CLASSIFIED MATTER PROTECTION AND CONTROL

Assessment Guide

December 2016

Office of Cyber and Security Assessments
Office of Enterprise Assessments
U.S. Department of Energy

CLASSIFIED MATTER PROTECTION AND CONTROL ASSESSMENT GUIDE

December 2016

Table of Contents

Acronyms

CAS	Central Alarm Station
CI	Critical Information
CMPC	Classified Matter Protection and Control
CSS	Central Security Service
DCID	Director Central Intelligence Directive
DOE	U.S. Department of Energy
EA	Office of Enterprise Assessments
EA-21	Office of Cyber Assessments
EA-22	Office of Security Assessments
EDC	Estimated Date of Completion
EPL	Evaluated Product List
GSA	General Services Administration
ICD	Intelligence Community Directive
NATO	North Atlantic Treaty Organization
NDT	Non-Destructive Testing
NMC&A	Nuclear Material Control and Accountability
NNSA	National Nuclear Security Administration
NSA	National Security Agency
ODFSA	Officially Designated Federal Security Authority
OPSEC	Operations Security
PPM	Protection Program Management
PSS	Physical Security Systems
SAP	Special Access Program
SCI	Sensitive Compartmented Information
SCIF	Sensitive Compartmented Information Facility
SNM	Special Nuclear Material
SSP	Site Security Plan
SSSP	Site Safeguards and Security Plan
TSCM	Technical Surveillance Countermeasures
USPS	United States Postal Service
WFO	Work for Others

Section 1: Introduction

Purpose

The Classified Matter Protection and Control (CMPC) Assessment Guide provides guidance, procedures, and assessment tools that enable assessors to prepare for, conduct, and report the results of an assessment of the CMPC topic. The guide serves to promote consistency and ensure thoroughness. Further, it serves to enhance the quality of the assessment process developed by the U.S. Department of Energy (DOE) Office of Security Assessments (EA-22) within the Office of Enterprise Assessments (EA).

The guide is useful for both the novice and the experienced assessor. For the experienced assessor, the organization of information allows easy reference and serves as a reminder during the conduct of assessment activities. For the novice assessor, the information serves as a valuable training tool. With the aid of an experienced assessor, 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 Classified Matter
- Section 4 – Control of Top Secret Matter
- Section 5 – Control of Classified Materials
- Section 6 – Special Programs
- Section 7 – Interfaces
- Section 8 – Analyzing Data and Interpreting Results
- Appendix A – Performance Test Scenarios and Sample Performance Test Plans
- Appendix B – Forms and Worksheets.

The introductory section (Section 1) provides general guidelines, details on organization of the guide, and explanations of the assessment tools and their use. The section also describes the topic and the methods commonly used for assessing 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 assessing the CMPC subtopics:

- Section 2, Program Management, includes: Organization and Planning and the Operations Security (OPSEC) program.

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

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

- Section 5, Control of Classified Materials, includes: Marking, Accountability, and Physical Protection and Storage.

- Section 6, Special Programs, includes: Work for Others (WFO), Sensitive Compartmented Information (SCI) and Sensitive Compartmented Information Facilities (SCIFs), and Special Access Programs (SAPs). This section is for Official Use Only and is published as a separate document.

Section 7, Interfaces, contains guidelines for assessors to aid in coordinating their activities both within the CMPC topic team and with other topic teams. The section provides information on the EA-22 integration process that allows topic team members to align their efforts and benefit from the knowledge and experience of other topic team members. This section provides some of the common areas of interface for the CMPC team and explains how integration contributes to the quality and validity of assessment results.

Section 8, Analyzing Data and Interpreting Results, contains guidelines on how assessors organize and analyze information gathered during assessment 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 Test Scenarios and Sample Performance Test Plans, provides a set of commonly used performance test scenarios, as well as several variations of those scenarios that assessors 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 assessors when assessing the CMPC topic.

General Considerations

The guide contains tools and information that assessors frequently need. It is designed as a reference manual, for use at the assessor's discretion. Typically, assessors select the tools that are most useful on an assessment-specific basis. Generally, the guide presents information according to security subtopics, so assessors can easily locate specific subjects. Although the guidelines cover a variety of assessment 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 assessment-specific needs, and sometimes assessors may have to design new tools or activities to collect information not specifically covered in the guide.

The guide does not repeat verbatim the detailed information in DOE orders, manuals, or national drivers. Rather, it is intended to complement the governing instructions by providing practical guidance for planning the assessment and collecting and analyzing assessment data. One purpose in developing the guide was to capture the collective knowledge of EA-22's most experienced assessors. Assessors should refer to the guide as well as to DOE orders, manuals, or national drivers at all stages of the assessment process.

Every attempt has been made to develop specific guidelines that offer maximum utility to assessors. 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 assessment-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, manuals or national drivers 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. Assessors use the references as the basis for evaluating the assessed program and for assigning findings. It is useful to refer to the applicable orders and manuals during interviews and tours to ensure 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 assessors 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 EA-22 has noted on previous assessments. The information in this section is intended to help the assessor further focus assessment activities. By reviewing the list of common deficiencies and potential concerns prior to gathering data, assessors can be alert for these elements at the assessed facility during interviews, tours, and other data-gathering activities. Also, where appropriate, general guidelines are provided to help the assessor 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 assessment planning. These activities include document reviews and interviews with the facility physical security systems (PSS) 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 directly impacts the success of the assessment.

Performance Tests

General guidelines are provided to help the assessor 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, assessors typically gather information relevant to the accountability system, physical protection, document generation, and document reproduction.

Data Collection Activities

This section identifies activities that assessors 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.

Assessors do not normally perform every activity on every assessment. Specific activities and performance tests are normally selected during the assessment planning phase. The activities are those that are most often conducted and reflect as much EA-22 data collection experience and expertise as possible. Also, they are identified by alphabetical letter for easy reference.

Using the Tools in Each Assessment Phase

The assessment tools are intended to be useful during all phases of the assessment, including planning, conduct of the assessment, and closure.

The following summarizes the use of the assessment tools at each phase:

In the **planning phase**, assessors:

- 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 assessors (or small teams of assessors) 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 7 (Interfaces) to ensure that efforts are not duplicated.
- Review Section 8 (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 assessment time periods are sufficient to evaluate the assessed 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**, assessors:

- Use the detailed information in the Data Collection Activities section to guide interviews and tours. Assessors 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, assessors should then determine whether subsequent activities should be reprioritized.
- Review Section 8 (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 is needed to evaluate the program. If additional activities are needed, assessors should then determine whether subsequent activities should be reprioritized.

In the **closure phase**, assessors:

- 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 assessors in writing the analysis section of the assessment report.

Validation

Validation is the process of confirming with site representatives the accuracy of the information that EA-22 assessors have gathered. Whenever possible, assessors should confine validation to facts, not conclusions. However, site representatives should also understand the potential impact of the facts that are validated. The EA-22 validation procedure, discussed in detail in the EA-22 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 it may be difficult to reconvene the same personnel for the daily and summary validations. Daily validations normally take place at the end of each day during the data collection phase of the assessment. 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 EA-22 assessment 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. EA-22's current approach to the CMPC topic retains many aspects of past assessment methodologies for the control of classified matter and material (e.g., marking of matter, user and custodian knowledge, destruction, reproduction, control of Top Secret matter, SCI and SAPs).

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 EA-22 to organize assessment activities. One or more of these subtopics or special programs are included whenever EA-22 assesses CMPC. The determination as to which subtopics or special programs will be assessed 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 protecting 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 and national requirements, (2) it provides assessment team members with a baseline

picture of how the program operates at the site to be assessed, and (3) it may reveal weaknesses in policies or procedures that need to be further explored using other data collection tools and techniques.

Some required documents from the site being assessed may not be available during the planning meeting. The team may request that such information be made available by the site and ready for team use at the beginning of assessment conduct. Reviewing documentation continues throughout the assessment data collection phase. Often, the assessor 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 EA-22 Assessment 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, procedural guides, and work instructions. 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, facility approvals, and technical surveillance countermeasures (TSCM) equipment records.

Observation

Observation allows assessors to see how site personnel actually do their jobs, and assessors can evaluate them under normal, non-staged, non-controlled conditions. This provides the best data on whether site personnel 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 to be scheduled assessment 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 assessment tool, it is not a simple process:

- First, the topic team must determine 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 assessor may influence behavior and produce erroneous data.

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

For these reasons, observations are either generally confined to certain CMPC duties that occur on a routine basis, or are used to round out the assessment 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 assessors ask personnel and points of contact to provide information about all aspects

of the CMPC program. Interviews continue during the assessment conduct and provide an important source of information about the program.

Virtually any person associated with the program is a potential interview candidate. Interviews can be used to round out the assessor's knowledge, but more importantly help to determine an individual's knowledge and understanding of policies, procedures, and duties.

