top Secret documents are required. Often, they are not used as required because they are not readily available to those who need them. Inspectors should check to see that the forms listed above are available and are being used.

Planning/Data Collection

The planning and data collection activities applicable to this element are essentially the same as those explained in Section 3.1, "Generation." The primary differences in inspecting Top Secret Markings and Forms are that when inspecting this area, inspectors will:

- Deal with fewer people (Top Secret custodians)
- Deal with fewer and smaller accounts
- Usually have a less complicated sampling task.

This page intentionally left blank.

Section 4.3

Top Secret Control Systems: Access and Accountability

Contents

References

DOE Order 471.1, Chapter VIII
DOE Order 470.1
DOE Manual 471.2-1C
DOE Manual 471.2-1B
DOE Order 471.4
DOE Manual 452.4-1A
DOE Manual 473.1-1
DOE Manual 471.2-4
DOE Order 473.1

General Information

The Top Secret subtopic of the Classified Matter Protection and Control topic encompasses the various requirements and responsibilities assigned to Top Secret custodians:

- Accountability and accountability records
- Inventories and inventory reports
- Access control
- Receipt and transmission
- Storage
- Destruction
- Annual retention, destruction, and downgrading reviews
- Unaccounted-for and compromised documents
- Reporting requirements.

Custodians and alternate custodians are responsible for all aspects of the control and protection of Top Secret documents, including all aspects mentioned above. Top Secret custodian responsibilities dealing with receipt and transmittal, storage, and destruction are addressed in detail in later portions of this section.

Organizations holding Top Secret documents normally have one Top Secret account, and designate one Top Secret custodian and up to three alternate custodians. If circumstances warrant, additional custodians may be approved and designated. If an organization maintains a SCIF or SAPs, it may maintain additional Top Secret accounts for those entities. Generally, the Top Secret holdings at most facilities are limited, are centrally located, and involve few persons.

Common Deficiencies/ Potential Concerns

Inadequate Training

Training for custodians suffers from some of the same deficiencies identified in Section 2.1. Because there are usually only a few custodians, few facilities develop training programs that specifically address Top Secret control system functions.

Access Control

Each site that maintains a population of Top Secret documents is required to establish and use a control system to prevent unauthorized access to or unauthorized removal of classified information. Accountability systems constitute another control used to provide a system of procedures that provide an audit trail and to recognize those who have had access to Foreign Government Top Secret material, Sigma 14, and any other matter that requires accountability by national, international, or programmatic requirements. Inspectors reviewing these systems and stations should determine whether they function as required and implement the most current protection policies. Common deficiencies are untrained personnel, persons who do not have appropriate access authorizations working in close proximity to classified matter, outdated procedures, and need-to-know concerns.

Failure to Perform (or Late) Annual Inventories

Some custodians do not perform the annual Top Secret inventories when required. If inventories are not performed at the required intervals, the likelihood of inaccuracies in the accountability system increases. If inspectors find that inventories are not being performed at the required frequency or not being performed at all, they should conduct both front and back check performance tests to determine the accuracy of the Top Secret accountability system.

Missing Documents

Occasionally, a facility is unable to locate one or more documents in the sample selected for the document accountability front check. Any documents that are not found are considered missing, and the facility should initiate the required actions. The actions are outlined in Section 3.3 of this Inspectors Guide and detailed in DOE Order 471.4.

Sometimes documents are misfiled or accountability records reflect incorrect locations. The facility should be given every opportunity to locate missing documents during the data collection period. However, searching for documents is the facility's responsibility, and inspectors should not waste time trying to track down documents.

Documents Not in Accountability

The common deficiencies found when inspecting Top Secret document accountability systems are the same as those found in accountability systems for classified documents (see Section 3.3, "Accountability").

Sometimes, Top Secret documents are found not in accountability. While such cases usually surface during document accountability back checks, they may be encountered during any inspection activity involving document review. The types of documents that are most likely to be out of accountability include:

- Reproduced copies of other documents
- Computer media (diskettes, removable hard drives, etc.)
- Computer printouts
- Viewgraphs and slides
- Security repository combinations (SF 700)
- Photographic prints and negatives
- Drafts and worksheets (although these are not normally in the main accountability system, they should be under some form of listing).

Even isolated deficiencies concerning Top Secret Foreign Government or Sigma-14 documents are significant; and inspectors finding documents such as punch cards, viewgraphs, or computer media out of accountability may reasonably conclude that the same problem may exist with similar documents at the site. Further investigation is warranted.

Inaccurate or Incomplete Accountability Record Data

Certain elements of information are required to allow the positive identification of specific documents and to provide a clear audit trail for all documents. Errors and omissions on records can make it difficult to identify and track documents. While such problems can occur with any type of record, data entry errors are probably more prevalent in automated records. Inspectors should be alert to the significance of the missing or incorrect data elements and should determine if an adverse trend exists.

Failure to Maintain an Audit Trail

Maintaining an audit trail for each document requires records indicating the current location or disposition of the document, including receipts for transferred documents and records of destruction for destroyed documents. Sometimes, documents are transferred off site (or "loaned") without proper receipting. Receipts for documents transferred off site may not be returned, or may not be kept on file. Similarly, destruction records may not be completed or kept on file.

Top Secret Drafts Not Properly Accounted For

One of the most common deficiencies involves drafts more than 180 days old that have not been properly documented or entered into a formal accountability system. Another less common problem is not bringing drafts into accountability when they are distributed to anyone outside the office they originated in. Inspectors also frequently find that although drafts are usually marked with the classification level, many times they are not marked with the category or contain all required markings.

Planning Activities

The planning activities described in Section 3.3, "Accountability," are also applicable to this subtopic. Although the same procedures may be followed, the limited number of Top Secret accounts and their typically smaller size should make sampling less complicated.

Performance Tests

Since the Top Secret Custodian is responsible for most aspects of Top Secret control and accountability, the following performance tests provide data pertinent to this area:

- Document accountability front check
- Document accountability back check
- Receipt and transmittal
- Document reproduction
- Document destruction.

Sample scenarios for these performance tests are provided in Appendix A.

Other performance tests may be developed and used if needed to more fully test aspects of Top Secret custodian functions. For example, a facility staff member who does not have the appropriate clearance or a need to know could be recruited to attempt to get a Top Secret document through normal, overt procedures. A successful attempt would indicate that procedures are less than adequate or that some individuals are not thoroughly familiar with their responsibilities; in any case, this would signify the need for further investigation. Care should be taken by inspectors to prevent actual access to classified information by an unauthorized individual.

Data Collection Activities

The data collection activities described in Section 3.3, "Accountability," apply to the accountability-related portions of this element. However, inspectors should also interview Top Secret custodians and alternates and review appropriate program records to determine whether:

- Top Secret custodians are properly designated.
- Inventories are conducted and reported properly.
- Proper access control is maintained.
- Top Secret custodians are properly carrying out their other specific responsibilities.
- Required local procedures are in place, up to date, and accurate.

Section 4.4

Receipt and Transmittal

Contents

References

DOE Order 200.1
DOE Manual 471.2-1C
DOE Manual 452.4-1A
DOE Manual 473.1-1
DOE Manual 471.2-4
DOE Order 473.1

General Information

A basic overview of DOE requirements for receipt and transmittal of classified documents is provided in Section 3.4, "Receipt and Transmittal." It is unusual to find that Top Secret documents have been transmitted from one site to another (outside of SCIFs). However, due to the potentially grave impact on national security resulting from the loss or compromise of Top Secret documents, DOE has imposed very stringent controls on receipt and transmittal procedures. This section will look at these controls as they pertain to:

- Receipt of Top Secret documents from off site
- Transmittal of Top Secret documents off site
- Intra-site transfer of Top Secret documents
- Hand-carrying Top Secret documents.

Responsibility for the receipt and transmittal of Top Secret documents is assigned to the facility Top Secret custodian, who is personally responsible for all actions associated with receipt and transmittal. This includes the responsibility for receiving, accounting for, marking, wrapping, transmitting, and storing Top Secret documents held by the facility.

Receipt of Top Secret Documents from Off Site

Top Secret DOE documents may be transported between DOE security areas, by a courier, or transmitted over approved communications networks, as prescribed in DOE Order 200.1, *Information Management Program for Secure Communications Requirements*. Inspection interest normally begins at the point of receipt of an electronic Top Secret document or when a Top Secret document is transferred between a courier and the Top Secret custodian. The inspection effort continues through processing, initial storage, and eventual retransmittal or destruction.

Initial procedures for receipting begin with the physical examination of packaging to positively identify the parcel and to detect any evidence of tampering. If no tampering is detected and the package matches the description on the courier receipt (DOE Form 5635.3 or a comparable receipt), the receipt is signed and given to the courier.

The next step is for the Top Secret custodian to open the package and examine the contents against the receipt packed inside the inner envelope. If descriptions match materials

received, the receipt is signed and returned to the sender. If the documents are not as described, have been missent, were tampered with, or were improperly packaged, the sender's security office must be contacted immediately and appropriate action taken.

When Foreign Government, Sigma-14, or Top Secret documents are transferred, formal accountability must be updated to indicate their location. Incoming documents must also be reviewed to ensure that their markings meet DOE standards. Any deficiencies must be corrected (see Section 4.2, "Top Secret Markings and Forms").

The receipt process generally terminates with the signed receipt being returned to the courier and the storage of the Top Secret document by the Top Secret custodian. Such storage should be inspected. The requirements for the physical protection and storage of Top Secret documents are discussed in Section 4.7, "Physical Protection and Storage."

Transmittal of Top Secret Documents Off Site

Transmitting Top Secret documents off site is basically the reverse of the receipt process. The process begins with the Top Secret custodian preparing documents for transmittal by wrapping them in two opaque envelopes. DOE Form 5635.3, or a receipt comparable in content, which describes the classified contents, is enclosed in the inner envelope. Receipts shall not contain classified information. If enclosing the receipt in the inner envelope is not practical, the receipt may be sent to the recipient with the required advance notification of the shipment, or the receipt may be hand-carried. A copy of the receipt is maintained in a suspense file until the recipient returns a signed copy. The Top Secret custodian then turns the package over to the courier for transmittal under signature service.

Top Secret Documents

The transfer of Top Secret documents within a security area generally follows procedures similar to those used for offsite transmittal and receipt. However, DOE Form 5635.3, Classified Document Receipt, is used instead of DOE Form 5650.1, and the documents may be placed in a folder for transport. The Top Secret custodian, courier, or alternate Top Secret custodian may accomplish the actual transfer within the security area.

Hand-Carrying Top Secret Documents

Hand-carrying must be limited only to those unusual situations outlined in DOE Manual 471.2-1C and generally used only when other means of transmission are unfeasible. Hand-carrying between security areas can be accomplished by one DOE employee who has the proper clearance and has been specifically authorized to perform courier duties.

Common Deficiencies/ Potential Concerns

The receipt and transmittal of Top Secret information has been inspected so infrequently that trends or common deficiencies have not been identified. Potential concerns that should be reviewed during inspections are the same general problems discussed in Section 3.4, "Receipt and Transmittal."

Planning Activities

Inspectors interview points of contact and review available documentation (for example, SSSP, CMPC procedural guide, and any specialized procedures) during the planning meeting to characterize the classified document receipt and transmittal procedures. Key activities include:

- Contacting the site's control stations to determine any existing problems and to obtain a listing of documents charged to the activity to be inspected

- Identifying procedures used by the facility to receive and send Top Secret documents off site

- Identifying methods used to verify classified mailing addresses before documents are sent off site

- Determining the location of facility security areas and how documents are transferred between security areas

- Identifying any specific instructions governing the transfer of Top Secret documents to other government agencies or outside entities

- Determining details concerning local personnel authorized to serve as couriers for Top Secret documents.

Once inspectors understand the Top Secret receipt and transmittal program, they should determine which elements of the program are critical to the effective transfer and physical protection of documents, and which of these will be inspected. Activities to be considered include:

- Courier transfer procedures
- Receipt procedures
- Accountability procedures
- Use of required special DOE forms
- Dispatch procedures
- Interim storage and physical protection procedures
- Local courier procedures.

Many Top Secret receipt and transmittal elements can be inspected in conjunction with other Top Secret review activities. For example, inspection of receipt and transmittal provides the opportunity to look at markings, Top Secret custodian duties, and required Top Secret forms.

Performance Tests

The relative infrequency of Top Secret transfers at most sites normally precludes observing actual receipt, transmittal, and transfer actions. Consequently, performance testing usually represents the best method of checking local procedures and the knowledge of responsible personnel.

The following standard performance tests can be used to gather data applicable to this subtopic:

- Document receipt
- Document packaging
- Document transmittal.

Sample scenarios for these performance tests are provided in Appendix A.

Other performance tests may be developed and used to more fully test aspects of the receipt and transmittal process. For example, personnel locally authorized as couriers could be required to demonstrate transfer of simulated Top Secret documents between site security areas to determine whether all required procedures are followed.

Data Collection Activities

Receipt of Top Secret Documents From Off Site

A. It is usually best for inspectors to begin by discussing receipt procedures with the Top Secret custodian to determine how requirements are met by local programs. When possible, actual transfer procedures should also be reviewed to ensure that DOE custodians and couriers closely check materials for which they are signing, return receipts, and file required reports. Procedures should be observed to determine whether Top Secret documents are reviewed for proper marking and documentation.

B. Inspectors should observe internal distribution to determine whether documents are properly protected while en route to their storage

location. Storage facilities should also be checked to ensure that they meet DOE requirements and have current documentation (for example, combinations).

Transmittal of Top Secret Documents Off Site

C. Review of procedures and discussions with the Top Secret custodians are often sufficient to determine the adequacy of transmittal actions. However, at a minimum, inspectors should review the adjustment of accountability records, preparation and suspension of receipts, packaging, verification of classified mailing addresses, access controls, physical protection, and methods used to transfer Top Secret material.

D. This is also a good time for inspectors to look at the facility suspense file to determine whether proper and timely follow-up is being accomplished for documents that have already been transferred. If no documents are currently suspended, older (cleared) receipts are normally available and can be used in conjunction with interviews to indicate program effectiveness.

Intra-site Transfer of Top Secret Documents

E. The transfer of Top Secret documents between security areas of the facility incorporates many of the elements found in offsite receipt and transfer. Inspectors should tailor their inspection activities accordingly, once they understand the system in use at the site. When available, elements to be inspected should include:

- The actual method used to courier the documents
- Authorization of the couriers involved
- Accountability adjustment and tracking procedures
- Packaging
- The physical security afforded the documents.

Hand-Carrying Top Secret Documents

F. As indicated earlier, hand-carrying of Top Secret documents is to be generally limited to those situations in which more traditional means of transmission are unfeasible. If the facility indicates that hand-carrying of Top Secret documents is a necessity, the procedures should be reviewed carefully, using current guidance promulgated by DOE.

Section 4.5

Reproduction

Contents

References

DOE Manual 471.2-1C
DOE Manual 452.4-1A
DOE Manual 473.1-1
DOE Manual 471.2-4
DOE Order 473.1

General Information

A basic overview of the reproduction of classified documents and relevant DOE requirements is given in Section 3.5, "Reproduction." DOE requires Top Secret documents to be more rigorously protected during reproduction since compromise would have a more serious impact on national security.