EA-22 employs both formal and informal interview techniques during the course of an assessment. 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 upon initiation of the assessment. Usually the facility or topical points of contact can provide immediate answers to many of the questions early in the assessment process.

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

Since important issues may arise by chance, assessment 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, assessors should be wary of attempts by points of contact to coach or otherwise influence the individuals being interviewed.

Knowledge Tests

There is a certain body of knowledge, some Departmental and some site-specific, that people associated with CMPC must have. Knowledge tests may be used to determine whether personnel possess this knowledge. However, assessors normally obtain this information during the course of interviews.

Performance Tests

Performance testing is one of the most valuable data collection methods used to assess 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 to determine which elements of the program, whether they be personnel, procedures, or equipment, perform as expected.

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. EA-22 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 assessors 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** – A detailed safety plan is required if the performance test has safety implications. Normally CMPC performance tests do not impact safety, so this requirement would not apply.

Although this format has been provided, it should not be considered mandatory. Assessors 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.

Assessment Goal

The assessment 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. Reviewing every document in an accountability system or interviewing every custodian is normally impractical. Assessors 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.

The samples tested should 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 because of the need to maintain objectivity in 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 470.1B, Admin Chg 1, *Safeguards and Security Program*, outlines DOE's safeguards and security programs.

The Department's safeguards and security program will:

1. Identify all protection needs for the Department.

2. Establish clear roles and responsibilities for safeguards and security.

3. Implement Departmental policy through line management.

4. Establish safeguards and security oversight programs to assure that policy implementation meets established standards.

5. Seek and implement continuous improvements and efficiencies.

The safeguards and security program will incorporate the following principles:

1. Safeguards and Security considerations are thoroughly integrated with all aspects of mission accomplishment.

2. Protection requirements are commensurate with the consequences of loss or misuse of the protected asset.

3. Responsibility for the implementation of protection measures resides with DOE line management elements responsible for mission accomplishment.

4. Authority is delegated to appropriate levels to promote efficiency and effectiveness.

5. Program oversight ensures that opportunities for improvement, both in effectiveness or efficiency, are identified and acted upon.

6. Managers are empowered to make risk management decisions as necessary to support mission accomplishment.

7. Program focus is upon overall mission performance.

Section 2: Program Management

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. 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.

2.1 Organization and Planning

2.1.1 References

DOE Order 471.6, Admin Chg 2, *Information Security*
DOE Order 470.4B, Admin Chg 1, *Safeguards and Security Program*

2.1.2 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 because these areas 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 are deficient.

Usually, EA-22 assesses each major organization that holds classified matter at a site. In some cases, EA-22 reports the results for the local DOE office and prime operating contractor separately. The program management subtopic is not normally reported separately, 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 assessment results.

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 classified matter accounts, very few items 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 assess each organization's CMPC management program. A topic team member usually needs one or two days to review management for each program being assessed (the actual time required depends on the size and complexity of the assessed program). The CMPC team may want to schedule the review of management for the latter part of the assessment so they can focus on the management problems identified during earlier stages of the assessment; 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, assessors 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 assessment 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. Assessors 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 assessment activities, it may be desirable to interview managers at levels above the overall safeguards and security managers as well. An organized interview schedule, with other topic teams, in which the assessors 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.

2.1.3 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 and national drivers 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 ensure that a lack of management support does not adversely impact the effectiveness of security programs.

Lack of a Suitable Organizational Structure. Occasionally, assessors 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, assessors 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 National Nuclear Security Administration (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 or NNSA 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 comply 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 organizations, 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 formal training, relying instead on an unstructured form of on-the-job training. These organizations expect persons with classified matter responsibilities to learn from other, more experienced individuals. However, the experienced individuals themselves often lack adequate training, so improper practices continue. Organizations sometimes 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, assessors should focus on reviewing its effectiveness. If no training program exists, assessors should devote additional attention to activities designed to determine the knowledge level of individuals who perform CMPC functions (for example, interviews or performance 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, assessors 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 assessing organizations with several lower-level elements that develop separate procedures, assessors 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, store these parts in DOE-defined "non-conforming" open storage. Open storage is considered non-conforming 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 protection effectiveness measures equivalent to that provided to similar levels and categories of classified matter by standard configurations, such as protective force patrols or other protection measures that are sufficient to prevent adversaries from successfully accessing and removing the parts. Equivalent controls must be based on documented, approved analysis that considers the time needed to remove the parts, the parts' value, and the consequences to national security of the parts' removal. Most often, such analysis has either not been conducted, has not been conducted for *all* locations of non-conforming storage, or has 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, facilities 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.

5. Ensure that adequate resources are applied to correcting deficiencies.

6. Conduct follow-up reviews to ensure that the corrective action was effective in addressing the root cause.

Very often 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. Tracking systems 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, which usually results in recurring deficiencies. Many times, the organization corrects the surface problem or symptom rather than identifying and correcting the underlying cause, i.e., the root cause. For example, if an assessment 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 the necessary training, as well as a follow-up review to ensure efficacy. Unless management accurately determines the root cause of identified deficiencies, similar deficiencies will likely recur.

2.1.4 Planning Activities

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

- If directed, 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 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 assessment. This list should be tailored to the CMPC program of the site and the DOE field element.

Once assessors 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, assessing all organizations in the same depth or interviewing all individuals who perform document protection duties is impractical. In such cases, a representative sample may be selected for evaluation. Typically, assessors 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 assessment will influence the selection of managers to be interviewed. As program strengths and weaknesses are noted, the assessors should modify their planned activities appropriately.

2.1.5 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 assessment areas should be considered because strengths and weaknesses in the implementation of the program are often attributable to management deficiencies. 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.

2.1.6 Data Collection Activities

Line Management Responsibility for Safeguards and Security

A. Assessors should review the applicable planning documents that cover the CMPC program (for example, SSSPs or other planning documents). Assessors 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 the 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. Assessors should interview security managers, including the CMPC manager. Elements to cover include:

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

C. Assessors 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, assessors 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, if required.

D. Assessors 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 deficiencies 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, assessors 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 assessments 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. Assessors should determine how management communicates its goals and objectives and stresses the importance of CMPC. Assessors should determine what programs are used to maintain an appropriate level of security awareness.

F. Assessors 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 level. Assessors can also review individual position descriptions 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.

G. Assessors should review actual versus authorized staffing levels for CMPC positions to determine whether the program is operating short-handed. Assessors 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 EA-22 CMPC assessments can be attributed to inadequate or non-existent training programs. Assessors 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, assessors should examine the site programs that are responsible for ensuring the appropriate level of general security awareness, as well as CMPC awareness.

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

J. Assessors 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. Assessors 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, assessors should follow up those concerns with security managers to gather their views. In some cases, assessors may find that the security managers are unable to offer more training classes because of lack of resources or qualified training staff.

Comprehensive Requirements

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

L. Assessors 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), assessors 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. Assessors should determine whether procedures (including updates and revisions) are being distributed to those who need them. Assessors 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. Assessors should determine whether policy updates and directives issued by DOE Headquarters or NNSA 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, local DOE office surveys, and assessments. Assessors should determine what system or systems are being used and coordinate with the protection program management (PPM) topic team as necessary.

O. Assessors 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. Comparing the results of facility self-assessments to assessment findings or other audit results to learn whether the self-assessments are equally effective is helpful.

P. Assessors should determine who actually performs the self-assessments. The DOE or NNSA 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. Assessors should determine whether deficiencies identified during self-assessments are entered into a tracking system, and how corrective actions are selected and achieved.

Q. Assessors should determine whether an organization has a tracking system and how it operates. In conjunction with the PPM topic team, they should determine whether the tracking systems have a means of monitoring the status of all assessments, surveys, self-assessments, and other similar activities. Also, assessors 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. Assessors may 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. Assessors should determine whether corrective action plans exist for deficiencies and whether deficiencies are analyzed and prioritized. Assessors should determine whether schedules and milestones have been established and whether specific responsibilities to ensure completion have been assigned down to the individual level. Assessors should also determine whether root cause analyses are performed. If so, the assessors should request documentation of the 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, assessors may elect to review how resources required for corrective actions are introduced into the budget process.

S. At contractor facilities, assessors 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 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.

2.2 Operations Security Program

2.2.1 References

DOE Order 471.6, Admin Chg 2, *Information Security*

2.2.2 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.

2.2.3 Common Deficiencies/Potential Concerns

Lack of Basic Program Elements

OPSEC programs often 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 Information (CI) and attendant Essential Elements of Friendly Information (commonly called Indicators).

Lack of Relevant OPSEC Assessments and Reviews

Pertinent, site-specific OPSEC assessments 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

471.6, Admin Chg 2, *Information Security*, and thereby satisfy minimum OPSEC reporting requirements, the site may not have considered the most relevant, most sensitive, or highest-value programs or facilities. Moreover, due consideration may not have been given to the site's established CIs/Indicators when deciding what assessments should be performed.

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.

2.2.4 Planning Activities

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

- Documentation that can be supplied on program plans and procedures that indicates 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 CIs/Indicators
- Copies of OPSEC assessments
- Documentation on OPSEC awareness training and staff attendance
- OPSEC Awareness conducted or planned for the site.

2.2.5 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 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 concerning foreign nationals 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.

Section 3: Control of Classified Matter

References

DOE Order 470.4B, Admin Chg 1, *Safeguards and Security Program*
DOE Order 471.6, Admin Chg 2, *Information Security*
DOE Order 472.2, Admin Chg 1, *Personnel Security*
DOE Order 473.3, *Protection Program Operations*
DOE Manual 475.1-1B, *Identification and Protection of Unclassified Controlled Nuclear Information*

General Information

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

- Top Secret matter.
- Secret Restricted Data matter that is maintained *outside* a Limited Area or higher.
- Any matter designated as accountable by national, international, or programmatic requirements. Examples include, but are not limited to, Sigma 14 and North Atlantic Treaty Organization (NATO) Atomal.

During planning for an assessment, documentation from the site should be reviewed to assess the facility's total posture in the area of protection and control of classified 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 7 will assist assessors in determining how concerns noted by other topic teams impact 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 PSS used to control access to Limited Areas. The following questions may help the data collection regarding the PSS 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?

The human element of protection complements the physical systems that protect classified matter. 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?

3.1 Generation

3.1.1 References

DOE Order 470.4B, Admin Chg 1, *Safeguards and Security Program*
DOE Order 471.6, Admin Chg 2, *Information Security*
DOE Order 473.3, *Protection Program Operations*
DoD 5220.22-M, National Industrial Security Program Operating Manual

3.1.2 General Information

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

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

DOE requirements for generating classified matter extend beyond initial 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 matter. Included in the definition of classified matter is all records of information that require protection against unauthorized disclosure, regardless of physical form or characteristics. Classified matter is 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 (e.g., parts, metals, machinery, chemical compounds)
- 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.

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

3.1.3 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 matter preparation may indicate a lack of firm control over such preparation. In such cases, assessors 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 may not be 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, he/she may incorrectly mark and protect the document on the basis of his/her own estimate of its classification level, category, and classification duration. The second problem is that once marked by the originator, the document might never be reviewed by a proper classification authority.

Incorrect or Missing Markings

Incorrect and missing markings are commonly encountered on all types of classified matter. 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 titles are not marked with the proper classification or in the proper location.
- Classifier and declassification information is omitted.
- Markings for disks 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/presentations, and photographic prints. Assessors 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

Though not often encountered, this problem 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 assessors do not normally examine unclassified files, it is only by chance that assessors encounter documents changed to Unclassified. However, assessors 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. In cases of upgraded documents, the document markings should clearly reflect the upgrade information and identity of the derivative classifier that upgraded the document. 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

Classified documents are often temporarily or permanently placed in folders. At some facilities, all classified 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, assessors should expect to find a supply of the appropriate cover sheets in, on, or near the safe.

3.1.4 Planning Activities

During planning, assessors interview points of contact and review available documentation (for example, SSSP or SSP, 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 classified matter originated at the facility (including all types listed previously in this section).
- Which organizations or individuals create the classified matter (consider all types listed previously in this section).
- The established procedures and responsibilities for the various elements of classified matter 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, assessors should select a representative sample for evaluation. Typically, for efficiency, assessors cover other CMPC areas in addition to classified matter generation. Consequently, a variety of factors should be considered when selecting individuals and accounts to review. It is usually more efficient to observe the same individuals and accounts selected for "classified matter review and use" when looking at classified matter 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 classified matter generation and marking to several different individuals or elements (for example, originators, secretaries, and the central control station), it is advisable to ensure that the selected accounts include these different categories. If the facility generates special classified matter (for example, photographs or aperture cards), assessors should review the preparation of that classified matter, even if other assessment activities do not include those specific items.

3.1.5 Performance Tests

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

- Classified matter generation
- Classified matter marking
- Classified matter accountability front check
- Classified matter 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. Assessors should use such records to conduct performance tests to help determine whether the proper controls are in effect.

3.1.6 Data Collection Activities

Reviews of Individual Accounts

A. Assessors 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. Assessors should determine whether the individuals understand local classified matter 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. Assessors should also check for availability of necessary procedures, references, rubber stamps, and cover sheets. Assessors may choose to ask the custodian or responsible individual to demonstrate the procedures.

B. To supplement information provided by routine classified matter holders, assessors should interview selected individuals who only occasionally generate or prepare classified matter 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 who work outside the Limited Area. Typically, assessors indiscriminately select one to five readily available personnel to interview, rather than expending the effort to obtain a random sample. Assessors should determine exactly how the procedures are applied and compare the results with DOE and site policies. If local procedures do not exist, assessors should ask the responsible people to explain all aspects of how they prepare classified matter and interact with other individuals involved. Assessors may also elect to ask individuals whether they are currently writing or working on any classified matter. If so, assessors may ask to see the classified matter and conduct the activities identified in the following paragraph.

C. A valuable method for determining the adequacy of generation programs is to review classified matter that facility personnel have prepared or are in the process of preparing. This review is often done in conjunction with a classified matter file check (safe-kicking), when a wide cross-section of facility documents is examined. (Safe-kicking is similar to the back check performance test without attention to accountability

records.) The partially prepared classified matter, i.e., working papers, can be checked for markings consistent with the stage of development, and for proper storage practices. If appropriate individuals have classified matter to prepare, assessors may wish to observe generation activities and have personnel explain each step as it occurs.

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

3.2 Review and Use

3.2.1 References

DOE Order 470.4B, Admin Chg 1, *Safeguards and Security Program*
DOE Order 471.6, Admin Chg 2, *Information Security*
DOE Order 472.2, Admin Chg 1, *Personnel Security*
DOE Order 473.3, *Protection Program Operations*

3.2.2 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 death or long-term disability of a person formerly authorized access to such information. These steps 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 Areas or higher.

Proper marking and accountability overlap with other elements of the subtopic and are addressed in detail in Sections 3.1, 3.3, and 3.4; 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 assess. 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/her own," with little direct supervision. Therefore, individual practices throughout a facility may vary greatly, and assessors must visit numerous locations to form an accurate picture of sitewide practices.

The procedures for personnel who have been terminated or transferred, or for persons who have died or are on extended absence, may vary greatly from site to site. Specific checkout procedures may be promulgated site wide 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.

3.2.3 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 matter 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 matter. Inadequate checkout procedures can result in failure to:

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

3.2.4 Planning Activities

During planning, assessors interview points of contact and review available documentation (for example, SSSP or SSP, 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 areas (e.g., Limited Areas)

- Procedures for delivering and receiving classified matter to and from the post office, and for intra-site distribution

- Clearing procedures and requirements in cases of transfer, termination, death, or extended absence

- 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 matter, assessors normally assess all areas. If classified matter is stored in repositories throughout the facility, and classified matter is 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. The sample can also be used to evaluate other CMPC subtopics and subtopic elements.

Assessors should also determine the best way to assess checkout practices. Some aspects of these practices, such as transfer of classified matter 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.

3.2.5 Performance Tests

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

- Classified matter file check (similar to a traditional back check without attention to accountability records)
- Classified matter front check (used for holdings still requiring accountability).

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

Assessors may develop performance tests to evaluate this area. For example, assessors could recruit a facility employee, who does not have the appropriate clearance, or appropriate need-to-know, to attempt to obtain a classified document following normal facility procedures. Assessors would include the results of such an attempt in evaluating the effectiveness of the facility's systems and procedures in protecting classified matter. In no case should any compromise of information be allowed.

3.2.6 Data Collection Activities

Access Control Procedures

A. Assessors should interview selected classified matter holders, supervisors, secretaries, and other staff members to determine the procedures used for limiting access, enforcing need-to-know, and attending classified matter outside locked repositories. Also, assessors should determine whether staff members clearly understand the procedures. If the procedures are in writing, assessors 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 matter.

B. Assessors should observe actual practices to determine whether procedures are followed. Normal practices may become evident during the assessment. 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 if custodians indicate they refer to the list before granting access, assessors should determine whether the list is readily available at the appropriate locations.

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

D. Assessors 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. Assessors 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 classified matter has been transferred, their names removed from access lists, and appropriate combinations changed. The CMPC or personnel security topic team should determine whether security termination statements were completed and properly filed, and whether badges and credentials were recovered.

3.3 Accountability

3.3.1 References

DOE Order 470.4B, Admin Chg 1, *Safeguards and Security Program*
DOE Order 471.6, Admin Chg 2, *Information Security*
DOE Order 473.3, *Protection Program Operations*

3.3.2 General Information

Though most DOE elements have eliminated accountability for Secret classified matter within security areas, accountability is required for Top Secret matter; Secret matter stored outside a Limited Area or higher; SAPs; Sigma 14, NATO Atomal documents; and designated United Kingdom documents.