As with other classified documents, the reproduction of Top Secret documents includes not only requirements pertaining to the specifics of reproduction, but also related elements, including:

- Physical protection
- Marking
- Documentation
- Forms
- Accountability.

DOE requires that classified matter be protected continuously and has mandated strict controls to ensure that Top Secret documents receive the highest level of protection possible. Controls generally include those applicable to the reproduction of Secret documents:

- New Top Secret documents must receive appropriate markings.

- Accountable reproduced documents must be entered into accountability.

DOE also requires in some instances that permission to reproduce Top Secret documents be obtained from the originator of the original document. The only exceptions occur when DOE Headquarters reproduces documents pertaining to programs under its jurisdiction, or when the documents are compiled for the Secretary.

The reproduction of Top Secret documents encompasses both copying and printing. However, Top Secret reproduction occurs so seldom that at most facilities it is limited to the occasional copying of a document. Section 3.5, "Reproduction," discusses the methods, the identification and characterization of systems, and the features and problems associated with inspecting reproduction procedures.

Common Deficiencies/ Potential Concerns

Top Secret documents are reproduced so rarely that specific trends or common deficiencies have not been identified. Potential concerns are the

same as those found relative to the reproduction of Secret documents, discussed in Section 3.5:

- Adequate procedures are not developed or available.
- Permission is not obtained.
- Documents are not in accountability.
- Photocopy machine procedures are inadequate.

Planning Activities

Planning activities closely parallel those used for inspecting the reproduction of Secret and Confidential documents. Activities include interviewing points of contact and reviewing available documents to develop a clear understanding of how the reproduction process is organized, who is responsible for each facet, and any local procedures that may have been developed to govern the process.

Once inspectors understand the classified document reproduction program, they should determine which organizations and facilities will be inspected. Normally the actual inspection of Top Secret reproduction can be done efficiently in conjunction with the other Top Secret subtopics.

Performance Tests

If questions arise concerning procedures or their adequacy, performance testing may establish a clear picture of local procedures and the level of competence of those individuals normally assigned to reproduce Top Secret documents.

The following standard performance tests apply to this area:

- Document accountability front check
- Document accountability back check
- Reproduction.

Sample scenarios for these performance tests are provided in Appendix A.

Other performance tests may be developed and used to more fully test any aspect of the reproduction of Top Secret documents. For example, appropriate personnel could be required to reproduce a simulated classified document using a particular piece of equipment to determine whether they follow all required procedures.

Data Collection Activities

A. When inspecting Top Secret copying, it is useful for inspectors to concentrate on determining whether reproduction equipment is located in secure areas, whether each machine is posted with appropriate procedures for classified duplication, and whether equipment is used properly. Since Top Secret reproduction seldom occurs during the inspection, it is unlikely that the actual process can be observed. However, discussion with the Top Secret custodian is usually sufficient to determine whether requirements are understood and followed.

B. Printing or centralized facilities authorized for Top Secret reproduction require a more complex inspection process. The inspection normally would begin with a tour of the facility. Discussion with facility personnel may be sufficient to determine whether appropriate protection policy has been implemented and whether approved procedures are followed. Additionally, data gathered in the other Top Secret areas can provide information on accountability, marking, authentication, and physical protection of reproduced documents.

Section 4.6

Destruction

Contents

References

DOE Manual 471.2-1C
DOE Manual 452.4-1A
DOE Manual 473.1-1
DOE Manual 471.2-4
DOE Order 473.1

General Information

A basic overview of DOE requirements for destruction of classified documents is given in Section 3.6, "Destruction." Due to the serious impact on national security that the loss or compromise of Top Secret documents represents, DOE has imposed even more stringent controls on Top Secret accountable document destruction and handling. These additional controls include:

- All destruction must be accomplished in the presence of an official witness.
- An audit trail must be maintained until destruction.
- Destruction procedures must ensure that no portion of the document can ever be reconstructed.

Common Deficiencies/ Potential Concerns

The destruction of Top Secret documents has been inspected so infrequently and occurs so seldom that trends have not been identified or common deficiencies encountered. Analysis of the actions required to destroy Top Secret documents can be used to identify potential concerns that should be reviewed during inspections. These concerns closely parallel those encountered in the destruction of Secret and Confidential documents:

- Adequate procedures are not developed or available.
- Accountability is not maintained up through the time when the documents are physically destroyed.
- Documents are not adequately protected.
- Unapproved equipment is used.
- Equipment does not work properly.
- Equipment is improperly used.

Planning Activities

Inspectors interview points of contact and review available documentation (for example, SSSP, CMPC procedural guide, and any specialized procedures) during the planning meeting to characterize the Top Secret destruction process. Key elements include:

- Contacting the site DOE Top Secret custodian to identify any existing problems and to obtain a listing of documents destroyed by the activity being inspected
- Identifying procedures used by the facility to destroy Top Secret documents (for example, disintegrators or incineration)
- Determining the location of destruction facilities
- Identifying approved exceptions to requirements.

Once inspectors understand the Top Secret destruction program, they should determine the critical elements of the program, and which of these will be inspected. Activities to be considered include:

- Courier transfer procedures to the destruction facility
- Accountability adjustment procedures
- Use of required DOE forms
- Equipment usage and effectiveness
- Residue size and handling.

Performance Tests

The following standard performance test can be used to gather data applicable to this area:

- Document destruction.

A sample scenario for this performance test is provided in Appendix A.

Data Collection Activities

The relative infrequency of Top Secret destruction at most sites usually precludes observing the actual process. Discussion with the Top Secret custodian and alternates can provide an indication of their knowledge and how local procedures are implemented. However, performance testing is usually the best way to check the actual procedures and the knowledge of responsible personnel. Such tests are easily constructed by asking Top Secret custodians to duplicate the actual actions required by site procedures for destruction of a Top Secret document.

Section 4.7

Physical Protection and Storage

Contents

References

DOE Order 471.2A, Chapter IV
DOE Manual 471.2-1C
DOE Manual 471.2-1B, Chapter III.1.2.3
DCID 6/9
DOE Order 470.1 Change 1, with extension, Chapter VIII
DOE Manual 471.1, Chapter III
DOE Manual 452.4-1A
DOE Manual 473.1-1
DOE Manual 471.2-4
DOE Order 473.1

The references presented in Section 3 for physical protection and storage of Secret and Confidential documents are also applicable to protection of Top Secret documents. These references cover repositories, locks, intrusion detection systems, limited areas, exclusion areas, badges and passes, the protective force, document storage, review and use of documents, and transfer of documents. The references listed here identify additional requirements that are specifically applicable to Top Secret documents.

General Information

The scope of the Physical Protection and Storage element is defined in Section 3.7. As with Secret and Confidential documents, the inspection of these elements is normally a coordinated effort involving the computer security, physical security systems, protective force, personnel security, and CMPC topic teams.

Section 4.3, "Top Secret Control Systems: Access and Accountability," contains additional information about physical protection of Top Secret documents in use, which is the responsibility of the facility's CMPC manager and the Top Secret custodians. Section 4.4, "Receipt and Transmittal," contains additional information about protection of Top Secret documents in transit. Data processing systems that process, store, transfer, or provide access to Top Secret information may require additional protection as set forth in DOE Manual 471.2-1C, regarding non-standard storage. DOE Order 5639.8A contains special requirements applicable to Foreign Intelligence information and SCI. Special requirements for the protection and storage of such Top Secret information is found in DCID 6/9. The required practice is to store such information within a SCIF and to apply the extensive physical protection standards for SCIFs. The special requirements that apply to SCIFs are discussed further in Section 6, "Special Programs."

DOE orders require that Top Secret documents be afforded a high degree of protection while in use, storage, or transit. The requirements for physical protection and storage of Top Secret documents are similar to those for Secret and Confidential documents, although the specific requirements are more stringent because of the potentially more

serious consequences associated with the loss or compromise of Top Secret information.

DOE orders permit the storage of Top Secret matter in a locked, GSA-approved security container with one of the following supplemental controls:

- Under intrusion-detection alarm protection with a protective force response within 15 minutes of annunciation of the alarm
- Under protective force inspection every two hours
- Security container equipped with a lock meeting Federal Specification FF-L-2749, only if the container is located in a limited, exclusion, protected, or material access area
- Within a limited, exclusion, protected or material access area randomly patrolled by the protective force at least once every eight hours during nonworking hours. At least 25 percent of the containers in these areas must be inspected once every 24 hours, if the facility has a large number of containers.

Top Secret documents may also be stored in an approved vault meeting the criteria established in DOE Manual 473.1-1. The vault shall be equipped with intrusion-detection protection with a protective force response within 15 minutes of alarm annunciation. When vault-type rooms are used to store Top Secret matter, they also must meet the criteria established in the above referenced manual and approved by the cognizant DOE element. Vault-type rooms must be under intrusion detection alarm protection with protective force response within 15 minutes of alarm annunciation. The vault-type room shall be located within a limited, exclusion, protected, or material access area. When Top Secret matter is located outside of a limited, exclusion, protected, or material access area, in a vault-type room that has been approved by the local cognizant DOE element, the room shall be under intrusion-detection alarm protection with a protective force response within five minutes of alarm annunciation.

The physical protection requirements apply to all forms of documents and matter at the facility (for example, blueprints, viewgraphs, photographs, microfiche, and classified parts). When planning inspection activities, it is important that the inspectors consider all forms of Top Secret matter at the inspected facility.

Few DOE facilities have Top Secret documents, and most that do have only a small number of locations where those documents are used or stored. Most frequently, the Top Secret documents are stored in a separate safe within a centralized repository protected by alarm systems.

Common Deficiencies/ Potential Concerns

Most facilities store Top Secret documents in accordance with DOE requirements. However, deficiencies similar to those identified in Section 3.7, "Physical Protection and Storage," and those listed below have been noted at Top Secret repositories on a few occasions:

- Alarm systems have not been tested.
- Alarm heads in storage locations do not provide adequate protection.
- Intrusion-detection systems are not in place.
- The movement of equipment in storage locations has blocked alarm heads.

Although deficiencies involving physical protection of Top Secret documents are not common, inspectors should review the list of common deficiencies presented in Section 3 when Top Secret storage repositories or transfer procedures are reviewed to determine whether such deficiencies are present.

Planning Activities

Inspection activities for physical protection and storage of Top Secret documents are essentially identical to those used to review Secret and Confidential documents. Inspectors should refer to Section 3.7, "Physical Protection and Storage," for a detailed discussion of those activities. The information below supplements the information in Section 3.7 and presents a few additional activities that are specific to the review of physical protection and storage of Top Secret documents.

In addition to the information identified under Planning Activities in Section 3.7, inspectors should collect the following information (through interviews with points of contact and reviews of available documentation) at facilities that have Top Secret documents:

- The number of repositories in which Top Secret documents are currently stored or authorized to be stored; this includes the scope and nature of the Top Secret classified interests in each area (for example, the approximate number of documents stored in each repository)

- The location and physical protection measures in place at each repository, including: whether the repository is within a limited or exclusion area, the methods for controlling employee access to the repository, the methods for controlling visitor access, the type of repository (for example, vaults, vault-type rooms, safes, or GSA-approved cabinets), the type (if any) of alarm system and its coverage, the frequency of protective force patrols, and whether any additional measures are used to protect the repositories (for example, repository logs)

- All means of intrasite and intersite transit authorized at the facility to transport Top Secret documents

- The procedures used by couriers and escorts who transfer Top Secret documents

- Approved exceptions to requirements that affect Top Secret documents.

Once inspectors understand the structure of the Top Secret document physical protection and storage program, they should determine which organizations, centralized repositories, individual repositories, review and use areas, and security shipments will be reviewed in more depth during the inspection. Because most facilities have only a small number of Top Secret repositories, it is generally practical and advisable to inspect all organizations that possess Top Secret documents and all centralized or individual repositories where Top Secret documents are stored. Typically, for reasons of efficiency, inspectors cover other CMPC Top Secret elements at the same time as the physical protection and storage element.

Performance Tests

As with Secret and Confidential documents, all the tests in Appendix A provide data applicable to this element, and the physical protection provided to classified documents should be observed during any tests conducted. Additional guidance applicable to performance tests is provided in Section 3.7, "Physical Protection and Storage."

Data Collection Activities

A. In addition to the information in Section 3.7, "Physical Protection and Storage" (specifically review and use areas, repositories and storage areas, and security areas), inspectors should interview selected (preferably all) CMPC managers and Top Secret custodians to determine how they implement their responsibilities. In particular, they should determine how the Top Secret custodians assure that persons who ask to review Top Secret documents are appropriately cleared and have a need to know. Inspectors should also determine how the Top Secret custodians maintain control of documents that are being reviewed by other persons (for example, specially designated review areas, continuous attendance during the review).

B. In addition to the activities under the Security Shipments subsection of Section 3.7, inspectors should interview selected Top Secret custodians and couriers to determine how the procedures for protecting Top Secret documents in transit are implemented. The inspectors should devote particular attention to verifying that:

- The procedures are appropriately updated.
- The procedures require the documents to be transported by Department-approved couriers.
- The Departmental couriers and escorts have the required clearances and identification cards.
- Procedures are developed for Top Secret document transfers, and the individuals authorized to transport Top Secret documents understand and follow applicable procedures.

Section 5

CONTROL OF ACCOUNTABLE CLASSIFIED REMOVABLE ELECTRONIC MEDIA

Contents

References

DOE Manual 471.2-1C
DOE Manual 470.4-4

General Information

Following a series of losses of items of accountable classified removable electronic media (CREM) at a National Nuclear Security Administration (NNSA) site and concern that practices and procedures for handling CREM Department-wide might pose risks of similar incidents, the Secretary ordered a temporary Department-wide stand-down of all Department operations involving the handling of CREM. Concurrently, the Deputy Secretary expanded the requirements for the type of CREM that must be held in formal accountability, mandated stricter access and handling procedures, and established requirements to be met by individual sites before resumption of operations involving CREM. Restart requirements included: conducting and reconciling a 100% inventory of previously accountable CREM; identifying CREM that, under the new guidelines, will become accountable; having an independent local organization verify the accuracy of the 100% inventory; providing and clarifying CREM-related training for all CREM custodians and users; incorporating new CREM handling requirements into formal, performance-tested procedures; and having the completion of all of these steps validated by a local independent validation team. Based on the local validation, the Deputy Secretary authorized the resumption of operations involving CREM on a site-by-site basis.

The general administrative controls for the protection of CREM are delineated in Section 3 of this guide. Key aspects include: protection, generation, accountability, storage, marking, destruction, and control of access to the material. The expanded requirements for the type of CREM that must be held in formal accountability and the stricter access and handling procedures and requirements are noted below.

CREM Identification

DOE Manual 470.4-4 identifies accountable CREM as:

- Top Secret
- Secret RD/FRD
- Electronic storage media containing Sigma 1, 2, 14, and 15 or a combination of nuclear weapons design/testing data
- Any electronic media introduced into an approved information system accredited at the Top Secret classification level.

CREM storage media include:

- Removable hard drives
- Laptops with non-removable hard drives
- Zip and Jaz disks
- Floppy disks
- CDs/DVDs
- Optical disks
- Memory cards
- Bernoulli cartridges
- USB flash drives
- Magnetic tapes used to store digital data.