As stated in the introductory portion of Section 3, 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, or subject to a change of classification)
- Unique identification numbers
- Inventory of documents
- Procedures for dealing with unaccounted-for (missing) classified matter.

These requirements apply to all accountable classified matter. They include the need to maintain a clear audit trail that specifies the current location and custodian for each piece of classified matter. 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 classified matter and that 100 percent inventories be conducted at least every 12 months. Various steps and reports are also required when accountable classified matter is discovered to be missing.

Assessment of the accountability element centers on determining whether accountability records accurately reflect accountable holdings. That is, assessors should determine whether all classified matter on the records is present, whether all classified matter on hand is in the accountability records, and whether the required audit trail for all accountable classified matter is present. Accountability records include classified matter receipts and destruction records; classified matter receipts and destruction records are also addressed in Sections 3.4 and 3.6.

DOE policy specifies what a classified matter accountability system must accomplish and how it must be established and maintained through the use of control stations. Assessors may encounter several different types of systems that satisfy DOE accountability requirements. The characteristics of an accountability system significantly affect the methods used to assess the system.

The major difference in accountability systems pertains to the degree of centralization. In centralized systems, all accountable classified matter is carried in a single accountability system that is controlled and operated by designated personnel. Although classified matter may be held by individuals who are required to keep an

inventory record of classified matter they possess, the formal accountability records are held centrally. In such systems, all incoming and outgoing accountable classified matter is processed through the central accountability unit. Also, internal transfers are either routed through or reported to the central accountability unit. The central accountability unit is sometimes responsible for all destruction of accountable classified matter.

In a decentralized system, custodians holding classified matter maintain their own independent accountability systems. Such custodians may also receive, transmit, and destroy classified matter 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. In such cases, individual accountability systems and records are maintained by the various organizations (department, division, or group), but classified matter may also be held by individual custodians or subordinate organizations.

Another characteristic of an accountability system that affects assessment 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 classified matter 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 classified matter control cards and copies of receipts and destruction records. Assessors 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 assessment activities is the number of accountable holdings. The number of holdings assessed typically runs from large systems with tens or hundreds of thousands (or even millions) of pieces of classified matter down to small systems with only a few hundred pieces of classified matter. 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, classified matter located in SCIFs or SAPs is 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 assessment planning and data collection. A small, centralized, automated system that includes all accountable classified matter on site is the easiest system to assess, since only one sample must be assessed and the automated system can often generate random sample lists. Assessment 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 classified matter from each selected system is examined. Efficiently assessing 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 assessors, since individual samples from a number of accounts must be manually generated and reviewed.

3.3.3 Common Deficiencies/Potential Concerns

Missing Accountable Classified Matter

It is not unusual for a facility to be unable to locate one or more pieces of classified matter in the sample selected for the classified matter accountability front check. Any classified matter not found is considered

missing, and the facility should initiate the required actions. Detailed instructions on the specific procedures for handling instances of missing classified matter are presented in DOE Order 470.4B, Admin Chg 1.

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

Classified Matter Not in Accountability

On occasion, accountable classified matter is not found to be listed in the facility's accountability systems. Accountable classified matter is usually found during accountability back checks, but may be found during any assessment activity involving classified matter review. The types of classified matter that are most likely to be out of accountability include:

- Reproduced copies of other documents
- Computer media (e.g., disks, removable hard drives)
- 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 occur, assessors who find classified matter out of accountability may reasonably conclude that the same problem persists elsewhere on 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 classified matter 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. Assessors 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 classified matter and records of destruction for destroyed classified matter. Sometimes, classified matter is transferred off site (or "loaned") without proper receipting. Receipts for classified matter 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 Classified Matter

The requirement for each holder of Secret accountable classified matter to maintain a current list of classified matter on hand is frequently ignored. In decentralized systems in which each holder has an accountability system, those accountability records would satisfy this requirement. However, in centralized systems in which individual custodians also hold classified matter, 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 usually occurs when site CMPC procedures do not address the requirement.

Failure to Conduct a Proper 100 Percent Inventory

DOE requires, at a minimum, an annual 100 percent inventory of accountable matter. Inventory procedures at some locations include only the classified matter listed in accountability records. Such a procedure misses classified matter that should be, but is 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 a significant amount 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, assessors may find drafts that were not entered into accountability when distributed outside the office in which they originated. In addition, assessors 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 report and deal with inventory discrepancies according to DOE policy and requirements for reporting incidents of security concern. Details and timelines for inquiries and reporting requirements are currently found in DOE Order 470.4B, Admin Chg 1, *Safeguards and Security Program*.

3.3.4 Planning Activities

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

- The number of accountability systems at the facility and the specific identity of each (e.g., control station accounts)
- The amount of accountable classified matter 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 assessment generally involves determining how to sample the systems. If dealing with a small number of systems (one to three), it is practical to assess each system. When dealing with more systems, it is often necessary to select a sample of systems (two, three, or four) to assess. 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 libraries, they may be specifically included in the sample to be assessed. Information developed during planning interviews and document reviews, such as indications of past accountability problems, may help assessors decide which specific systems to assess.

Once the systems have been identified, the specific sampling methods must be determined and planned. For each system assessed, two types of samples are usually produced. The first is a sample of classified matter from the accountability records that assessors 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, assessors 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 assessors 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 assessment. If automatic sample generation is not possible, a more time-consuming method must be employed.

3.3.5 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 of these performance tests are provided in Appendix A.

3.3.6 Data Collection Activities

Accountability Systems and Procedures

A. Assessors 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. Assessors also should determine whether responsible personnel fully understand and are correctly maintaining the document accountability records.

Accountability Records

B. Assessors should review accountability records and backup classified matter to determine whether records contain all required information fields 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. Assessors should pay particular attention to determining whether the software allows the users to delete records. If so, assessors 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).

3.4 Receipt and Transmittal

3.4.1 References

DOE Order 470.4B, Admin Chg 1, *Safeguards and Security Program*
DOE Order 471.6, Admin Chg 2, *Information Security*
DOE Order 473.3, *Protection Program Operations*

3.4.2 General Information

This element of the subtopic deals with receipt and transmittal of classified matter. Activities include:

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

The responsibility for receipt and transmittal of classified matter is normally assigned to a central facility or individual. Centralized systems usually involve the facility mailroom or classified matter 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. Assessors should determine the completeness of procedures and the knowledge of the individuals who carry out receipt and transmittal responsibilities.

Receipt of Classified Matter from Off Site

Classified matter received from off site is 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. Assessment 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 mis-sent, were tampered with, or are improperly packaged, the sender's security office should be contacted immediately or other appropriate action taken.

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

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 classified matter. When such storage is a possibility, it should also be included in the scope of assessment activities.

Transmittal of Classified Matter Off Site

Offsite transmittal of classified matter is basically the reverse of the receipt process. For accountable classified matter, the process normally begins with accountability record adjustment. Receipts describing the classified matter 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 matter in transit.

Next, the classified matter is 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. Additionally, there is a possibility of electronically transmitting classified information.

Intra-site Transfer of Classified Matter

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 matter generally follows procedures similar to those used for offsite transmittal and receipt; facilities normally modify the procedures to meet site-specific needs. Assessors should determine whether local procedures have been developed and promulgated in appropriate security directives.

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

Hand-carrying Classified Matter

Under certain circumstances, hand-carrying classified matter is permitted. Normally, this is restricted to emergency situations when the classified matter 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 classified matter 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.

3.4.3 Common Deficiencies/Potential Concerns

Classified Matter Not Properly Protected

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

Classified Matter Not Properly Marked or Documented

Classified matter received from off site, especially from other agencies, is 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. Improper marking can also occur when classified matter is sent directly to the recipient and when recipients' hand-carry classified matter back from meetings. This problem is also addressed in Section 3.1.

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 assessors can check the offending facility. Rather, it is more common for the assessment to focus on prompt and aggressive follow-up on overdue suspense by the sending facility.

Misaddressed Classified Matter

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 classified matter to unauthorized facilities and uncleared recipients. Second, facilities receiving mis-sent classified matter may not report the problem to the sender's security office as required by DOE. The mis-sending of classified matter is often reflected in accountability problems.

Improper Wrapping

Single (rather than double) wrapping of classified matter 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 classified matter within the same facility.

Improper Transmittal Methods

The most common problem associated with actual transmittal of classified matter 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 be given classified matter at the servicing post office.

Improper Hand-carrying of Classified Matter

Failure to follow established procedures and contingency plans is a common problem with classified matter hand-carry programs. Individuals continue to take classified matter 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.

3.4.4 Planning Activities

Assessors 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 matter off site (responsibilities of individuals and central facilities)
- Methods used to ensure that facility recipients are authorized to receive incoming classified matter addressed to them
- Methods used to verify classified mailing addresses before classified matter is sent off site
- When required, accountability procedures used to ensure that an uninterrupted audit trail is maintained for all classified matter (including preparation of receipts and suspense systems)
- Location of facility security areas and how classified matter is transferred between security areas
- Specific instructions governing the transfer of classified matter 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.

Assessors should determine which elements of the program are critical to the effective transfer and physical protection of classified matter, and which will be assessed. 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 assessed in conjunction with other assessment topics. However, if circumstances permit, assessors should plan to observe the actual receipt, transfer, and dispatch of classified matter and discuss procedures with responsible employees as they perform their duties.

3.4.5 Performance Tests

The assessment 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.

3.4.6 Data Collection Activities

Receipt of Classified Matter from Off Site

A. It is usually best for assessors 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, assessors 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? Assessors 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 classified matter is 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 classified matter is brought into accountability at the appropriate time.

E. Assessors should observe internal distribution to ensure that classified matter is properly protected while en route to the intended recipients or storage location. If classified matter is temporarily stored, those procedures should also be checked to ensure compliance with DOE requirements.

Transmittal of Classified Matter 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, assessors 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 matter.

G. Assessors should determine whether receipts are prepared to formally transfer the classified matter, a copy of each receipt is retained in a suspense file, and records are annotated to show which accountable classified matter is being transferred. This is also a good time for assessors to look at the facility suspense file to determine whether proper and timely follow-up is accomplished for classified matter that has already been transferred. If no classified matter is currently in suspense, assessors 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. Assessors 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 classified matter should be reviewed. During the entire process, assessors should carefully observe the physical protection afforded classified matter to ensure that it meets DOE requirements.

Intra-site Transfer of Classified Matter

I. As discussed earlier, the transfer of classified matter within a DOE facility may incorporate many of the elements found in offsite receipt and transfers. If necessary, assessors should modify their assessment 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 matter is transferred between security areas), and the physical security afforded the documents.

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

Hand-carrying Classified Matter

K. Methods used to assess 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, assessors should interview those individuals responsible for exceptions, if any.

L. On the other hand, some facilities regularly permit hand-carrying. Usually, these facilities have established a full, formalized program. Although observing actual hand-carrying is impractical, assessors 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, assessors may attend a training session and talk with people who have been given authorization to hand-carry. Also, assessors can ask to review security infraction records to determine how well authorized personnel comply with program requirements.

3.5 Reproduction

3.5.1 References

DOE Order 470.4B, Admin Chg 1, *Safeguards and Security Program*
DOE Order 471.6, Admin Chg 2, *Information Security*
DOE Order 473.3, *Protection Program Operations*

3.5.2 General Information

Reproduction of 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. Reproduced matter must be properly marked to reflect required information, including the classification level and category, and reproduced accountable matter must also be entered into accountability.

Reproduction of classified matter within DOE can be divided into three categories: copying, printing, and electronic reproduction. 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. Electronic reproduction is associated with moving data on one piece of electronic media to another.

Whatever methods the facility uses, assessors 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 assess. Most facilities limit the number of copying machines authorized for classified reproduction. Consequently, in some cases the assessment 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 assess. 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 assessors 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 assessors may need to adequately review procedures and determine program compliance. A comprehensive review of a large facility could require several days and several assessors, 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.

3.5.3 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 the site will comply with DOE physical protection,

marking, documentation, accountability, and transmittal requirements. The need for local procedures, and their adequacy when in place, 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 that assessors identify. Also, assessors should determine whether fax machines are routinely used to copy classified documents; if this is the case, the same issues identified for copy machines apply to the fax machines.

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.

Matter Not in Accountability

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.

3.5.4 Planning Activities

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

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

3.5.5 Performance Tests

The assessment team may consider using performance tests to establish a clear picture of local procedures and the competence of the 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.

3.5.6 Data Collection Activities

A. For normal copying and duplication programs, assessors should concentrate on whether copy machines are located in security areas, conspicuously marked with the procedures for classified duplication, and used properly. Assessors 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, assessors tour the facility and interview assigned personnel. Once reproduction procedures are understood, assessors 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 assessment, assessors should observe the process. If not, assessors should interview facility personnel to determine whether procedures are followed, or ask them to reproduce an imitation classified document.

3.6 Destruction

3.6.1 References

DOE Order 470.4B, Admin Chg 1, *Safeguards and Security Program*
DOE Order 471.6, Admin Chg 2, *Information Security*
DOE Order 473.3, *Protection Program Operations*

3.6.2 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. Assessment procedures for classified materials are contained in Section 5.

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 matter is collected at various locations and taken to the facility for destruction, either on a scheduled basis or when a sufficient quantity has accumulated. Frequently, classified matter is 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 matter is stored, to larger shredders serving an entire department or building. Decentralized systems are usually operated by individuals who use the classified matter, rather than designated operators.

The National Security Agency/Central Security Service (NSA/CSS) publishes the Evaluated Product List (EPL) for various types of destruction equipment (for paper, hard drives, optical media, etc.). Only destruction equipment on this list is approved for the destruction of classified matter.

Some non-paper media cannot be adequately destroyed by shredding or pulverizing. Some examples are computer disks, 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 of non-solid state hard drives on NSA-approved equipment is considered destruction, but additional destruction by disintegrator is encouraged. The pertinent NSA/CSS EPL provides the product list of NSA-approved degaussing equipment. It is important for the DOE program, site office, or Chief Information Officer to 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.

3.6.3 Common Deficiencies/Potential Concerns

Non-approved or Inadequate Destruction Equipment

Destruction equipment (e.g., shredders, pulverizers) that NSA has not approved is sometimes used. Assessors 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 do not meet the maximum size requirements.

Use of Shredders for Non-paper Media

Classified computer media must be destroyed in accordance with DOE cyber policy, and utilizing equipment approved by NSA.

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, classified matter is 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

Failing to maintain a written audit trail for accountable classified matter until it is physically destroyed is a common deficiency. This problem is mainly found at facilities with a centralized destruction system. Frequently, custodians remove classified matter from the accountability system by completing and signing the record of destruction. This often is done when the document is taken or transferred 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 classified matter is not accounted for from the time the record of destruction is signed until the classified matter is actually destroyed. The destruction can be performed by any appropriately cleared and authorized person as long as the audit trail for each piece of classified matter is maintained until actual, physical destruction.

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

3.6.4 Planning Activities

During the planning meeting, assessors interview points of contact and review available documentation (for example, SSSP or SSP, 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, incinerators, and all other mechanical, chemical, or thermal means)
- The established procedures and responsibilities for document destruction (including whether the Officially Designated Federal Security Authority [ODFSA] has issued procedures or approved the facility procedures)
- Approved exceptions to requirements, including whether the exceptions were formally approved by DOE Headquarters or the appropriate risk-accepting official.

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

If a large number of organizations or stations are involved, assessors may select a representative sample for evaluation. Typically, for reasons of efficiency, assessors 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.

3.6.5 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. Assessors 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 be destroyed by means other than shredding).

3.6.6 Data Collection Activities

Documentation

A. Assessors should review records of destruction to determine whether procedures are implemented as intended and whether records are maintained as required. Typically, assessors 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 classified matter, consistent with site and DOE requirements. The following factors should also be considered:

- Type of records maintained (for example, is a Record of Destruction or a form similar in content, used to record the destruction of accountable classified matter?)
- 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 classified matter.

Audit Trails

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

C. Tracing a small sample of indiscriminately selected destruction records back through the system to verify that they are consistent with other site records is sometimes advisable. 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, assessors can determine whether records are accurately maintained and can sometimes identify potential gaps in the accountability record. **Note:** Assessors 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 ten 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. Assessors 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 classified matter to be destroyed is 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 classified matter to the collection point; physical protection during transfer (is the classified matter left unattended?); methods for transferring accountability for each document (including determining who accepts responsibility for and signs for the classified matter at the receiving or collection point)

- The storage location for the classified matter after it is collected; physical protection measures in place at the collection and storage area; duration of storage.

E. Assessors should observe the actual facilities for storing and destroying classified matter to determine whether they comply with DOE orders. Shredder and other equipment items 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. Assessors should assess 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.

Decentralized Destruction Stations

F. Assessors 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. The following should be determined:

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

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

- Personnel authorized to operate the shredders.

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

3.7 Physical Protection and Storage

3.7.1 References

DOE Order 470.4B, Admin Chg 1, *Safeguards and Security Program*
DOE Order 471.6, Admin Chg 2, *Information Security*
DOE Order 472.2, Admin Chg 1, *Personnel Security*
DOE Order 473.3, *Protection Program Operations*

3.7.2 General Information

DOE orders require that classified matter be adequately protected while in use, storage, or transit. The effectiveness of systems utilized to provide the required protection is 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 matter, 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
- Badges and passes.