CREM Handling Requirements

In addition to the usual requirements for classified material, CREM must be handled in accordance with the following specific requirements:

- Only one primary custodian and only one alternate custodian
- Formal accountability system
- Unique identification number assigned to each piece of CREM
- Daily check in/check out procedures
- Weekly inventory and reporting of discrepancies
- Standard CMPC destruction requirements.

CREM custodians (only one primary and only one alternate) are responsible for:

- Maintaining a formal accountability system
- Receipting as required when CREM is transferred from one custodian to another custodian
- Performing weekly inventories
- Performing two-person witnessed destruction
- Maintaining accountability via SF 700 for security containers storing accountable CREM. Combinations to these repositories must be classified and protected at the classification level and category of the matter being stored within the container.

When there are multiple shifts, the combination may be provided to the custodian and alternate for each shift. One individual designated as Emergency Notification Personnel may be provided the combination only when the custodian and alternate are not available and access is required.

Individual users of CREM are responsible for:

- Knowing and following the relevant procedures
- Notifying custodians when transferring CREM to coworkers.

In all cases, whoever checks out the CREM assumes personal responsibility for the CREM until it is returned to the custodian or alternate.

Accountability Records

CREM accountability records must include:

- Date of matter
- Brief description (unclassified if possible)
- Unique identification number
- Classification level and category
- Disposition.

In addition to the local accountability records, daily check in/check out records for accountable CREM are required. Daily check in/check out records must be kept for each item of CREM removed from a classified repository. The CREM custodian (and/or alternate) must:

- Ensure the return of accountable CREM at close of business
- Return accountable CREM to the same classified repository
- Retain records in accordance with the Records Inventory Disposition Schedule (RIDS).

Storage

For accountable CREM stored in approved vaults or vault-type rooms:

- For "closed storage" areas, CREM must be stored in GSA-approved safes.
- For "open storage" areas, CREM must be stored in GSA-approved safes or lockable filing cabinets.
- All containers must be locked except when CREM is being retrieved or stored.
- All containers require use of an SF-702 (including filing cabinets).
- Regardless of whether storage is open or closed, only one custodian and one alternate custodian are authorized to have the combination or key to the filing cabinet lock containing accountable CREM (unless a specific variance for additional custodians has been approved).
- For areas using filing cabinets, a documented key control procedure is required.
- Vaults and vault-type rooms must be occupied when open.
- A weekly inventory is required. The weekly inventory may be waived if the locked filing cabinet or GSA-approved repository is located in a vault or vault-type rooms and the container has not been accessed since the last inventory.
- The custodian must maintain visual contact when storage container is open.
- All CREM must be segregated from other classified media stored in the repository.

For accountable CREM stored in GSA-approved containers in limited security areas that are not vaults or vault-type rooms:

- The accountable CREM must be stored in GSA-approved repositories.
- There must be only one custodian and only one alternate custodian unless a specific variance for additional custodians has been approved.
- The container must be locked at al times unless opening for retrieval or storage.
- Each time the container is closed, a new security seal must be affixed and the SF-702 annotated.
- A weekly inventory is required.

Common Deficiencies/ Potential Concerns

Deficiencies/concerns regarding control of accountable CREM are generally identical to those cited for documents (see the "Common Deficiencies/Potential Concerns" portions of Sections 3.1 through 3.7). Inspectors should particularly note how the site addresses the specific differences between general requirements and the specific requirements noted above for CREM handling, accountability, and storage.

Planning Activities

Planning activities regarding control of accountable CREM are generally identical to

(and carried out concurrently with) those cited for documents (see the "Planning Activities" portions of Sections 3.1 through 3.7). During planning, inspectors should particularly note how the site addresses the specific differences between general requirements and the specific requirements noted above for CREM handling, accountability, and storage.

Performance Tests

Performance tests regarding control of accountable CREM are generally identical to (and may be carried out concurrently with) those cited for documents (see the "Performance Tests" portions of Sections 3.1 through 3.7). CREM-related portions of performance tests should be constructed specifically to identify how effectively the site implements current policies and procedures for CREM handling, accountability, and storage.

Data Collection Activities

Line Management Responsibility for Safeguards and Security

A. Inspectors should determine whether:

- There is sufficient management support and oversight.
- There is documented assignment of responsibility for the protection of CREM.
- Personnel with responsibility for security have sufficient authority and control for the protection of CREM.
- Planning documents that cover the CMPC program (for example, site-specific procedures, site security plans, or other planning documents) are current.
- Planning documents appropriately identify the goals, objectives, responsibilities, and overall policies for all aspects of the organization's CMPC program, including CREM.
- Operations personnel interface effectively with the security organization to implement classified matter protection requirements.
- Security personnel are always afforded sufficient access to evaluate and ensure the effectiveness of provisions implemented by line management.
- The organizational structure facilitates efficient communication and positive working relationships between the various organizational elements, and between persons who deal with classified matter (and CREM in particular).
- Management is effective in communicating its goals and objectives, and stresses the importance of CMPC.
- Incentives are used to encourage good performance, and programs are in place to maintain an appropriate level of security awareness.
- Position descriptions for specific individuals reflect responsibilities for the CMPC program (and CREM in particular).
- Management has accepted the identified risks (e.g., via exceptions to policy) in terms of protecting classified information (specifically CREM). Any exceptions have been approved at the proper management level (i.e., through SSA to S-2).

Personnel Competence and Training

B. Inspectors should determine whether:

- A training program is in place, and CREM custodians and other personnel with unescorted access to CREM are adequately trained. A formal training program should

be based on needs and job task analyses, and should include written lesson plans and mandate that tests certifying competency be given to custodians and other persons with key roles in working with classified matter.

- Sufficient staff members are available to accomplish CREM-related CMPC functions.
- Operations and other managers, custodians, and users are satisfied with the available training programs.
- CREM users have a clear understanding and acceptance of their responsibilities.

Comprehensive Requirements

C. Inspectors should determine whether:

- Local CMPC procedures and practices for the protection of CREM are consistent with DOE requirements and sitewide policies.
- Items of CREM are properly identified and controlled in an appropriate location.
- Policies and processes are clear and effective in ensuring that CREM is correctly categorized (e.g., Sigma level).
- Storage repositories containing CREM are adequately controlled at all times (including during day and night while custodians are not on duty).
- A process is in place to determine need-to-know, and the organization has a process to decide who should be granted unescorted access.
- Need-to-know is enforced within vaults or shared repositories at all times (including when custodians are at lunch or on break).
- The number of personnel who are granted authorized unescorted access to repositories containing CREM is not excessive.
- Measures are in place to control access to repositories containing CREM.
- Effective physical security measures are in place (vaults, alarms, protective force response).
- Appropriate controls are maintained to ensure that only personnel with appropriate access authorization and/or escort are employed at sensitive locations.
- The site has appropriate policies and/or risk assessments such that an appropriate graded approach to protection is established, with the highest priority assets being afforded the highest levels of protection.
- Site procedures incorporate the most current DOE/NNSA Headquarters CREM guidance.
- Revisions and updates to policies/procedures are adequately communicated, in a timely manner, to the personnel who must implement them.
- DOE/NNSA policy is adequate and sufficiently clear to ensure that CREM protection objectives are met.
- If seals are used as part of the site's protective measures, the associated procedures and processes are documented and incorporated into the site's training program.

Feedback and Improvement

D. Inspectors should determine whether:

- An adequate self-assessment process is in place, and responsibility for carrying out the process is assigned.

- Security surveys have been conducted as required.
- Identified deficiencies are prioritized and tracked to completion.
- Corrective actions for identified deficiencies are timely.
- Root causes are identified.

Section 6

CONTROL OF CLASSIFIED MATERIALS

Contents

This section addresses inspection activities regarding the control of classified materials or parts. Classified materials include chemical or metallic substances (metals, fabricated or processed items, parts, assemblies, tools, and equipment). SNM may also be classified due to its composition, configuration, or other factors. Classified configurations of SNM must meet the applicable SNM protection requirements for the category and attractiveness level of the material, as well as the requirements for protection of classified information. These protection requirements are frequently more stringent than those for other classified materials in general.

As is the case for classified documents, classified material protection strategies do not always include accountability systems. Normally, the CMPC topic team reviews the measures in place to protect classified material and, when required, to maintain accountability. However, nuclear material control and accountability is not normally included in the scope of this subtopic, since more restrictive SNM protection requirements apply and are inspected by the physical security systems and material control and accountability topic teams; integration between these teams and the CMPC team is essential to ensure complete coverage of the status of protection provided for classified material.

This page intentionally left blank.

Section 6.1

Classified Material Marking

Contents

References

DOE Order 471.2A, Chapter IV
DOE Manual 471.2-1C
DOE Manual 452.4-1A
DOE Manual 473.1-1
DOE Manual 471.2-4
DOE Order 473.1

General Information

The Classified Material Marking element includes the specific requirements pertaining to classification level and category markings on classified materials. Classified material includes such items as equipment, components, and parts, which may be in various stages of manufacture. DOE policy requires that classified materials be marked, by some suitable means, with classification level and category and "other necessary extra markings," which would include (for Secret and Top Secret) serial number or other marking suitable for identification for accountability purposes when accountability is required.

Classified material marking practices vary widely within the DOE community. Essentially, each facility possessing classified materials has a unique approach to marking. Depending upon the size, shape, composition, function, degree of completion or position in the production cycle, etc., items may be marked by:

- Painting (stenciling)
- Stamping
- Engraving
- Labels
- Tags
- Placards.

For various reasons, some facilities do not mark the classified item itself, but may mark its container or covering, or may indicate classification information on accompanying paperwork. Some practices may require formal exceptions from DOE Headquarters.

Responsibility for marking classified material also varies from facility to facility, particularly at facilities that fabricate materials. In most cases, the classification level and category of the material is known before the item is fabricated, and the actual marking is often included as a step or requirement in the production process.

Some unique problems may be encountered in inspecting classified parts. For example:

- Materials may be at a point in the manufacturing process where they are not accessible to the inspector, e.g., in a kiln, glovebox, or autoclave.

- Some parts may have already been assembled and incorporated into larger units or assemblies.

- The classification level of some parts may change as the part progresses through production or reclamation cycles.

Common Deficiencies/ Potential Concerns

The most common deficiency encountered in this subtopic is failure to properly mark classified materials. Even though DOE requirements allow significant latitude in marking methods, materials are frequently not marked at all. The reasons for this vary: in some cases the production process or the precise composition of the material makes marking impractical or impossible; in other cases the material may be too small to mark in a practical manner. In such cases, there may be acceptable alternatives to marking the material itself. Other alternatives, when used, should be formally approved by DOE. However, such approval is often not sought. In other cases category markings are omitted because the original engineering drawings do not show category markings. Additionally, parts are often incorrectly marked when the process involves rollup or rolldown of components into new forms with different classification levels.

Planning Activities

During the planning meeting, inspectors interview points of contact and review available documentation (e.g., SSSP, CMPC procedures) to characterize material marking at the facility much in the same way as described in Section 3 for Secret matter. Elements to cover include:

- Types and quantities of classified materials on hand

- Which organizations or individuals are responsible for marking materials/and ensuring that materials are properly marked

- Method(s) used to mark materials on hand.

The next step is to determine which materials to inspect. Depending upon the quantity of materials present, it may be necessary to use sampling techniques to inspect this subtopic. The sampling guidance provided in Appendix B is applicable to this subtopic. Another approach is to choose the highest-value material items for inspection. These would include locations having weapons trainers or mockups (typically containing all internal bomb components except SNM and high explosives, and referred to as Nuclear Explosive Like Assemblies), weapons assemblies, subassemblies, and individual weapons components.

Performance Tests

If the inspected site has any accountable material items, the following standard performance tests yield data applicable to this subtopic:

- (Material) front check
- (Material) back check.

Sample scenarios for these performance tests are provided in Appendix A.

Data Collection Activities

A. Inspectors should interview selected individuals responsible for material marking (and/or ensuring that material is properly marked) to determine whether site-specific procedures are understood and implemented. Inspectors should also determine the actual marking practices.

B. Inspectors should examine a selected population or sample of classified materials to determine whether they are properly marked.

Section 6.2

Classified Material Accountability

Contents

References

DOE Order 471.2A, Chapter IV
DOE Manual 471.2-1C
DOE Manual 452.4-1A
DOE Manual 473.1-1
DOE Manual 471.2-4
DOE Order 473.1

General Information

Although rare, when accountability for non-SNM classified material is required, the Classified Material Accountability element encompasses the same requirements as for accountability of Secret and Top Secret matter. At some sites, Confidential material may also be in accountability.

Current DOE orders do not specifically address, in sufficient detail, classified material accountability requirements. However, OA's position, concurred in by Headquarters and generally accepted by the field, is that accountability requirements for material generally mirror those for documents. (Section 3 discusses how document accountability systems are to be inspected.) In other words, at a minimum, items must be assigned unique identifiers, accountability records must be maintained, and the records must provide a clear and complete audit trail of each item from creation (or entry into DOE custody) to destruction (or transfer from DOE custody). Records must indicate the current location of each item, and must reveal the loss or unaccountability of any item.

Inspection of this subtopic generally centers on determining whether accountability records accurately reflect accountable holdings—that is, determining whether all material on the records is present; all material present is on the accountability records; and accountability records provide a clear audit trail for all accountable material.

The accountability record systems typically employed for classified materials may differ from those used for classified documents, in that often they are not designed solely to account for classified material. Classified equipment may be carried on a property accounting system, which may include all physical property, both classified and unclassified. Classified parts may be accounted for by means of a production control system, a parts tracking system, or another similar (frequently commercial) system, which could include all parts, classified and unclassified. Any of these systems could be automated or manual. The discussion of accountability systems contained in Section 3.3, "Accountability," is generally applicable to this subtopic and should be reviewed.

Common Deficiencies/ Potential Concerns

Materials Not in Accountability

Materials that should be in accountability, but are not, are often identified during accountability back check performance tests. Material not in accountability may also be encountered during any inspection activity involving material. The materials most commonly found to be out of accountability are those received from off site, rather than those manufactured or fabricated on site. While individual deficiencies of this nature do occur, sometimes an entire lot or shipment (or portion thereof) may be left out of accountability. Additionally, parts may not be properly accounted for if the assembly process involves a change in classification.

Inaccurate Internal Audit Trail

During manufacturing processes, individual items may move from location to location. Typically the accountability system maintains a record of their current location (audit trail). However, the system may not accurately reflect the location of some items. This situation often arises when an item deviates from the normal production cycle, such as if it is sent to undergo a special procedure, is recycled through a part of the production cycle, is pulled out of the cycle for a quality assurance check, or is found to be defective and sent to destruction. In most such cases, the items are not truly "lost" or "missing," but the accountability records do not reflect their actual location, and a time-consuming search may be required to locate them.