The assessment of these areas is normally a coordinated effort involving the PSS, 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 classified matter in use. Section 3.4, Receipt and Transmittal, contains additional information about protection of classified matter in transit. SCIFs and SAPs are subject to special requirements, which are discussed further in Section 6 of this assessment guide.

Physical protection requirements apply to all forms of classified matter at the facility (e.g., blueprints, viewgraphs, photographs, microfiche), as well as to all material items (e.g., weapons components). When planning assessment activities, assessors should consider all forms of classified matter at the assessed facility.

DOE orders permit the use of either alarm systems or protective force patrols to protect classified 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 a small percentage of the site's repositories during a 24-hour period, if at all. The CMPC assessors 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, classified 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 Check Sheet.

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

3.7.3 Common Deficiencies/Potential Concerns

Security Areas Not Established

The requirement to establish security 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 a 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 assessing 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 matter is precluded. Assessors 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 matter. Tests of this type should incorporate control measures to ensure that the uncleared or L cleared person does not inadvertently gain access to classified matter.

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. The use of built-in locks that do not meet 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 or 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 do not 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 classified matter in storage. If this is the primary protection method, the patrols should be consistently performed since protective force patrols do not provide continuous protection. In some 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.

3.7.4 Planning Activities

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

- Identification of all Limited 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 assessment team a general idea of the scope and nature of the security area for planning purposes.

- General search policies and procedures at each Limited Area and security 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 Area and security area.

- The general methods for controlling visitor access (for example, badges, escort policies) within each Limited 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 inter-site 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, assessing all organizations or all individual security areas and repositories is impractical. In such cases, a representative sample may be selected upon which to base the evaluation. Typically, for reasons of efficiency, assessors will be covering other CMPC elements and subtopics as well as the "physical protection and storage" element. Assessing the same accounts and custodians selected for interviews concerning destruction or reproduction is usually more efficient than selecting a separate sample of accounts that store classified matter. 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 classified matter, it is also advisable to ensure that a representative sample is reviewed.

3.7.5 Performance Tests

All the tests in Appendix A provide data applicable to this subtopic. The physical protection provided to classified matter 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 PSS topic team) and used to more fully test this area. Additional guidance for conducting performance tests is included in the EA-22 PSS and Protective Force Assessment Guides.

The document user awareness test may be particularly applicable at facilities that have areas dedicated to reviewing classified matter (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 the CMPC and PSS or protective force topic teams.

3.7.6 Data Collection Activities

Review and Use Areas

A. Assessors 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. Assessors 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, assessors 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, assessors should focus on how the individuals control access to the area. Assessors 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 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. Assessors 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. Assessors 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). Assessors 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 Areas or security 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, assessors may elect to determine whether alarms are operable and whether sensor coverage is adequate. The CMPC team would review alarm sensors only if the PSS topic team is not planning to conduct tests of alarm sensors in the classified storage areas of interest to the CMPC team.

D. Assessors 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, assessors 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, assessors 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. Assessors 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 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 classified matter being protected, the number of employees assigned to each area).

- Verifying that the search policies and procedures at Limited Areas and security 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/CAIN booths) to each Limited Area and security area portal.

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

- 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.

Security Shipments

G. Physical protection of classified matter during intra-site transit should be reviewed concurrent with the review of other aspects of transmittal and receipt. The assessors 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 Matter

Many of the basic control and handling requirements that apply to Secret matter also apply to Top Secret matter. Therefore, the basic guidance regarding assessment activities provided in Section 3 remains valid when assessing Top Secret holdings and is referred to in this section. Additionally, accountability for all Top Secret matter is required for National Security Information, Restricted Data, and Formerly Restricted Data, as well as matter designated by national, international, or programmatic requirements. The control and protection of SCI Top Secret matter is prescribed in the appropriate national security directives, which provide guidance on assessing SCI matter and the program office. Therefore, the assessment of Top Secret matter focuses heavily on access control and physical protection and storage.

4.1 Top Secret Accounts

4.1.1 References

DOE Order 470.4B, Admin Chg 1, *Safeguards and Security Program*
DOE Order 471.6, Admin Chg 2, *Information Security*
DOE Order 473.3, *Protection Program Operations*
Director Central Intelligence Directive (DCID) 6-9, *Physical Security*
Intelligence Community Directive (ICD) 705, *Sensitive Compartmented Information Facilities*

4.1.2 General Information

The Top Secret element regarding the control of Top Secret matter includes various requirements and responsibilities. Elements included are:

- The designation of Top Secret custodians
- Classification of Top Secret matter, including drafts and working papers
- Downgrading and declassification of Top Secret matter.

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 custodians (and alternates) is normally very small. The largest concentrations of Top Secret matter are frequently found in SCIFs and SAPs. Special considerations for assessing SCIFs and SAPs are addressed in Section 6.

4.1.3 Common Deficiencies/Potential Concerns

Failure to Conduct Review of Top Secret Matter

DOE Order 471.6, *Information Security*, requires that Top Secret matter is accountable, and an inventory of accountable matter is required annually. Each item listed in an accountability record must be visually and physically verified. Discrepancies in the inventory will be reported to the ODFSA. All sites must develop procedures to ensure that all accountable matter has been entered into the accountability system.

4.1.4 Planning Activities

During planning, assessors interview points of contact and review available documents (for example, SSSP/SSP and CMPC procedures) to identify:

- The number and identities of Top Secret accounts and custodians
- The comprehensiveness of local procedures in addressing Top Secret
- The current protection strategy.

Once this information has been compiled, assessors determine which of the Top Secret accounts will be assessed. Usually, there are so few Top Secret accounts that they can all be assessed. If that is not the case, a sample of Top Secret accounts can be selected for assessment.

4.1.5 Performance Tests

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

- Matter accountability front check
- Matter accountability back check.

During these performance tests, assessors observe all markings and accountability information to ascertain whether the custodians are properly maintaining the matter. Sample scenarios for these performance tests are provided in Appendix A.

4.1.6 Data Collection Activities

During the onsite assessment, Top Secret custodians should be interviewed to determine the frequency of their holdings reviews, as well as how well they know their responsibilities and how they fulfill those responsibilities. Assessors should also review program records and Top Secret matter to determine whether the custodians are correctly performing their various duties.

4.2 Top Secret Markings and Forms

4.2.1 References

DOE Order 470.4B, Admin Chg 1, *Safeguards and Security Program*
DOE Order 471.6, Admin Chg 2, *Information Security*
DOE Order 473.3, *Protection Program Operations*
DCID 6-9, *Physical Security*
ICD 705, *Sensitive Compartmented Information Facilities*

4.2.2 General Information

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

- Top Secret Cover Sheet
- Classified Matter Receipt
- Courier Receipt
- Destruction Record.

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

4.2.3 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.

4.2.4 Planning/Data Collection

The planning and data collection activities applicable to this element are essentially the same as those explained in Section 3.1. The primary differences in assessing Top Secret markings and forms are that when assessing this area, assessors will:

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

4.3 Top Secret Control Systems: Access and Accountability

4.3.1 References

DOE Order 470.4B, Admin Chg 1, *Safeguards and Security Program*
DOE Order 471.6, Admin Chg 2, *Information Security*
DOE Order 473.3, *Protection Program Operations*
DCID 6-9, *Physical Security*
ICD 705, *Sensitive Compartmented Information Facilities*

4.3.2 General Information

This subtopic of the CMPC 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
- Reporting requirements.

Custodians and alternate custodians are responsible for all aspects of the control and protection of Top Secret matter, including all aspects mentioned above. Top Secret custodian responsibilities dealing with receipt and transmittal, storage, and destruction are addressed in detail in Sections 4.4, 4.7, and 4.6, respectively.

Organizations holding Top Secret matter have Top Secret custodians and alternate custodians assigned to each account. 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.

4.3.3 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 matter 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 establish 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. Assessors 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 assessors 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 items in the sample selected for the matter accountability front check. Any items that are not found are considered missing, and the facility should initiate the required actions. The actions are outlined in Section 3.3.

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

Matter Not in Accountability

The common deficiencies found when assessing Top Secret matter accountability systems are the same as those found in accountability systems for classified matter (see Section 3.3).

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

- Reproduced copies of other matter
- Computer media (e.g., disks, removable hard drives)
- 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).

Assessors who find Top Secret matter, such as punch cards, viewgraphs, or computer media, out of accountability may reasonably conclude that the same problem may exist with similar matter 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 items and to provide a clear audit trail for all matter. Errors and omissions on records can make it difficult to identify and track matter. While such problems can occur with any type of record, data entry errors are probably more prevalent in automated records. Assessors 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

Maintaining an audit trail for each item requires records indicating the current location or disposition of the item, including receipts for transferred matter and records of destruction for destroyed matter. Sometimes, items are transferred off site (or "loaned") without proper receipting. Receipts for matter 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 Top Secret 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 where the drafts originated. Assessors also 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.