Some types of non-SNM materials are classified because of their chemical or radiological composition. These materials can take the form of either solids or liquids, and the accountability records should accurately specify the quantity. Because a small portion of these types of materials can provide the same classified information as the entire quantity, periodic inventories should apply some method to verify that the entire original amount is still present. One acceptable method includes initially verifying the amount of material, and then applying a numbered, tamper-indicating seal to the container (similar to techniques used in material control and accountability). Subsequent inventories only have to verify that the container is present and that the seal has not been disturbed. A system that does not utilize this system, or one that does not provide comparable assurance of detection of the theft of small quantities, does not adequately protect these types of materials.

Planning Activities

During the planning meeting, inspectors interview points of contact and review available general documentation (e.g., SSSP, CMPC procedures, and other pertinent documents) to characterize the classified material accountability system at the inspected facility. The characterization should include:

- The number of classified material accountability systems at the facility
- The size (number of accountable items) of each system
- The types of classified materials
- Whether each system is automated or manual, and how it functions
- Who is responsible for the operation (maintenance of accountability records) of each system, including responsibility for receipt, transmittal, and destruction (if applicable), and the corresponding accountability records
- The number and identities of custodians in each system
- The storage locations of items associated with each system

- Any special access requirements applicable to the material.

The discussion of planning for review of classified document accountability systems, found in Section 3.3, "Accountability," also applies to the inspection of classified material accountability systems. Inspectors should refer to that section.

Performance Tests

Most of the data concerning classified material accountability is developed from two significant performance tests:

- (Material) accountability front check
- (Material) accountability back check.

The primary purpose of these two performance tests is to determine the accuracy of the accountability system and the principal accountability records. If necessary, other performance tests can be conducted to test other aspects of the accountability system. These include:

- (Material) receipt and transmittal
- (Material) destruction.

Sample scenarios for all these performance tests are provided in Appendix A.

Data Collection Activities

A. Inspectors should interview accountability system managers and staff as well as selected custodians to determine whether site-specific accountability procedures are understood and are effectively implemented. Inspectors should also determine whether responsible personnel fully understand and are correctly maintaining accountability records.

B. Inspectors should review accountability records and backup documents to determine whether records contain appropriate information and are properly maintained. In large automated systems, particularly mainframe-based systems, it may be helpful to interview appropriate data processing personnel to learn the application system's capabilities, weaknesses, and potential vulnerabilities.

This page intentionally left blank.

Section 6.3

Physical Protection and Storage

Contents

References

DOE Order 471.2A, Chapter IV
DOE Manual 471.2-1B, Chapter III.1.2
DOE Manual 452.4-1A
DOE Manual 473.1-1
DOE Manual 471.2-4
DOE Order 473.1

The references presented in Section 3.7, "Physical Protection and Storage," also apply to protection of classified materials. These references cover repositories, locks, intrusion detection systems, limited areas, exclusion areas, badges and passes, the protective force, and storage and transfer of materials.

General Information

The term "materials" is used to refer to any classified matter other than documents. This term includes classified weapons components, equipment, tools, and bulk materials. However, SNM protection measures must also meet other requirements. Classified configurations of SNM must meet the physical protection requirements for SNM (at the applicable category) or for classified information (at the applicable category and level), whichever is more restrictive.

The scope of the Physical Protection and Storage element is as defined in Section 3.7. As with Secret and Confidential documents, the inspection of these elements is normally a coordinated effort involving the physical security systems, protective force, personnel security, and CMPC teams. DOE orders require that classified matter be adequately protected while in use, storage, or transit. All requirements for using or transporting classified documents also apply to classified materials. The requirements for storage of classified materials are similar to those for Secret and Confidential documents, although the specific requirements are more flexible to allow facilities to store large or bulky components or equipment. Information relevant to the use of classified material is contained in Section 3.2. Information relevant to the transfer of classified material is contained in Section 3.4.

DOE orders permit the use of either alarm systems or protective force patrols to protect classified matter in storage. The specific patrol frequency requirements depend on the other measures in place and are defined in the cited references.

Common Deficiencies/ Potential Concerns

Inadequate Need-to-Know Enforcement

Deficiencies similar to those identified in Sections 3.2, 3.4, and 3.7 have been noted at DOE facilities. The enforcement of the need-to-know principle is a particular problem at facilities with classified materials that reside in production lines or large open-storage areas, or that are large and bulky and not easily concealed.

Classified Tools or Test and Handling Equipment Not Adequately Protected

Facilities sometimes focus on protecting the classified item being manufactured and overlook protecting classified production support equipment. This equipment often must be left on the production line during non-operating hours due to its size or complexity of removal. Procedures normally exist to provide protection, but they are not always observed.

Classified Material Items in Open Storage Not Adequately Protected

Open storage areas rather than repositories are commonly used throughout the weapons complex to process and store classified material items, including both small and large items. Many such areas were typically used in past years as production areas, and many were never alarmed, thereby not being approved as either vaults or vault-type rooms. Such locations, if currently used for parts storage, are called non-standard storage areas. Their use as storage areas for classified material items is prohibited unless the site has met all the requirements of the current DOE CMPC Manual involving a thorough, documented, validated, and approved assessment of the storage area that characterizes the assets, any compensatory protective measures used in lieu of alarms (e.g., protective force patrols), the time lines for an adversary to remove those assets, and the consequences to national security of that removal.

Planning Activities

The activities that are conducted to review physical protection and storage of classified materials are essentially identical to those used to review Secret and Confidential documents. Inspectors should refer to Section 3.7 for a detailed discussion of those activities. This section includes guidelines to supplement that information and presents a few additional activities that are specific to the review of physical protection and storage of classified materials.

In addition to the information identified under the Planning Activities sections of Sections 3.2, 3.4, and 3.7, inspectors should collect the following information (through interviews with points of contact and reviews of available documentation) at facilities that have classified materials:

- The locations where classified materials are currently, **or are authorized to be**, used or stored, including a general description of the scope and nature of the classified materials in each area (e.g., the number of locations where classified materials are used and stored, the type and level of materials being protected); this information need not be precise as long as it is sufficient to give the CMPC team a general idea of the scope and nature of holdings for planning purposes

- The general methods for controlling visual access when visitors, uncleared persons, or persons without need-to-know (e.g., computer repair personnel) are admitted to areas containing classified materials for official business. Such methods might include, for example, covering large materials with opaque covers, and instituting escort policies

- The location and physical protection measures in place at each repository, including whether the repository is within a Limited or exclusion area, the methods for controlling employee access to the repository, the methods for controlling visitor access, the type of repository (e.g., vaults, vault-type rooms, safes, GSA-approved cabinets, locked rooms), the type (if any) of the alarm system coverage, the frequency of protective force patrols, and whether any additional measures are used to protect the repositories (e.g., repository logs); alarm use and coverage are typically coordinated closely with the physical security systems team, which can conduct a series of tests to determine the effectiveness or coverage of alarm systems that may be doubtful

- The general policies and procedures for protecting classified matter in transit

- All means of intra-site and inter-site transit authorized at the facility (hand-carry, rail, plane, registered mail, etc.) and a general idea of the frequency of use of each mode (e.g., the average number of shipments per month by rail, plane, truck, registered mail, hand-carry, etc.)

- General information about the classified manufacturing process (if applicable), including at what point in the process an item becomes classified, or changes classification level or category, and how it is protected at and after that point

- Approved exceptions to requirements (e.g., use of locks or cabinets that do not meet standards).

At the completion of planning activities, inspectors should understand the structure of the classified material physical protection and storage program, and can determine which organizations, centralized repositories, individual repositories, review and use areas, and security shipments will be reviewed in more depth during the inspection.

At large facilities, it is not practical to inspect all organizations or all individual security areas and repositories. In such cases, a representative sample may be selected for evaluation. Typically, for reasons of efficiency, inspectors will cover other CMPC subtopics along with physical protection and storage.

It is usually more efficient to inspect the same accounts and custodians selected for classified materials accountability performance tests and to look at physical protection concurrent with the front and back check accountability activities, rather than selecting a separate sample of accounts that store classified materials. It is generally advisable to select areas/repositories that cover the spectrum of size and complexity at the facility (from the largest centralized storage areas to an individual custodian's safe and office). If the facility manufactures classified materials (or disassembles classified materials into unclassified materials), inspectors should observe the process during both operating and non-operating hours to determine the adequacy of protection measures. If the facility uses a variety of means to transport classified materials, it is also advisable to assure that a representative sample is reviewed.

Performance Tests

As with Secret and Confidential documents, all of the tests in Appendix A provide data applicable to this subtopic, and the physical protection provided to classified materials should be observed during any tests conducted by OA that involve classified materials. Sections 3.2, 3.4, and 3.7 provide additional guidance applicable to performance tests.

Data Collection Activities

A. In addition to the information identified in Section 3.7, "Physical Protection and Storage," inspectors should tour selected classified materials use and storage areas to determine how procedures for controlling visual access are implemented. In particular, inspectors should

determine how the responsible operations and /or production supervisors determine whether persons who do not have routine access to the areas where classified materials are accessible have appropriate need to know. Also, inspectors should determine how classified materials are protected from visual access by such persons.

B. In addition to the information identified under the Security Shipments subsection of Section 3.7, "Physical Protection and Storage," inspectors should interview selected persons who transfer classified materials to determine how the procedures for protecting classified materials are implemented. Inspectors should devote particular attention to determining how any large or bulky items are wrapped or covered when transported.

C. As mentioned earlier in this section, the need for adequate compensatory measures based on documented, approved assessments is a critical consideration for classified parts kept in non-standard (unalarmed) open storage. Open storage locations are typically found in such areas as (but not limited to) large parts processing areas such as "high bays" and buildings typically constructed to handle/store larger, less portable classified parts (e.g., bomb casings). Data collection activities should include a request for a listing of all such locations that either actually store/process or **are authorized to** store/process classified parts. In touring/observing such locations, the inspector should determine what alarm sensors, if any, might be present and functioning (i.e., perimeter only, or both perimeter and interior), the compensatory measures used in lieu of alarms (e.g., patrol frequencies), the building construction (e.g., corrugated sheet metal, wood frame, or concrete/block), the locations' proximity to non-security areas, (e.g., adjacent to property protection areas), and the types and relative value of parts stored there.

Section 7

SPECIAL PROGRAMS

This section is for OFFICIAL USE ONLY and is published separately.

This page intentionally left blank.

Section 8

INTERFACES

Contents

Integration

Integration is the process of inspection team members working together to achieve a better understanding of the overall protection programs used at DOE facilities. In this context, it includes all the associated attributes: coordinating, cooperating, interfacing, and the assimilating of information. The fundamental goal of integration is to ensure that DOE facilities are provided the necessary degree of protection and that vulnerabilities are clearly identified and analyzed. It also results in a more effective and organized inspection effort, a refinement of inspection techniques, and a more comprehensive inspection report. Lastly, the integration effort significantly contributes to OA's ability to provide an accurate, in-depth evaluation of protection programs throughout the DOE complex.

No inspection topic team operates in a vacuum. The primary objective of a comprehensive inspection is to provide a meaningful, management-level evaluation of the overall status of safeguards and security at the inspected facility. To ensure the accomplishment of this objective, the CMPC team and all other topic teams must work closely together throughout every phase of the inspection process, carefully integrating their efforts with those of the other topic teams. Integration is realized by exchanging information and discussing how information collected by one topic team influences protection program elements observed by other topic teams. Additionally, integration provides a means of prioritizing the efforts of the various topic teams, of assigning particular issues for investigation to particular teams, and of mobilizing special inspection team elements to examine issues that transcend topic boundaries.

No more than five or six days are available for data collection during a typical comprehensive inspection. During this time, the various topic teams will collect a massive quantity of data pertaining to their particular subject matter areas. A careful delineation of each team's inspection activities is required to avoid wasteful duplication of effort. However, even with a clear definition of activities, the boundaries between topic teams are not always neatly differentiated, and each topic team is bound to discover data of interest and significance to other teams. Such data must be shared in a timely manner and determinations made as to which topic team will pursue the issues posed to a point of resolution.

Much of the required integration occurs informally. During both the planning and data collection phases, topic leads and individual topic team members share information with their opposite numbers from other topic teams. More formal integration takes place during the inspection planning meeting during daily coordination sessions involving the inspection team lead and the topic team leads. During the data collection phase of the inspection, a formal team meeting is scheduled on a daily basis (typically at 4 or 5 p.m.), which provides a forum for the exchange of information between the topic teams.

It is essential that the integration process be instilled with the realization that the fundamental DOE protection philosophy is based on the concept of protection in depth—layers of protection applied in a manner that ensures that the failure of a single layer does not expose the protected asset. To be effective, layered protection requires the careful integration of protection layers and of the protection elements within each layer. In this sense, integration is the basic process through which OA ensures that the security interests at a particular facility are afforded the necessary degree of protection in depth. The formal part of this process is to: identify and characterize the priority security interests at a facility, test and evaluate the protection system elements that are critical to the protection of these interests, and analyze the impact of deficiencies in these critical system elements to determine the overall status of safeguards and security at the inspected facility.

Integration by the CMPC Topic Team

The CMPC program is an important part of the overall security system at a facility. This section provides guidelines to help inspectors coordinate their activities with other CMPC elements and with other topics. Classified matter protection is pervasive in nature, interacting with a number of the other inspection areas. This interdependence requires close coordination with other topic teams, particularly protective force, physical security systems (PSS), personnel security, cyber security, and protection program management (PPM).

Protective Force and Physical Security Systems

There is significant integration between the CMPC team and the protective force and PSS topic teams. Normally, the CMPC team reviews non-technical aspects of physical protection (for example, the presence of alarms and sensors, where required), whereas the technical aspects of physical protection (for example, alarm line supervision) are reviewed by the PSS team. Similarly, the CMPC team might review limited aspects of the protective force operations that relate directly to the CMPC topic (for example, repository checks by guards), whereas the protective force team would conduct detailed reviews of all aspects of protective force activities. Other interfaces with physical protection are addressed in Section 3.7 and 4.7.

Aspects of the physical protection program that the CMPC team would typically include within the scope of its review include:

- Physical protection during transfers
- Storage repository, vault, and vault-type room requirements
- Access controls at use and storage areas
- Physical control of documents in use
- Lock combination change procedures
- Repository checks.

When reviewing the above items during the inspection, physical protection concerns identified by the CMPC team should be communicated to the PSS or protective force teams as soon as practical so that their significance can be evaluated. For example, if repository check sheets indicate that guard checks are not being routinely performed after hours, the CMPC team should interface with the protective force team to determine what the guards' post orders and procedures require regarding repository checks. Similarly, if the location of sensors in a vault-type room appears to be blocked by tall shelving, the PSS team should be notified to possibly conduct comprehensive room sensor coverage tests.

Other examples of integration between the CMPC team and either the PSS or protective force teams include:

- Coordinating with the protective force team to obtain security incident reports that may indicate follow-up in determining issuance of infractions

- Learning from the protective force team the protective force procedures and practices for picking up, transporting, and storing classified matter awaiting destruction

- Coordinating with the protective force team to determine patrol schedules for checking classified matter stored outside of approved repositories, vaults, or vault-type rooms

- Integrating with the PSS team to determine which team might be conducting alarm sensitivity tests at vaults and vault-type rooms containing classified matter

- Determining from the PSS team the frequency of site alarm testing for vaults and vault-type rooms.