4.3.4 Planning Activities

The planning activities described in Section 3.3 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.

4.3.5 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:

- Matter accountability front check
- Matter accountability back check
- Receipt and transmittal
- Matter reproduction
- Matter 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 need-to-know could be recruited to attempt to obtain Top Secret matter 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 assessors to prevent actual access to classified information by an unauthorized individual.

4.3.6 Data Collection Activities

The data collection activities described in Section 3.3 apply to the accountability-related portions of this element. However, assessors 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.

4.4 Receipt and Transmittal

4.4.1 References

DOE Order 470.4B, Admin Chg 1, *Safeguards and Security Program*
DOE Order 471.6, Admin Chg 2, *Information Security*
DOE Order 473.3, *Protection Program Operations*
DCID 6-9, *Physical Security*
ICD 705, *Sensitive Compartmented Information Facilities*

4.4.2 General Information

A basic overview of DOE requirements for receipt and transmittal of classified matter is provided in Section 3.4. It is unusual to find that Top Secret matter has 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 matter, DOE has imposed controls on receipt and transmittal procedures. This section will look at these controls as they pertain to:

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

Responsibility for the receipt and transmittal of Top Secret matter 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 matter held by the facility.

Receipt of Top Secret Matter from Off Site

Top Secret matter may be transported between DOE security areas by a courier or transmitted over approved communications networks. Assessment interest normally begins at the point of receipt of electronic Top

Secret matter or when Top Secret matter is transferred between a courier and the Top Secret custodian. The assessment effort continues through processing, initial storage, and eventual re-transmittal or destruction.

Initial procedures for receipt of Top Secret matter 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, 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 matter is not as described, has been mis-sent, was tampered with, or was improperly packaged, the sender's security office must be contacted immediately and appropriate action taken.

When Foreign Government, Sigma 14, or Top Secret matter is transferred, formal accountability must be updated to indicate its location. Incoming matter must also be reviewed to ensure that its markings meet DOE standards. Any deficiencies must be corrected (see Section 4.2).

The receipt process generally terminates with the signed receipt being returned to the courier and the storage of the Top Secret matter by the Top Secret custodian. Such storage should be assessed. The requirements for the physical protection and storage of Top Secret matter are discussed in Section 4.7.

Transmittal of Top Secret Matter Off Site

Under the approval of the ODFSA, Top Secret matter may be transmitted in one of the following ways:

- By Defense Courier Service
- By the Department of State Courier System (if outside the U.S.)
- Over approved communications networks
- By individuals authorized to hand-carry Top Secret matter.

Transmitting Top Secret matter off site is basically the reverse of the receipt process. The process begins with the Top Secret custodian preparing matter for transmittal by wrapping it in two opaque envelopes. A DOE classified matter receipt, or a receipt comparable in content that 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. If Top Secret matter is being hand-carried, the Top Secret custodian then turns the package over to the individual authorized to hand-carry the matter.

Intra-site Transfer of Top Secret Matter

The transfer of Top Secret matter within a security area generally follows procedures similar to those used for offsite transmittal and receipt. However, a classified matter receipt is used, and the matter 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 Matter

Hand-carrying must be limited only to those unusual situations outlined in DOE Order 471.6, Admin Chg 2, *Information Security*, and is generally used only when other means of transmission are not feasible. 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.

4.4.3 Common Deficiencies/Potential Concerns

The receipt and transmittal of Top Secret information have been assessed so infrequently that trends or common deficiencies have not been identified. Potential concerns that should be reviewed during assessments are the same general problems discussed in Section 3.4.

4.4.4 Planning Activities

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

- Contacting the site's control stations to identify any existing problems and to obtain a listing of matter charged to the activity to be assessed
- Identifying procedures used by the facility to receive and send Top Secret matter off site
- Identifying methods used to verify classified mailing addresses before matter is sent off site
- Determining the location of facility security areas and how matter is transferred between security areas
- Identifying any specific instructions governing the transfer of Top Secret matter to other government agencies or outside entities
- Determining details concerning local personnel authorized to serve as couriers for Top Secret matter.

Once assessors 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 Top Secret matter and which of these will be assessed. Activities to be considered include:

- Courier procedures
- Receipt procedures
- Accountability procedures
- Use of required DOE forms
- Interim storage and physical protection procedures.

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

4.4.5 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:

- Matter receipt
- Matter packaging
- Matter 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.

4.4.6 Data Collection Activities

Receipt of Top Secret Matter From Off Site

A. It is usually best for assessors 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 matter is reviewed for proper marking and documentation.

B. Assessors should observe internal distribution to determine whether matter is properly protected while in route to its 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 Matter 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, assessors 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 assessors to look at the facility suspense file to determine whether proper and timely follow-up is being accomplished for matter that has already been transferred. If no matter is 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 Matter

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

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

Hand-Carrying Top Secret Matter

F. As indicated earlier, hand-carrying of Top Secret matter is to be generally limited to those situations in which more traditional means of transmission are not feasible. If the facility indicates that hand-carrying of Top Secret matter is a necessity, the procedures should be reviewed carefully, using current guidance promulgated by DOE.

4.5 Reproduction

4.5.1 References

DOE Order 470.4B, Admin Chg 1, *Safeguards and Security Program*
DOE Order 471.6, Admin Chg 2, *Information Security*
DOE Order 473.3, *Protection Program Operations*
DCID 6-9, *Physical Security*
ICD 705, *Sensitive Compartmented Information Facilities*

4.5.2 General Information

A basic overview of the reproduction of classified matter and relevant DOE requirements is given in Section 3.5.

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

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

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

- New Top Secret matter must receive appropriate markings.
- Accountable reproduced matter must be entered into accountability.

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

The reproduction of Top Secret matter encompasses both copying and printing. However, Top Secret reproduction occurs so seldom that at most facilities it is limited to the occasional copying of matter. Section 3.5 discusses the methods, the identification and characterization of systems, and the features and problems associated with assessing reproduction procedures. The equipment used must be specially approved for the reproduction of Top Secret matter.

4.5.3 Common Deficiencies/Potential Concerns

Top Secret matter is reproduced so rarely that specific trends or common deficiencies have not been identified. Potential concerns are the same as those identified in the reproduction of Secret matter, discussed in Section 3.5:

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

4.5.4 Planning Activities

Planning activities closely parallel those used for assessing the reproduction of Secret and Confidential matter. Activities include interviewing points of contact and reviewing available matter 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 assessors understand the classified matter reproduction program, they should determine which organizations and facilities will be assessed. Normally, the actual assessment of Top Secret reproduction can be done efficiently in conjunction with the other Top Secret subtopics.

4.5.5 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 matter.

The following standard performance tests apply to this area:

- Matter accountability front check
- Matter 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 matter. For example, appropriate personnel could be required to reproduce simulated classified matter using a particular piece of equipment to determine whether they follow all required procedures.

4.5.6 Data Collection Activities

A. When assessing Top Secret copying, it is useful for assessors 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 assessment, 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 assessment process. The assessment normally begins 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 matter.

4.6 Destruction

4.6.1 References

DOE Order 470.4B, Admin Chg 1, *Safeguards and Security Program*
DOE Order 471.6, Admin Chg 2, *Information Security*
DOE Order 473.3, *Protection Program Operations*
DCID 6-9, *Physical Security*
ICD 705, *Sensitive Compartmented Information Facilities*

4.6.2 General Information

A basic overview of DOE requirements for destruction of classified matter is given in Section 3.6. Because of the serious impact on national security that the loss or compromise of Top Secret matter represents, DOE has imposed even more stringent controls on Top Secret accountable matter 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 matter can ever be reconstructed.

4.6.3 Common Deficiencies/Potential Concerns

The destruction of Top Secret matter has been assessed 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 matter can be used to identify potential concerns that should be reviewed during assessments. These concerns closely parallel those encountered in the destruction of Secret and Confidential matter:

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

4.6.4 Planning Activities

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

- Contacting the Top Secret custodian to identify any existing problems and to obtain a listing of matter destroyed by the activity being assessed

- Identifying procedures used by the facility to destroy Top Secret matter (for example, disintegrators or incineration)

- Determining the location of destruction facilities

- Identifying approved exceptions to requirements.

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

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

4.6.5 Performance Tests

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

- Matter destruction.

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

4.6.6 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 Top Secret matter.

4.7 Physical Protection and Storage

4.7.1 References

DOE Order 470.4B, Admin Chg 1, *Safeguards and Security Program*
DOE Order 471.6, Admin Chg 2, *Information Security*
DOE Order 473.3, *Protection Program Operations*
DCID 6-9, *Physical Security*
ICD 705, *Sensitive Compartmented Information Facilities*

The references presented in Section 3.7 for physical protection and storage of Secret and Confidential matter are also applicable to protection of Top Secret matter. These references cover repositories, locks, intrusion detection systems, Limited Areas, security areas, badges and passes, the protective force, matter storage, review and use of matter, and transfer of matter. The references listed here identify additional requirements that are specifically applicable to Top Secret matter.