In special circumstances, the CMPC team might be required to review some elements normally handled by the PSS team. For example, the CMPC team may be required to review the alarm system in more detail if the physical security systems are not being inspected and if previous inspections indicate some alarm system deficiencies. Here, however, it is essential that the team include at least one member having the requisite PSS skills if highly technical or specialized PSS areas are to be inspected in depth. The addition of a PSS technical expert may also be required if a large number of vaults and vault-type rooms are inspected.

Personnel Security

At some facilities, security training relating to the protection and control of classified matter is an element of the overall security education program administered by the personnel security staff. In such cases, close coordination with the personnel security topic team is essential. The CMPC inspection team should coordinate with the personnel security team to determine whether the security education program incorporates materials to educate staff on their responsibility to control and protect classified matter and to report infractions. Additionally, because the CMPC team reviews the security infraction program, coordination with the personnel security team may include having that team check personnel security files on individuals who received infractions and verifying that the infraction records are maintained in those files.

Visitor control, including in particular foreign visits and/or assignments, and the security termination procedures also come under the personnel security topic. Issues identified concerning either visitor control or security terminations can have a direct impact on the CMPC topic due to potential unauthorized access to classified matter. Inspectors looking at "review and use" under control of Top Secret, Secret, and Confidential documents should coordinate with the personnel security topic team and should request assistance for such follow-up activities as checking security termination statements of departed personnel.

The CMPC team may elect to provide the personnel security team with a list of personnel supposedly having certain special access authorizations (for example, SCI access, weapons data sigmas) and have the team verify that those persons do have the required authorizations listed in their personnel security files.

Protection Program Management

Frequently, the PPM topic is inspected in addition to inspecting the management topic in CMPC. If inspectors reviewing CMPC management encounter any conditions that could be attributed to lack of management attention or inadequate oversight, such conditions should be reported to the PPM topic team for coordination. For example, failure to provide policies and procedures for generation, preparation, review and use of classified matter or CREM, the physical protection of classified documents or CREM, the lack of fully documented and approved vulnerability assessments for classified assets residing in non-standard open storage, or failure of self-inspections or surveys to detect and address existing problems in this area, should be

communicated to the PPM topic team for further investigation.

Likewise, coordination with the PPM team may be warranted if the CMPC team uncovers evidence that operations office oversight over special programs is lacking. Facilities with special programs must strike an appropriate balance between the need for tight controls (including the need to limit access to a minimum number of persons) and the need for oversight of CMPC for special programs. It must be determined whether operations office security managers have had adequate input into the planning and design of the protection strategy for special programs, as well as whether they have ample ongoing oversight of those programs.

Cyber Security

Cyber security inspections are conducted by the Office of Cyber Security and Special Reviews (OA-20). A cyber security team may or may not be operating on site at the time of a CMPC topic inspection. If the CMPC inspection team identifies a problem that requires cyber security expertise, but no OA-20 team is on site, the CMPC topic lead should coordinate with inspection management to obtain OA-20's help.

Cyber security and CMPC are closely related and have the common goal of protecting classified information, and the efforts of the CMPC and OA-20 teams must be coordinated to ensure that all pertinent elements are covered with minimal duplication of effort. Frequently, the CMPC team will note deficiencies in program implementation in areas where CMPC responsibilities overlap with cyber security responsibilities (for example, protection of CREM). Such deficiencies can often be traced to failure of facility management to assign responsibilities for all required security functions, or to confusion at the operational level as to which requirements apply. All such deficiencies should be reviewed from both the cyber security and information security perspectives to identify the root causes. For example, if the CMPC team discovers that insufficient resources are available for the training program, they may communicate that concern to OA-20, which should then devote more attention to the cyber security training programs. In this manner, the inspection team can better determine whether training resources are a sitewide problem. Similar considerations apply for corrective actions and self-assessment programs.

OA-20 usually reviews pertinent aspects of the generation and handling of computer-related documents, including storage media and printouts. Because the CMPC team also reviews document generation and handling, it frequently touches upon classified computing equipment (generally personal computers), facilities, and practices. Any cyber security items of concern here that may require follow-up should be communicated.

OA-20 also typically examines, where applicable, accountability of computer media and output as a part of its normal activities, and normally looks at more such media than does the CMPC inspection team. Sometimes a computer tape library has a stand-alone accountability system. Here, OA-20 may conduct front and back checks on that system, eliminating the need for the CMPC team to do so. Coordination is needed to ensure that the CMPC team knows of the accountability systems that OA-20 is reviewing, and that pertinent results regarding accountability are collected from that team.

Both OA-20 and the CMPC team usually review some aspects of the reproduction and destruction (degaussing or full destruction) of computer-related items, including hard disks, floppy disks, and other storage media. Again, close coordination and integration are needed to ascertain what each team will be reviewing in terms of reproduction and destruction to ensure that all facets of these areas are adequately inspected without duplicating effort, and to assure that the review results are exchanged between the teams.

OA-20 customarily reviews some aspects of the physical protection of computer-related items, including access to, specific need-to-know, and proper use and storage of media and printouts. However, when the CMPC team is reviewing these areas of document protection, they also frequently come upon classified computing equipment (generally personal computers), facilities, and practices. Items of concern that may require follow-up regarding physical security should be communicated.

OA-20 should be included in the initial planning and data collection phases if any special programs or SCIFs to be inspected involve the use of computers for classified processing. Coordination with the cyber security team is especially important when reviewing WFO programs in which the sponsoring agency includes cyber security as part of its activities. This will allow requests for topic team access to be responded to in a timely manner and thus allow the inspection to progress smoothly.

Another area for concern is the increasing importance of the protection provided sensitive information found on unclassified computer networks. While not directly related to the protection of classified matter, problems in the implementation and coordination of the unclassified cyber security program can impact site CMPC programs. Poor unclassified computer user security awareness can also be indicative of an overall lack of security awareness or deficiencies in the security education program itself. The failure to develop necessary unclassified cyber security procedures and plans can lead to the revelation that CMPC procedures and plans are also lacking. As the unclassified cyber security program matures and changes to meet new security threats, additional interfaces may be identified between the CMPC and unclassified cyber security programs.

This page intentionally left blank.

Section 9

ANALYZING DATA AND INTERPRETING RESULTS

Contents

Introduction

This section provides guidelines to help inspectors analyze data and interpret the results of data collection. The guidelines include information on the analysis process, including factors to consider while conducting an analysis. Information is also included on the significance of potential deficiencies, as well as suggestions for additional activities when deficiencies are identified. After completing each activity, inspectors can refer to this section for assistance in analyzing data and interpreting results and for determining whether additional activities are needed to gather the information necessary to accurately evaluate the system.

When analyzing the data collected on a particular aspect of the site security system, it is important to consider both the individual segments of the security system and the system as a whole. In other words, the failure of a single segment of a security system does not necessarily mean the entire security system failed. However, a number of relatively insignificant systemic deficiencies can point to a failure of the entire security system. This is why integration among topic teams is so important. It provides for a look at the "big picture" within the framework of the site mission when determining whether the overall security system is effective.

Data Review

Data review consists of sorting out and logically grouping all validated data collected for each subtopic during each phase of the inspection (remembering that data is collected during the planning process as well as the conduct phase). Although the topic team is generally aware of most of the data, not all team members will be familiar with all data collected. Therefore, it is important for the topic team to review data at the end of each day to begin to develop a comprehensive picture of how effectively the CMPC program meets requirements. This can be best accomplished while preparing for the daily inspection team meeting. In this way individual elements of the CMPC team can come together to discuss each validated data point, begin the process of analysis, and identify impact as it may exist at that point in time (recognizing that additional data may eliminate, mitigate, or increase the impact of a particular concern).

Generally, it is helpful to arrange the data according to positive or negative features. This will aid in clearly identifying strengths, weaknesses, and positive or negative trends. Proper organization and thorough review of all inspection data are essential to analysis and report preparation.

Analysis of Results

The process of analyzing results begins with the first document to be reviewed, briefing received, or person interviewed during planning. It is not completed until the final inspection report is disseminated. By recognizing this concept early in the inspection process, the topic team can enhance the completeness and usefulness of its analysis.

The information collected for each of the subtopics is reviewed to determine whether the overall CMPC program complies with the requirements in DOE orders. In addition to mere compliance, the analysis process involves the critical consideration by topic team members of all inspection results, particularly identified strengths and weaknesses or deficiencies, framed within the parameters of the site mission. Analysis should lead to a logical, supportable conclusion regarding how well the CMPC program is meeting the required standards and satisfying the intent of DOE requirements. A workable approach is to first analyze each subtopic individually. The results can then be integrated to determine the effects of the subtopics on each other and, finally, the overall status of the topic. As mentioned before, it is important to weigh the significance of a weakness or deficiency in light of the entire system.

If there are no deficiencies, or if those that are identified do not impact the rating, the analysis is relatively simple. In this event, the analysis is a summary of the salient inspection results supporting the conclusion that protection needs are being met. If compensatory systems or measures were considered in arriving at the conclusion, these should be discussed in sufficient detail to clearly establish why they counterbalance the identified deficiencies. Since some of these compensating measures may be from other security programs (that is, security systems or the protective force), these discussions should include input from other topic teams.

If there are negative findings, weaknesses, deficiencies, or standards that are not fully met, the analysis must consider the significance and impact of these factors. The deficiencies must be analyzed both individually and collectively, then balanced against any strengths or mitigating factors to determine their overall impact on the site security system's ability to meet DOE requirements and site mission objectives. Deficiencies identified in other topic areas should be reviewed to determine whether they have an impact on the analysis. Other considerations include:

- Whether the deficiency is isolated or systemic
- Whether the operations office or contractor management previously knew of the deficiency and, if so, what action was taken
- The importance or significance of the standard affected by the deficiency
- Mitigating factors, such as the effectiveness of other protection elements that could compensate for the deficiency
- The deficiency's actual or potential effect on allowing the loss, compromise, or unauthorized disclosure of classified information.

Findings

Inspection findings are the primary means of identifying those elements of the CMPC program that are having a significant negative impact on the effectiveness of the overall program. Topic teams are normally expected to exercise judgment in determining findings, omitting minor and non-systemic items, and limiting formal findings to items of significance. Where several findings address specific aspects of a requirement, the inspection team should determine whether a single rollup finding should be reported addressing that requirement. It is more important that the finding identify the specific nature of the deficiencies, and the finding should be clear whether the deficiency is specific to a location at the site or to a specific system.

Ratings

The conclusions reached through the analysis of the CMPC program inspection usually results in the assignment of a single rating for the topic. However, subtopic ratings may be required when more than one organization's CMPC program is inspected. It may also become necessary to assign ratings to individual subtopics to pinpoint the exact nature of the concerns related to a particular CMPC program. The topic team is responsible for assigning ratings; however, approval of final ratings rests with OA upper management.

Guidelines for assigning ratings are:

- Effective Performance – Assigned when the system (topic or subtopic) provides reasonable assurance that the identified protection needs are met; or other compensatory factors exist that provide equivalent protection; or the impact of any identified deficiency is minimal and does not significantly degrade the protection provided.

- Needs Improvement – Assigned when the system only partially meets identified protection needs; or provides questionable assurance that the identified protection needs are met; or identified deficiencies are only partially compensated for by other systems or compensatory factors, and the resulting deficiencies degrade the effectiveness of the system.

- Significant Weakness – Assigned when the system being inspected does not provide adequate assurance that the identified protection needs are met, there are no compensating factors to reduce the impact of identified deficiencies on system effectiveness, and the deficiencies seriously degrade the effectiveness of the system.

Interpreting Results

Program Management

During an inspection, the management program is not to be reviewed based on any particular view of how a management program should function. Rather, inspectors should take a results-oriented approach and examine the management program in light of the effectiveness of the program in protecting classified information, and in terms of compliance with DOE requirements. Thus, the primary purpose behind reviewing the management program is not to evaluate management itself as adequate or inadequate, but to use the management review to identify root causes of deficiencies observed in the organization's implementation of DOE policy during the inspection of other CMPC program areas. Additionally, deficiencies identified in the management review may cue inspectors to examine more closely corresponding areas. For example, if the management inspection reveals that procedures do not contain recent DOE Headquarters guidance about accountability records, inspectors may want to redouble their efforts in examining these records to determine whether they are being completed properly. Conversely, if the results of inspection activities for any requisite document accountability systems indicate that findings identified during the previous OA inspection have not been adequately addressed, inspectors may wish to closely examine the management tracking system and corrective action plans to determine why.

Planning, Organization, and Oversight. Deficiencies in any of the management areas of planning, organization, oversight, or human resources can seriously affect the ability of the CMPC program to adequately protect DOE classified security interests because these areas establish the framework within which the organization implements DOE policies and local procedures. If significant problems in any of

these areas are discovered, inspectors should attempt to determine whether the management deficiencies have resulted in possible vulnerabilities in the protection of classified information. Of special importance is the existence of a program of annual reviews of the CMPC program. The absence of any means for the site CMPC program manager to determine the status of the program results in problems not being identified or corrected. Additionally, if deficiencies are identified, inspectors should attempt to determine whether key managers were adequately informed of the status of tracking and completion of corrective actions.

Foreign Ownership, Control, or Influence. Systemic deficiencies in the FOCI determination process that would result in the placement of classified information within an organization that had not received appropriate DOE facility approval or was owned, controlled, or influenced by foreign governments, individuals, or organizations are very significant and pose undue risk to the protection of such information. If such deficiencies are noted, the inspector should coordinate with inspectors reviewing the safeguards and security survey program to determine the effectiveness of other aspects of the facility approval process, survey oversight, and the overall impact on protection effectiveness. This would include the existence of a security plan and the successful completion of a satisfactorily rated survey.

Security Infractions. Serious deficiencies in the program to detect infractions can have a significant impact on the ability of the CMPC program to protect classified information and reduce the potential of compromise. A comprehensive program to detect and monitor infractions is a primary means of determining whether persons are following required procedures, whether the proper corrective actions are taken, and whether there are deficiencies in the security education program. An established program to train staff in their security responsibilities represents the primary means by which security awareness is heightened, deficiencies are eliminated, and infraction frequency is reduced.

Deficiencies in other aspects of an organization's infraction program must be analyzed in light of the degree of deficiency and the effect on the program's ability to encourage good security performance and to detect and correct inadequate performance. The complete absence of any program element seriously hampers the program's ability to achieve its intended goal.

Control of Secret and Confidential Documents

Review and Use. Deficiencies in procedures and practices for reviewing and using classified documents that would result in unauthorized access are significant. Some instances of unauthorized access will have more impact than others. For example, deficiencies that would allow uncleared persons access to classified information, or "L" cleared personnel access to Secret/Restricted Data weapons data would normally be considered more significant than sloppy document practices in an area accessible only to appropriately cleared personnel. If access control procedures appear to be inadequate or practices appear sloppy, inspectors should investigate further to determine the actual likelihood that classified documents are not being adequately protected.

Deficiencies in checkout procedures and practices could also affect the protection of classified information. Such procedures are relied on to ensure the proper transfer and accountability of classified documents and to prevent access by persons no longer authorized or needing access. While improper practices related to dead or disabled personnel probably do not significantly affect security, similar practices applied to transfer or non-prejudicial termination of personnel provide more potential for abuse. The insider threat is increased by inadequate outprocessing of persons whose access authorizations have been terminated for cause, or whose employment has been involuntarily terminated.

Physical Protection and Storage. Systemic deficiencies in physical protection and storage of classified documents that could result in documents being left unattended and accessible to uncleared persons (or persons without the appropriate need to know) are very significant. Such deficiencies could result in the compromise of information. The importance of effective physical protection has been made more significant by the advent of modified accountability. If such deficiencies are noted, inspectors should devote additional attention to the effectiveness of complementary systems (especially access controls, security infraction programs, and inventory practices) to determine the likelihood that classified information may be compromised.

Deficiencies that do not lead directly to the potential for uncleared or unauthorized persons to gain access to classified information (for example, failure to change a lock combination when needed) are less significant. If a small number of deficiencies are noted and there are no discernable systemic deficiencies, inspectors may conclude that the deficiencies are isolated instances and the impact is minimal. A significant number of errors, however, may indicate a lack of management attention, ineffective audit procedures, lack of adequate training programs, or inadequate resources. If a significant number of physical protection deficiencies are identified, the inspectors should consider reviewing the relevant aspects of the management program to determine the root cause.

Document Generation. The lack of, or failure to follow, document generation procedures could result in documents not being entered into accountability or not marked at all. Such deficiencies are very significant and could result in documents not being adequately protected. If such deficiencies are noted, inspectors should devote additional attention to reviewing data indicating the effectiveness of complementary systems (especially physical protection, storage practices, and access controls) to determine the overall impact on protection effectiveness.

When inspectors review a large number of documents, they often encounter incorrectly marked documents or other procedural errors. Minor discrepancies in document marking, page counts, or the use of cover sheets are not easily exploited by adversaries if the documents are properly controlled (including formal accountability, when required) and afforded adequate physical protection. Thus, inspectors may conclude that the deficiencies are isolated instances and the impact is minimal if:

- The percentage of incorrectly marked documents is small.
- There is no discernable systemic procedural or awareness deficiency.

A significant number of errors, however, may indicate a lack of management attention, ineffective audit procedures, lack of adequate training programs, or inadequate resources. If a significant number of errors is identified, a review of the relevant aspects of the management program should identify the root cause.

Receipt and Transmittal. Deficiencies in document receipt and transmittal can represent significant weaknesses in controlling classified matter. Deficiencies could result in the loss or unauthorized disclosure of classified documents, classified matter not being adequately protected, and documents not being entered into accountability.

If deficiencies are detected in the receipt, transmittal, intra-site transfer, or hand-carrying of classified documents, inspectors should take whatever actions are needed to determine the full extent of the problem. They may need to use additional inspection techniques, including performance testing, observation of additional iterations of applicable procedures, or direct staff interviews. Inspectors should also carefully review any complementary systems that may affect protection effectiveness.

Reproduction. Widespread problems in the reproduction of classified documents can indicate

systemic deficiencies in the control of classified documents. These deficiencies could result in classified documents being vulnerable to loss or compromise. Further, the failure of site personnel to follow prescribed procedures could indicate that the security awareness training program is not fully effective. If deficiencies are detected in the reproduction of classified documents, inspectors should determine the full extent of the problem, using additional inspection techniques such as performance testing and management interviews to determine the root cause. Inspectors should also carefully review any complementary systems (especially physical controls) that may mitigate identified concerns.

Destruction. With the advent of modified accountability, the physical protection of classified waste and the effectiveness of destruction devices are of critical concern. Systemic deficiencies in these areas of document destruction could result in inadvertent disclosure of classified information to unauthorized personnel, even if for only brief periods of time. If such deficiencies are noted, inspectors should devote additional attention to the effectiveness of complementary systems (especially physical protection, storage practices, and access controls) to determine the overall impact on protection effectiveness. The window of opportunity available to potential adversaries should also be considered.

A lack of procedures or a pattern of deficiencies in policy implementation or understanding may indicate a broader lack of management attention, inadequate training programs, or inadequate resources. If a significant number of deficiencies are identified, inspectors should consider reviewing the relevant aspects of the management program to determine the root cause.

Accountability. Though few sitewide document accountability systems are now found within the Department, most classified WFO programs and SAPs require accountability systems. Since these special programs include some of the most sensitive information that DOE is charged with protecting, missing documents or documents not in accountability are a serious problem. Missing documents pose an obvious problem—the system has not adequately protected them, and they may have been lost, stolen, or compromised.

Missing documents or documents not in accountability identified during review of a sample of any accountability system are indicators of similar problems in the entire population of documents. While individual deficiencies of this nature are significant in themselves, other factors should be considered in evaluating their impact on the entire accountability system and document population. Facts to consider include whether the deficiencies are distributed throughout the sample or concentrated in a single subaccount; whether the deficiencies involve old, archived documents or newer documents containing current information; and whether the deficiencies reflect inadequate procedures, sloppy practices, or insufficient or ineffective oversight.

Deficiencies such as incomplete documentation on documents and incomplete or incorrect data in accountability records may also be significant, particularly if they are common and result in incomplete document audit trails. Often, enough information is present in the documentation and accountability data to positively identify the document. In such cases, the significance of these types of deficiencies diminishes unless they indicate haphazard or sloppy accountability record-keeping.

Control of Top Secret Documents

Top Secret Classifiers. The Top Secret classifiers assume the lead role in the proper classification of Top Secret documents, and errors or omissions on their part can degrade the protection afforded Top Secret information. If deficiencies are found, inspectors should pursue them to determine their root causes (for example, poor training or inadequate oversight) and the actual impact on the protection of Top Secret information.

Markings and Forms. Significant deficiencies in document marking, such as documents not marked at all or numerous marking errors or omissions, are significant. Occasional minor marking errors may not have a serious impact on information protection. However, Top Secret documents are so sensitive, and many of the accounts are so small, that there really should be no marking errors. If significant or numerous marking deficiencies are found, inspectors should devote additional attention to determining the effectiveness of complementary systems (such as physical protection, storage, and access controls) to determine the overall impact on protection effectiveness. Additionally, the training, or lack thereof, given to staff handling Top Secret matter should be reviewed to determine whether it is a factor contributing to the deficiencies.

Receipt and Transmittal. Systemic deficiencies in Top Secret document receipt and transmittal would represent significant weaknesses in the control of very sensitive information, with potentially serious implications for national security. Deficiencies could result in the loss of classified documents and Top Secret documents not receiving adequate protection.

If deficiencies are detected in the receipt and transmittal of Top Secret documents, the full extent of the problem, as well as the problem's root cause (for example, lack of procedures or training), must be determined so that the facility can implement corrective measures immediately. This may require use of additional inspection techniques such as specially developed performance testing. Additionally, inspectors should carefully review other aspects of the Top Secret protection system to determine whether deficiencies are mitigated by other system elements.

Reproduction and Destruction. If deficiencies are noted in the reproduction or destruction of Top Secret documents, the root cause of the problem must be promptly determined. Additional inspection techniques such as performance testing may indicate the exact nature of the problem (for example, lack of procedures or training). Further, the site acquisition process for reproduction and destruction equipment must be considered to determine whether management is ensuring that only appropriate items are being used. Inspectors should also carefully review all other aspects of the Top Secret protection system to identify any possible mitigation.

Physical Protection and Storage. Any indications that the physical protection of Top Secret documents could result in documents being left unattended and accessible to uncleared persons (or persons without the appropriate need to know) are very significant. Such deficiencies could result in compromise of information and have grave consequences. In these cases, inspectors should devote additional attention to determining the effectiveness of complementary systems (especially access controls, security infraction programs, and inventory practices) to determine the overall impact on protection effectiveness.

Deficiencies that do not lead directly to the potential for uncleared or unauthorized persons to gain access to classified information (for example, failure to change a lock combination within the required interval) are less significant but are still a matter of concern because of the particularly sensitive nature of Top Secret documents. Management of the security awareness training program, as well as program procedures and training of program officials, should be reviewed to determine the root cause.

Accountable CREM

As noted in Section 8, deficiencies in procedures and practices involving accountable CREM may indicate weak processes for assuring that requirements flow down appropriately through the organization. This area is normally addressed by the PPM topic team.

Deficiencies that could result in unauthorized access to CREM are significant, especially if they would allow unauthorized access to the information contained in the media. The considerations for determining significance are

as described above under "Control of Secret and Confidential Documents."

Control of Classified Materials

Marking. Deficiencies in marking classified material that would result in the inability to identify an item as classified would be significant. Marking provides the only identification and notification that an item requires the special protection afforded classified matter. When required, marking the serial number or other unique identifier provides the only reliable method of accounting for individual items.

A systemic failure to properly (or adequately) mark classified materials could indicate inadequate protection of the material if not compensated for in other ways. As discussed previously, some classified materials do not lend themselves to marking in the normal manner, and some facilities may use alternative approaches (which should be approved by DOE). In cases where materials are not marked, the entire protection system associated with the material should be evaluated to determine the real impact on the protection being afforded the material.

Accountability. Missing material and material not in accountability are both significant problems. Because the loss of materials not in accountability would not normally be detected, there is no opportunity for damage assessment or damage control. Further, materials for which no one is accountable are less likely to receive the same level of care and protection as materials for which someone is accountable.

Material identified as missing or as not in accountability may indicate similar problems in the entire population of materials. While individual deficiencies of this nature are significant in themselves, other factors should also be considered in evaluating their impact on the entire accountability system and materials population. Factors to consider include whether the deficiencies reflect inadequate procedures, sloppy practices, or insufficient or ineffective oversight.

Deficiencies involving inaccurate data in accountability records or, more frequently, delays in updating accountability records when an item is moved or undergoes some other change, may not be extremely significant, depending upon their effect on maintaining positive accountability of each item. For example, slow item-location updates in a production control system may make it difficult and time-consuming to locate a particular item on short notice, but does not really indicate serious loss of control of the item. If, however, inaccuracies in the accountability records are systemic and result in loss of adequate control of materials, that is a more significant problem.

Physical Protection and Storage. Deficiencies identified during review of physical protection and storage of classified materials have essentially the same impacts as those for classified documents. However, the relatively open environment of material production areas magnifies the impact of concerns about physical protection.

Special Programs and SCIFs

The specific deficiencies identified during the review of a special program are, for the most part, interpreted in the same manner as other elements of information security (that is, whether the facility protects the classified matter through reliable accountability systems when required, and whether there is an effective program to ensure that classified matter is adequately identified, marked, and handled to minimize the opportunity for compromise). For non-SCI programs, the guidelines presented for control of Secret and Confidential documents, control of Top Secret documents, and control of classified materials are generally applicable to evaluating the impact of identified deficiencies. Though programs in SCIFs follow different guidelines, the impact of any identified concern must be measured against the sensitivity of the classified information.

Deficiencies involving management and oversight should be given special attention.

Programs found to be outside of security oversight are a particular concern and frequently warrant immediate attention. Such deficiencies may indicate systemic management issues that transcend the CMPC topic and impinge upon the facility's management and oversight. Such deficiencies should be thoroughly reviewed, considering such factors as operations office "ownership" and oversight of special programs and SCIFs, their proper registration, any classified processing system (for example, computers and facsimile machines) approval and accreditation, and formal approval of security plans and procedures in place before commencing classified work.

Consideration of Integrated Safeguards and Security Management

ISSM provides a useful diagnostic framework for analyzing the causes of identified deficiencies. For example, inspectors may find that a required action is not being completed. Upon further investigation, the inspectors may determine that the reason is that responsibility for completing the required action was not clearly designated. This situation may indicate a weakness related to line management responsibilities. In such cases, the inspectors would cite the deficient condition (i.e., the failure to complete the required action) as the finding and reference the requirement. In the discussion and opportunities for improvement, however, the inspectors may choose to discuss the general problem with assignment of responsibilities as a contributing factor.

As part of the analysis process, OA inspectors should review the results (both positive aspects and weaknesses/findings) of the review of CMPC in the context of ISSM. Using this diagnostic process, inspectors may determine that a number of weaknesses at a site or particular facility may have a common contributing factor that relates to one or more of the management principles. For example, a problem in classified document control within a particular facility could indicate that line management had not fully accepted its responsibility for security and had not established and communicated expectations to the workforce and held personnel accountable for performance. In such cases, the analysis/conclusions section of the CMPC report appendix could discuss the weaknesses in management systems as a contributing factor or root cause of identified deficiencies.

This page intentionally left blank.

APPENDIX A

PERFORMANCE TEST SCENARIOS AND SAMPLE PERFORMANCE TEST PLANS

Contents

APPENDIX A

PERFORMANCE TEST SCENARIOS AND SAMPLE PERFORMANCE TEST PLANS

PERFORMANCE TEST SCENARIOS

This section describes some of the performance test scenarios commonly used in reviewing the Classified Matter Protection and Control (CMPC) subtopics. It is recognized that the scenarios provided are not all-inclusive and that other equally useful ones may exist. Organized by subtopic area, the scenarios provided here include at least one "generic" scenario, followed in some instances by variations of the same scenario. The generic scenarios are meant for ready inclusion in most inspection guides and can be employed at the majority of sites inspected. The variations are meant to address a different situation or set of site-specific conditions/procedures, or to test a slightly different aspect of a given subtopic area.

Document Generation Test

Objective

To determine whether personnel responsible for generating classified documents are doing so in accordance with U.S. Department of Energy (DOE) order requirements.

Scenario

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

Document Marking Test

Objective

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

Scenario

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

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

Front Check

Objective

To evaluate the accuracy of the document accountability system and determine whether documents are marked in accordance with DOE requirements.

Scenario

The inspection team selects a computer-generated random sample of documents listed on the inspected organization's accountability records. Selected documents are then assembled and reviewed at a single, central location or at their storage locations, as appropriate. The inspection team examines each document to ensure that it is the item described in the accountability records. Additionally, each document is checked for markings, documentation, dates, titles, page counts, cover sheets, and other applicable requirements to determine compliance with DOE orders. Each repository is also inspected for compliance with DOE storage requirements.

Back Check

Objective

To determine whether accountable classified documents on hand are properly entered into accountability and properly documented and marked.

Scenario

The inspection team selects and visits a sample of document storage locations (or a sample of document custodians). At each location visited, accountable documents are selected and checked to verify that they are properly described and reflected in accountability records. Markings, handling procedures, and proper storage are also checked. Concurrently, custodians are questioned about their specific responsibilities, and repositories are examined for compliance with DOE requirements. As applicable, classified parts are selected and checked for proper marking and storage.

Offsite Cross-Check

Objective

To verify that documents sent off site can be produced, or their disposition determined, at the receiving facility.

Scenario

Inspection team members obtain a sample of transmittals for classified documents recently mailed (e.g., in the past two years) to a DOE facility scheduled for inspection (most easily accomplished at the DOE Headquarters planning meeting, where transmittal forms on documents recently returned from DOE Headquarters to the facility can be obtained). During the inspection of that facility, personnel are asked to produce (1) the documents themselves, (2) their destruction forms, or (3) their transmittal slips.

Intrasite Cross-Check

Objective

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

Scenario

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

Custodian Receipt

Objective

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

Scenario

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

Variations:

(1) Send to a test participant a simulated Secret document that was incorrectly transmitted, was incorrectly or incompletely marked, or is missing pages. Verify his/her response (e.g., to return the document, issue an infraction, or initiate other action).

(2) Prepare a classified document to be sent off site through the classified mail. The document prepared should indicate a classification level/category that the receiving facility is not authorized to accept. Verify the test participant's response.

Transmittal/Onsite Transfer

Objective

To determine whether classified matter is transmitted and received within a site in accordance with DOE requirements.

Scenario

A sample of personnel who normally transmit classified documents is selected for testing. Each test participant is given a simulated Secret document and asked to package it and prepare the appropriate paperwork to send it to an offsite classified mailing address. If personnel possess document hand-carry

authorizations, local procedures for hand-carrying classified documents off site are reviewed, records of authorizations are inspected, and a sample briefing for hand-carrying is requested.

Variation: As an alternative to the above tests, transfer procedures can be reviewed by tracking an accountable document from its receipt at the U.S. Postal Service (USPS) until it reaches its final custodian. This includes receipt by the central mailroom, transfer to Document Control, entry into the accountability system, courier transfers, any Field File Station procedures, and custodian receipt, as applicable.

Reproduction

Objective

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

Scenario

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

Variations:
(l) Use the same scenario but instead of a typical paper document, use microfiche, viewgraphs, blueprints, or any other type of medium containing classified information.
(2) Carry out the scenarios at the inspected site's print shop, photo lab, or other facility tasked with reproducing classified information.
(3) Submit improperly/incompletely marked simulated classified documents for reproduction and determine whether discrepancies are noted.

Destruction

Objective

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

Scenario

The inspection team selects a sample of personnel to be tested who are normally responsible for the destruction of classified documents. Test participants are given a simulated (or actual) Secret document and instructed to destroy it using their normal procedures. Procedures for the transfer of the document, adjustments to accountability records, and the actual destruction are observed. Also, specific procedures for destroying electronic media are reviewed, and the test participants' knowledge of when to employ degaussing is determined. DOE approval for specific models of destruction equipment is verified, as is the size of the destroyed document residue.

Variation: Use the same scenario as above but use a non-paper medium. If microfiche is being destroyed, verify specific techniques used.

Repository Check

Objective

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

Scenario

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

Document User Awareness

Objective

To determine whether those responsible for attending/protecting classified documents in use or storage are attentive to unauthorized individuals' admittance into security areas.

Scenario

The inspection team obtains a "red" badge for a cleared person (possibly an Office of Independent Oversight and Performance Assurance (OA) administration team member) and have that person wear the badge while wandering into and around an open storage area or "Q" access-only security area. Any actions to challenge that person will be noted. [Note: Scenario requires safety plan and coordination with the protective force.]

Storage Area Entry

Objective

To determine whether a facility's Central Alarm Station (CAS) routinely verifies the identities of those requesting access to classified storage areas.

Scenario

The inspection team has an unauthorized person request that the facility CAS put security area alarms in access mode, and then determine whether the requestor's identity is first verified by the CAS before actuating access (consistent with site-specific procedures). [Note: Scenario requires safety plan and coordination with the protective force.]

Emergency/Special Procedures

Objective

To determine whether appropriate site-specific procedures for emergency evacuation of a security area are followed.

Scenario

Inspection team members direct facility personnel to conduct an emergency evacuation according to their normal procedures. Such an evacuation should be carried out only in easily controlled environments, and facility personnel should be informed that it is only a test. Appropriate site-specific procedures for emergency evacuation of a security area will be noted. [Note: Scenario requires safety plan and coordination with the protective force.]

Search Procedures

Objective

To ascertain whether the attempted unauthorized removal of classified media results in detection and appropriate response by the protective force.

Scenario

A composite adversary team or facility team member attempts to exit a portal with plainly marked (simulated) classified documents or electronic media in his/her hand or briefcase. Team members determine whether the protective force observes and appropriately responds to the situation. [Note: Scenario requires safety plan and coordination with the protective force.]

SAMPLE PERFORMANCE TEST PLANS

Classified Matter Protection and Control (CMPC)

Document Accountability Performance Test Plan – Front Check

DOE San Diego Operations Office

Objective

To evaluate the accuracy of the DOE San Diego Operations Office (SDO) document accountability system and to determine if documents are protected, stored, and marked in accordance with DOE requirements.

System Description

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

Sampling Technique

SDO is unable to provide the total number of documents contained in active holdings. They estimate 2,400 control tickets are in use to reflect active holdings, but some tickets represent multiple copies of documents.

OA will select a random sample of 200 documents by computer generating a list of random numbers reflecting document control tickets. Corresponding control tickets will then be examined and documents reflected on the selected tickets will be used as the inspection sample for the front check of the DOE SDO accountability system.

Scenario

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

Safety Plan

Not required.

Document Accountability Performance Test Plan – Back Check

DOE San Diego Operations Office

Objective

To determine whether accountable classified documents on hand at SDO repositories are in accountability, properly documented, marked, and stored.

Sampling Technique

SDO will provide a list of document custodians and repositories currently used to store accountable documents. OA will randomly select custodians and repositories from which a sample of 200 documents will be indiscriminately drawn and back checked to ensure custodian holdings are entered into accountability.

Scenario

Inspection team members will visit a sampling of Secret and Confidential storage locations in use at SDO. Classified matter at each location will be checked for proper marking and storage. A sample of 200 Secret documents will be selected from locations holding Secret documents. Each will be checked to ensure it is described in accountability records.

Safety Plan

Not required.

Document Accountability Performance Test Plan – Front Check

NUCO-El Cajon BDAS System

Objective

To evaluate the accuracy of the NUCO-El Cajon Barcode Document Accountability System (BDAS), and to determine if documents are protected, stored, and marked in accordance with DOE requirements.

System Description

The document accountability system is maintained using a computerized bar code system. NUCO-El Cajon personnel advise no computer enumeration of a master list of active holdings by document number can be generated, nor can the system generate a random sample of documents. The system can generate a master list of active documents by custodian.

Sampling Technique

NUCO-El Cajon will provide the total number of active documents contained in the BDAS. OA will computer-generate a random sample of 200 numbers which will then be used to select specific sample documents from the BDAS by matching the random number to the list of document custodians and their respective holdings.

Scenario

The inspection team will select a sample of 200 Secret documents listed in the NUCO-El Cajon accountability system. Selected documents will be reviewed at their storage locations, or at a central location as appropriate. Each will be checked to ensure that it is the item described in the accountability records. Additionally, documentation, markings, dates, titles, and pages will be checked to determine compliance with DOE requirements. Each repository will also be inspected for compliance with DOE storage requirements.

Safety Plan

Not required.

Document Accountability Performance Test Plan - Back Check

NUCO-El Cajon BDAS System

Objective

To determine whether accountable classified documents in NUCO-El Cajon repositories are in accountability, properly documented, marked, and stored.

Sampling Technique

NUCO-El Cajon will provide the total number of repositories used to store active BDAS documents. OA will computer-generate a random sample of 25 numbers, which will then be used to select specific repositories to be sampled by matching the random number to the list of repositories.

Scenario

Inspection team members will visit each repository identified in the random sample selection. Classified matter at each location will be checked for proper marking and storage. Additionally, a sample of accountable documents will be selected from each repository. Each will be checked to ensure it is properly described and reflected in accountability records.

Safety Plan

Not required.

Document Accountability Performance Test Plan – Front Check

NUCO-El Cajon NDT System

Objective

To evaluate the accuracy of the NUCO-El Cajon Non-Destructive Testing (NDT) document accountability system for the laboratory located in Building 724, and to determine if classified X-rays are protected, stored, and marked in accordance with requirements.

System Description

NUCO-El Cajon personnel advise that document accountability is maintained using a series of log books, some of which have been reduced to microfilm. No master list or computer assistance is available.

Sampling Technique

NUCO-El Cajon will provide the total number of logbooks (both books and microfilmed logs) used to maintain NDT #1 accountable holdings. OA will computer-generate a random sample of numbers, which will then be used to select specific logbooks. Sample documents will then be determined by computer-generating random numbers for each selected log book and identifying the specific accountable holding each number represents.

Scenario

The inspection team will use the random sample of 100 Secret documents listed in the accountability logbook system used by the NDT center in building 711. Selected documents will be reviewed at their storage locations, or at a central location as appropriate. Each will be checked to ensure that it is the item described in the accountability records. Additionally, documentation, markings, dates, titles, and pages will be checked to determine compliance with DOE requirements. Each repository will also be inspected for compliance with DOE storage requirements.

Safety Plan

Not required.

Document Accountability Performance Test Plan – Back Check

NUCO-El Cajon NDT #1 System

Objective

To determine whether accountable classified X-rays on hand in the NUCO-El Cajon NDT repositories are in accountability, properly documented, marked, and stored.

Scenario

Inspection team members will visit the document storage locations used by the Non Destructive Testing Center located in building 711. Classified matter will be checked for proper marking and storage. Additionally, a sample of 100 Secret documents will be selected from NDT location #1 holdings. Each will be checked to ensure that it is properly described and reflected in accountability records.

Safety Plan

Not required.

Document Accountability Performance Test Plan – 100% Audit

WB Security Incorporated

Objective

To evaluate the accuracy of the WB Security Incorporated (WB) document accountability system, and to determine if documents are marked in accordance with DOE requirements.

Scenario

The inspection team will review all accountable documents listed in the WB El Cajon accountability system. Documents will be reviewed at their storage locations. Each will be checked to ensure that it is the item described in the accountability records. Documentation, markings, dates, titles, and pages will be checked to determine compliance with DOE requirements. Additionally, each repository will be inspected for compliance with DOE storage requirements, and to ensure all accountable documents have been entered into the WB accountability system.

Safety Plan

Not required.

Material Accountability Performance Test Plan – Front Check

NUCO-El Cajon Parts System

Objective

To determine if the NUCO-El Cajon Parts accountability system accurately reflects Secret parts on hand and to ensure that all classified parts are protected in a manner consistent with DOE requirements.

System Description

Parts accountability is maintained using a computerized system. NUCO-El Cajon personnel advise that computer enumeration of a master list of accountable parts can be generated. However, the system cannot generate a random sample of documents.

Sampling Technique

NUCO-El Cajon will provide the total number of accountable parts. OA will computer-generate a random sample of 100 numbers, which will then be used to select specific sample documents from the system by matching the random number to the computerized list of parts.

Scenario

The team will visit locations where each selected part is located to verify that the accountable parts are actually on hand. Disassembly of major assemblies is not contemplated.

If time permits, team personnel will also visit selected locations where any unaccountable classified parts are located to ensure that all parts are stored or protected as required by applicable directives.

Safety Plan

Not required.

Material Accountability Performance Test Plan - Back Check

NUCO-El Cajon Parts System

Objective

To determine if the NUCO-El Cajon Parts accountability system accurately reflects Secret parts on hand and to ensure that all classified parts are protected in a manner consistent with DOE requirements.

Scenario

The inspection team and site representatives will visit plant production and parts storage locations and identify 100 Secret parts. Team and plant personnel will then check each to ensure it is properly described and reflected in accountability records. Classified parts selected will also be checked for proper marking and storage.

Team personnel will also record pertinent information identifying accountable classified documents controlled under the NUCO El Cajon Parts System to be used as a back check of the effectiveness with which the NUCO El Cajon Parts System controls documents. Space for recording accountable documents has been provided on the data sheets designed for recording pertinent NUCO El Cajon Parts System information (See attached Performance Test for NUCO El Cajon Parts System Document Back Checks).

If time permits, team personnel will also visit selected locations where unaccountable classified parts are located to ensure all parts are stored or protected as required by applicable directives.

Safety Plan

Not required.

Classified Transmittal Performance Test Plan

USPS Receipt/Transmittal

Objective

To determine if classified matter is transferred to and from the USPS at Warren Heights, California, in accordance with requirements.

Scenario

Transfer procedures will be reviewed by tracking certified and registered mail from its receipt at the U.S. Post Office until it reaches its final custodian within El Cajon. Observation will include receipt from USPS personnel; transportation to El Cajon; delivery to DOE-SDO, NUCO-El Cajon and WB Security; entry into the appropriate accountability system; and custodian receipt procedures, as applicable. Should any required actions not occur during the OA inspection, site personnel will be asked to perform actions on simulated classified matter.

Safety Plan

Not required.

Classified Transmittal Performance Test Plan

Site Transfers

Objective

To determine if classified matter is transmitted within the confines of the El Cajon Plant in accordance with DOE requirements, and to determine if classified information is receipted only to individuals with a valid need to know.

Scenario

Inspection team members will observe NUCO-El Cajon personnel receipting and internally distributing classified matter. Should any required actions not occur during the inspection, site personnel will be asked to perform actions on simulated classified matter.
The inspection team will interview El Cajon Plant employees and review operating procedures to ensure

that internal distribution and hand-carry procedures meet DOE requirements. A sampling of procedures for transfer of classified documents will be reviewed and observed as such transactions occur during the inspection. If necessary, simulated documents will be placed in local distribution and tracked to determine site procedures.

Special attention will be given to procedures for handcarrying classified matter off site. A sample briefing will be requested, local procedures will be reviewed, and records of hand-carry authorization will be inspected.

Safety Plan

Not required.

Classified Document Destruction Performance Test Plan

Objective

To determine if classified documents are destroyed in accordance with DOE directives.

Scenario

Inspection team members will observe DOE-SDO, NUCO-El Cajon, and WB Security El Cajon personnel destroying classified matter, using routine local procedures. Should destruction of classified not be planned during the inspection, site personnel will be asked to describe procedures or perform actions on simulated classified matter.

Safety Plan

Not required.

Reproduction of Classified Documents Performance Test Plan

Objective

To determine if accountable classified documents are reproduced in accordance with DOE directives.

Scenario

Personnel normally charged with duplicating classified will be interviewed and observed reproducing accountable classified documents. Should the reproduction of accountable classified not actually occur during the inspection, site personnel will be asked to perform actions on simulated classified matter.

Facilities authorized for the reproduction of classified will also be inspected to ensure that they meet requirements and are properly posted.
Special emphasis will be placed on reviewing NUCO-El Cajon Printing Plant procedures to ensure that all

DOE requirements for the safeguarding of classified information are implemented.

Safety Plan

Not required.

This page intentionally left blank.

APPENDIX B

FORMS AND WORKSHEETS

Contents

APPENDIX B

FORMS AND WORKSHEETS

DOCUMENT REQUEST LIST

1. Table of organization/document control sections including names, telephone numbers, and building/room numbers of Classified Matter Protection and Control (CMPC) managers, supervisors, and key CMPC staff.

2. Standard operating procedures or other local guidance dealing with program management, physical security of classified documents, control of classified documents (Top Secret and Secret, as applicable), sensitive compartmented information facilities, special access programs, the security infraction program, and Foreign Ownership, Control, or Influence (FOCI).

3. Site safeguards and security plan(s).

4. Operations security assessments and operations security reviews.

5. Vulnerability assessments.*

6. Survey reports* and status of corrective actions.**

7. Self-assessment reports and subsequent corrective action reports.*

8. Infraction records for the past 24 months.

9. Documentation dealing with approved, pending or requested exceptions relating to the CMPC program.**

10. Classified mailing address.**

11. Number of classified document inventories performed over the last 18 months.

12. Number of special access programs, including those in the Sensitive Compartmented Information Facilities (SCIFs) and out of the SCIFs; include the responsible individuals, number of documents, and the responsible program office that can grant access.

13. All local policies and procedures regarding access control to vaults and vault-type rooms that contain classified material.

---

* Check in applicable facility files.

** Check Safeguards and Security Information Management System database.

14. Site map showing the locations of all vaults and vault-type rooms in which classified documents and material are stored.

15. Description of alarm systems used to protect the vaults and vault-type rooms.

For Top Secret document accounts:

1. Description of Top Secret control programs and names of responsible individuals.

2. Location of Top Secret repositories. (map if possible)

For Secret matter under traditional accountability:

1. Total number of lost/unaccounted for classified for all accounts.

2. List of each accountability system(s).

3. Number and types of classified materials, classification levels, and their production and storage locations. Map/diagram of storage and production locations.

4. Number of document custodians and/or accountability center/stations (names, organizations, locations, and phone numbers).

5. Accountability Center/Station access procedures.

PLANNING MEETING TASK CHECKLIST

___ Review and analyze documentation

___ Identify site security interests

___ Identify information program missions

___ Identify appropriate threat level

___ Characterize the CMPC program

___ Identify questions, issues, and discrepancies

___ Resolve questions, issues, and discrepancies

___ Select subtopics and inspection focus/emphasis

___ Coordinate and integrate with other topic teams

___ Select data collection activities

___ Prioritize data collection activities

___ Assign data collection tasks to team members

___ Schedule data collection activities

___ Plan data collection activities

___ Identify sample sizes and configurations for all activities

___ Select samples (as required)

___ Identify support requirements for site visit

___ Communicate and arrange internal support requirements

___ Communicate external support requirements to site representatives/point(s) of contact

___ Prepare and submit inspection guide

___ Prepare and submit report outline input

___ Prepare and submit inspection plan/action plan input

___ Prepare performance test/safety plans

___ Prepare and deliver management briefing input

SAMPLING METHODOLOGY

Introduction

OA conducts inspections to assess the effectiveness of DOE 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, 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.

OA has developed statistically valid, practical procedures for gathering information during inspections. The procedures specify methods and indicate the type 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 appendix is organized as follows. Section 2.0 presents a general sampling methodology that is applicable to most topics. In Section 3.0, OA's application of sampling methods to the review of classified document and material accountability is discussed. This appendix focuses on sampling techniques, which are only one of the activities conducted by OA to review a facility's information security program.

General Sampling Methodology Considerations

Although OA comprehensive inspections are very broad, there are frequently 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 in OA inspections 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 OA 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 B-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 B-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 was 200 and two documents could not 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 was 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 B-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 B-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)			

DATA COLLECTION ASSIGNMENTS

Purpose:

Used to record data collection activities assigned each inspector during the inspection planning process.

Data Entry:

Data collection activities listed parallel those outlined in the CMPC Inspectors Guide. Room is provided for listing additional data collection activities or elaborating on listed items if special needs are encountered.

Columns are provided for listing up to four programs that are scheduled for inspection. Each column heading should list the specific program (e.g., the DOE Operations Office classified document program, the contractor document program, contractor material program, security force document program).

CLASSIFIED MATTER PROTECTION AND CONTROL (CMPC)

PLANNING SHEET

DATA COLLECTION ASSIGNMENTS

DATA COLLECTION ACTIVITY	PERSONNEL ASSIGNMENTS			
	PROGRAM:	**PROGRAM:**	**PROGRAM:**	**PROGRAM:**
PROGRAM MANAGEMENT				
Organization & Planning				
Foreign Ownership, Control, or Influence (FOCI)				
Security Infractions				
CONTROL OF SECRET AND CONFIDENTIAL DOCUMENTS				
Generation				
Review and Use				
Accountability				
Receipt & Transmittal				
Reproduction				
Destruction				
Physical Protection & Storage				
CONTROL OF TOP SECRET DOCUMENTS				
Classified Material Marking				
Classified Material Accountability				
Physical Protection and Storage				

DATA COLLECTION ACTIVITY	PERSONNEL ASSIGNMENTS			
	PROGRAM:	**PROGRAM:**	**PROGRAM:**	**PROGRAM:**
SPECIAL PROGRAMS				
Work for Others (WFO)				
Sensitive Compartmented Information				
Special Access Programs (SAP)				
Communications Security (COMSEC) Accounts/Materials				
OTHER AREAS AND ASSIGNMENTS				

LIST OF EXCEPTIONS

Purpose:

Designed to record any exceptions from DOE requirements that have been granted to the program, and to identify the level at which the exception was granted. This information is important in characterizing the program and determining if exceptions were granted at an appropriate level.

Data Entry:

Entry of subtopical area will assist inspectors in quickly identifying any exceptions, which pertain to the specific programmatic area they are reviewing.

A typical sheet might be filled out as follows:

CLASSIFIED MATTER PROTECTION AND CONTROL (CMPC)

PLANNING SHEET

LIST OF EXCEPTIONS

PROGRAM: El Cajon Documents Page 1 of 1

SUBTOPICAL AREA	NATURE OF EXCEPTION	DATE OF APPROVAL	APPROVED BY
Destruction	Permits use of central collection area and destruction by guards who gather documents from central collection room.	8/9/91	San Diego Operations Office
Physical Protection	Allows for use of locally developed forms versus Standard Forms 700.	12/1/87	DOE/OSS

CLASSIFIED MATTER PROTECTION AND CONTROL (CMPC)

PLANNING SHEET

LIST OF EXCEPTIONS

PROGRAM:_____ Page ___ of ___

SUBTOPICAL AREA	NATURE OF EXCEPTION	DATE OF APPROVAL	APPROVED BY

PREVIOUSLY IDENTIFIED DEFICIENCIES

Purpose:

Record of deficiencies identified during previous reviews of the program to be inspected. Serves as a quick reference to ensure that the inspection being planned will address all areas of weakness and ensure that all identified weaknesses were adequately addressed, corrected, and validated.

Data Entry:

Space is provided for noting deficiencies identified during documentation reviews and interviews with site personnel, DOE supervisory agencies, and DOE Headquarters organizations, etc.

Exercise caution when using this form, as data entry may result in the form becoming classified.

A typical sheet might be filled out as follows:

(CAUTION: MAY BE CLASSIFIED WHEN FILLED IN)

CLASSIFIED MATTER PROTECTION AND CONTROL (CMPC)

PLANNING SHEET

PREVIOUSLY IDENTIFIED DEFICIENCIES

PROGRAM: El Cajon Documents Page 1 of 1

DEFICIENCY	DATE FOUND	FOUND BY	CORRECTIVE ACTION	EDC	VALIDATED BY
No unique document numbers	1/14/91	OA	All accountable documents will have a unique number assigned	11/1/91	No Validation Noted
FOCI forms not submitted	1/14/91	OA	Subcontractor forms send SDFO		DOE/OSS Visit 8/1/91
Destruction residue too large	1/14/91	OA	New shredder ordered	9/30/91	No Validation Noted
Infractions not reported	8/22/90	SDFO	Quarterly reports being submitted	Complete	OA I&E 1/14/91
No accountability system	3/1/90	SDFO	New accountability system adopted sitewide	Complete	SD Operations Office Survey 8/22/90

(CAUTION: MAY BE CLASSIFIED WHEN FILLED IN)

(CAUTION: MAY BE CLASSIFIED WHEN FILLED IN)

CLASSIFIED MATTER PROTECTION AND CONTROL (CMPC)

PLANNING SHEET

PREVIOUSLY IDENTIFIED DEFICIENCIES

PROGRAM: _____ Page _____ of _____

DEFICIENCY	DATE FOUND	FOUND BY	CORRECTIVE ACTION	EDC	VALIDATED BY

(CAUTION: MAY BE CLASSIFIED WHEN FILLED IN)

MAIL ROOM

(Short Form)

Purpose:

An abbreviated reminder of points to be covered when reviewing receipt and transmittal of classified documents between the U.S. Postal Service and the site mail room, operations of the mail room, and internal distribution procedures. A longer version of the form is also provided.

Data Entry:

Space is provided for recording notes on inspection data points applicable to mail room operations pertaining to classified documents. Entries should be self-explanatory.

Ensure proper protection and handling if completed forms contain any classified information.

CLASSIFIED MATTER PROTECTION AND CONTROL (CMPC)

DATA COLLECTION SHEET

MAIL ROOM

Location: _____ Operated by: _____

Accountability (Receipt and Transmittal, Pick up and Delivery):

Delivery Procedures from U.S. Post Office:

Delivery Procedures to U.S. Post Office:

Physical Protection between Post Office and Site:

Access Controls:

Storage (in Mail Room):

Physical Protection during Internal Delivery:

Other Comments:

REPRODUCTION AND GRAPHIC ARTS

Purpose:

A reminder of points to be covered when reviewing reproduction of classified documents in a formal reproduction or graphic arts facility.

Data Entry:

Space is provided for recording notes on inspection data points applicable to reproduction of classified documents at such facilities. Entries should be self-explanatory.

Ensure proper protection and handling if completed forms contain information that would make them classified.

CLASSIFIED MATTER PROTECTION AND CONTROL (CMPC)

DATA COLLECTION SHEET

REPRODUCTION AND GRAPHIC ARTS

Accountability (Receipt, Processing, Delivery):

Storage:

Production Area/Access Controls:

Classified Work Area/Machinery Markings:

Documentation/Accountability of Products:

Overruns:

Sanitization of Machines/Materials:

Other Comments:

COPY MACHINES

(Short Form)

Purpose:

An abbreviated remainder of points to be covered when reviewing reproduction of classified documents on office copy machines. A longer version is available under "Copy Machines, Long Form."

Data Entry:

Space is provided for recording notes on inspection data points applicable to reproduction of classified documents on office copy machines. Entries should be self-explanatory.

Ensure proper protection and handling if completed forms contain any classified information.

CLASSIFIED MATTER PROTECTION AND CONTROL (CMPC)

DATA COLLECTION SHEET

COPY MACHINES

Location: _____ Responsible Organization: _____

Permission from Originator:

Internal Control Procedures:

Authorization/Procedures Posted?

Machine in Security Area?

Access Controls During Copying:

Sanitization Procedures:

SELF-ASSESSMENT PROGRAM

Purpose:

A reminder of points to be covered when reviewing security self-inspection programs.

Data Entry:

Space is provided for recording notes on inspection data points applicable to facility security self-inspection programs. Entries should be self-explanatory.

CLASSIFIED MATTER PROTECTION AND CONTROL (CMPC)

DATA COLLECTION SHEET

SELF-ASSESSMENT PROGRAM

Program Management Responsibility:

Program Directives:

Program Procedures:

Program Resources:

Program Scope/Coverings:

Tracking/Validation of Previous Deficiencies:

Program Findings Versus OA Results:

Program Records:

SECURITY INFRACTION PROGRAM

Purpose:

A reminder of points to be covered when reviewing the security infraction program.

Data Entry:

Space is provided for recording inspection data applicable to the security infraction program. Entries should be self-explanatory.

Ensure proper protection and handling if complete forms contain information of a personal nature, which would be covered by under “right to privacy” status.

CLASSIFIED MATTER PROTECTION AND CONTROL (CMPC)

DATA COLLECTION SHEET

SECURITY INFRACTION PROGRAM

Location: _____ Responsible Organization: _____

Program Procedures/Directives:

Internal Reporting:

Investigation:

Appropriate Management Involvement?

Disciplinary Schedule?

Appropriate (Disciplinary) Action?

Trend Analysis?

Corrective/Preventive Actions:

Required Reports Submitted?

Other Comments:

DESTRUCTION FACILITY

Purpose:

A reminder of points to be covered when reviewing programs and facilities for the destruction of classified matter.

Data Entry:

Space is provided for recording notes on inspection data points applicable to policy, procedures, and facilities pertaining to facility destruction programs. Entries should be self-explanatory.

CLASSIFIED MATTER PROTECTION AND CONTROL (CMPC)

DATA COLLECTION SHEET

DESTRUCTION FACILITY

Location: _____ Responsible Organization: _____

Accountability (Upon Receipt):

Approved Destruction Personnel?

Type of Machinery (Approved?):

Residue Size:

Storage (Prior to Destruction):

Records of Destruction:

Other Comments:

TOP SECRET DOCUMENTS

Purpose:

A reminder of points to be covered when reviewing Top Secret programs.

Data Entry:

Space is provided for recording notes on inspection data points applicable to Top Secret document accounts. Entries should be self-explanatory.

CLASSIFIED MATTER PROTECTION AND CONTROL (CMPC)

DATA COLLECTION SHEET

TOP SECRET DOCUMENTS

Account Size: _____ Number Checked: Front _____ Back _____ Personnel (TSCO, TS Classifier):

Authentication:

Markings/Cover Sheets:

Inventories:

Destruction:

Receipt/Transmittal:

Reproduction:

Other Comments:

SPECIAL ACCESS PROGRAM

Purpose:

A reminder of points to be covered when reviewing special access programs.

Data Entry:

Space is provided for recording notes on inspection data points applicable to special access program document accounts. Entries should be self-explanatory.

Ensure proper protection and handling if completed forms contain information that would make them classified.

CLASSIFIED MATTER PROTECTION AND CONTROL (CMPC)

DATA COLLECTION SHEET

SPECIAL ACCESS PROGRAM

Applicable Control Requirements (DOE, Sponsor): _____

_____

Account Size: _____ Number Checked: Front _____ Back _____

Markings:

_____

_____

Storage:

_____

_____

Access Controls:

_____

_____

Inventories/Audits:

_____

_____

Receipt/Transmittal Procedures:

_____

_____

Reproduction:

_____

_____

Destruction:

_____

_____

Other Comments:

_____

_____

SUMMARY ANALYSIS WORKSHEET

This worksheet is intended to be used by an inspector, if desired, to help organize conclusions reached during data collection and analysis. A checkmark indicating a rating of Effective Performance (E), Needs Improvement (N), or Significant Weakness (W) for each subtopic area reviewed may result in portraying a picture of the total survey program environment that is not otherwise evident. The worksheet may be completed by an individual inspector or indicate the collective conclusions of all topic team members.

FACILITY INSPECTED: _____ DATE: _____

SUBTOPIC	E	N	W	REMARKS
MANAGEMENT PROGRAM				
Planning				
Security Organization				
Self-Assessment Program				
FOCI				
CLASSIFIED MATTER PROTECTION AND CONTROL				
Access to Classified Matter				
Need-to-Know and Clearance				
Access Authorization Changes				
Control of Secret and Confidential Documents				
Preparation				
Receiving/Transmitting				
Review and Use				
Reproduction				
Destruction				
Document Accountability				
Control of Top Secret Documents				
Classifiers				
Marking and Documentation				
Destruction				
Forms				
Reproduction				
Transmission				

SUBTOPIC	E	N	W	REMARKS
Reporting Problems				
Classification Appraisals				
Conduct				
Records				
Corrective Actions				
SECURITY INFRACTIONS				
Procedures				
Notification				
Reporting				
Records				
Disciplinary Guidelines				
Disciplinary Actions				
Corrective Actions				