4.7.2 General Information

The scope of the "physical protection and storage" element is defined in Section 3.7. As with Secret and Confidential matter, the assessment of these elements is normally a coordinated effort involving the cyber security, PSS, protective force, personnel security, and CMPC topic teams. Section 4.3 contains additional information about physical protection of Top Secret matter in use, which is the responsibility of the facility's CMPC manager and the Top Secret custodians. Section 4.4 contains additional information about protection of Top Secret matter 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 Order 471.6, regarding non-conforming storage. Any

non-conforming storage must be approved by the ODFSA. DCID 6-9 and ICD 705 contain special physical security requirements applicable to Foreign Intelligence information and SCI. 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 matter be afforded a high degree of protection while in use, storage, or transit. The requirements for physical protection and storage of Top Secret matter are similar to those for Secret and Confidential matter, 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.

- In a locked vault or vault-type room within a Limited Area, security areas, property protection area, or material access area. The vault or vault-type room must be equipped with intrusion detection equipment, and protective force personnel must respond within 15 minutes of alarm annunciation.

- In a locked vault or vault-type room within a property protection area or outside of a security area, and under intrusion detection system protection. Protective force personnel must respond within 5 minutes of alarm annunciation.

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

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

4.7.3 Common Deficiencies/Potential Concerns

Although deficiencies involving physical protection of Top Secret matter are not common, assessors 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.

4.7.4 Planning Activities

Assessment activities for physical protection and storage of Top Secret matter are essentially identical to those used to review Secret and Confidential matter. Assessors should refer to Section 3.7 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 matter.

In addition to the information identified in Section 3.7.4, assessors should collect the following information (through interviews with points of contact and reviews of available documentation) at facilities that have Top Secret matter:

- The number of repositories in which Top Secret matter is 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 amount of matter stored in each repository)

- The location and physical protection measures in place at each repository, including whether the repository is within a Limited Area or security 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 intra-site and inter-site transit authorized at the facility to transport Top Secret matter

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

- Approved exceptions to requirements that affect Top Secret matter.

Once assessors understand the structure of the Top Secret matter 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 assessment. Because most facilities have only a small number of Top Secret repositories, it is generally practical and advisable to assess all organizations that possess Top Secret matter and all centralized or individual repositories where Top Secret matter is stored. Typically, for reasons of efficiency, assessors cover other CMPC Top Secret elements at the same time as the "physical protection and storage" element.

4.7.5 Performance Tests

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

4.7.6 Data Collection Activities

A. In addition to the information in Section 3.7 (specifically with respect to review and use areas, repositories and storage areas, and security areas), assessors should interview selected (preferably all) CMPC managers and Top Secret custodians to determine how they implement their responsibilities. In particular, assessors should determine how the Top Secret custodians ensure that persons who ask to review Top Secret matter are appropriately cleared and have a need-to-know. Assessors should also determine how the Top Secret custodians maintain control of matter that is 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 3.7.6, assessors should interview selected Top Secret custodians and couriers to determine how the procedures for protecting Top Secret matter in transit are implemented. The assessors should devote particular attention to verifying that:

- The procedures are appropriately updated.
- The procedures require the matter 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 matter transfers, and the individuals authorized to transport Top Secret matter understand and follow applicable procedures.

Section 5: Control of Classified Materials

This section addresses assessment 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). Special nuclear material (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 matter, 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 (NMC&A) is not normally included in the scope of this subtopic. Since more restrictive SNM protection requirements apply and are assessed by the PSS and material NMC&A 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.

5.1 Classified Material Marking

5.1.1 References

DOE Order 471.6, Admin Chg 2, *Information Security*

5.1.2 General Information

This 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 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 either program offices, ODFSA, or DOE Headquarters depending on program office directions.

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 are 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 assessing classified parts. For example:

- Materials may be at a point in the manufacturing process where they are not accessible to the assessor, e.g., in a kiln, glove-box, 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.

5.1.3 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 addition, category markings are sometimes omitted because the original engineering drawings do not show category markings. Also, parts are often incorrectly marked when the process involves rollup or rolldown of components into new forms with different classification levels.

5.1.4 Planning Activities

During the planning stage, assessors may interview points of contact and review available documentation (e.g., SSSP/SSP, 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 assess. Depending upon the quantity of materials present, it may be necessary to use sampling techniques to assess this subtopic. The sampling guidance provided in Appendix B can be applicable to this subtopic. Another approach is to choose the highest-value material items for assessment. This 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.

5.1.5 Performance Tests

If the assessed 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.

5.1.6 Data Collection Activities

A. Assessors 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. Assessors should also determine the actual marking practices.

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

5.2 Classified Material Accountability

5.2.1 References

DOE Order 471.6, Admin Chg 2, *Information Security*

5.2.2 General Information

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

Current DOE directives do not specifically address, in sufficient detail, classified material accountability requirements. In the field, accountability requirements for material generally mirror those for matter; this process has been concurred by the policy office at Headquarters. (Section 3 discusses how document accountability systems are to be assessed.) 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.

Assessment of this subtopic generally centers on determining whether accountability records accurately reflect accountable holdings, i.e., determining whether all material on the records is present; whether all material present is on the accountability records; and whether 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 matter, 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 in Section 3.3 is generally applicable to this subtopic and should be reviewed.

5.2.3 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 assessment 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; for example, 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 method, or one that does not provide comparable assurance of detection of the theft of small quantities, does not adequately protect these types of materials.

5.2.4 Planning Activities

During the planning stage, assessors can interview points of contact and review available general documentation (e.g., SSSP/SSP, CMPC procedures, and other pertinent matter) to characterize the classified material accountability system at the assessed 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.

Planning for the review of classified document accountability systems is discussed in Section 3.3, which also applies to the assessment of classified material accountability systems. Assessors should refer to that section.

5.2.5 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 of these performance tests are provided in Appendix A.

5.2.6 Data Collection Activities

A. Assessors 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. Assessors should also determine whether responsible personnel fully understand and are correctly maintaining accountability records.

B. Assessors should review accountability records and backup matter to determine whether records contain appropriate information and are properly maintained. For 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.

5.3 Physical Protection and Storage

5.3.1 References

DOE Order 471.6, Admin Chg 2, *Information Security*

The references presented in Section 3.7 also apply to protection of classified materials. These references cover repositories, locks, intrusion detection systems, Limited Areas, security areas, badges and passes, the protective force, and storage and transfer of materials.

5.3.2 General Information

The term "materials" is used to refer to any classified matter other than matter. 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 this element is as defined in Section 3.7. As with Secret and Confidential matter, the assessment of these elements is normally a coordinated effort involving the PSS, protective force, personnel security, and CMPC teams. DOE directives require that classified matter be adequately protected while in use, storage, or transit. All requirements for using or transporting classified matter also apply to classified materials. The

requirements for storage of classified materials are similar to those for Secret and Confidential matter, 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 guidance permits 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.

5.3.3 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 nonconforming storage areas. Their use as storage areas for classified material items is prohibited unless the site has met all the requirements involving a thorough, documented, validated, and approved analysis of the storage area that characterizes the assets, any equivalent protection measures used instead of alarms (e.g., protective force patrols), the timelines for an adversary to remove those assets, and the consequences to national security of that removal.

5.3.4 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 matter. Assessors 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, assessors 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 gives 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 Area or security 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). Reviews of alarm use and coverage are typically coordinated closely with the PSS team, which can conduct a series of tests to determine the effectiveness or coverage of alarm systems.

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

- All means of intra-site and inter-site transit authorized at the facility (e.g., hand-carry, rail, plane, registered mail) 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).

- 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, assessors 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 assessment. At large facilities, assessing all organizations or all individual security areas and repositories is impractical. In such cases, a representative sample may be selected for evaluation. Typically, for reasons of efficiency, assessors will cover other CMPC subtopics along with physical protection and storage.

Assessing the same accounts and custodians selected for classified materials accountability performance tests and looking at physical protection concurrent with the front and back check accountability activities is usually more efficient 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 or disassembles classified materials, assessors 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 ensure that a representative sample is reviewed.

5.3.5 Performance Tests

As with Secret and Confidential matter, 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 EA tests that involve classified materials. Sections 3.2, 3.4, and 3.7 provide additional guidance applicable to performance tests.

5.3.6 Data Collection Activities

A. In addition to the information identified in Section 3.7, assessors should tour selected classified materials use and storage areas to determine how procedures for controlling visual access are implemented. In particular, assessors 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, assessors 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 3.7.6, assessors should interview selected persons who transfer classified materials to determine how the procedures for protecting classified materials are implemented. Assessors 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 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 assessor should determine what alarm sensors, if any, might be present and functioning (i.e., perimeter only, or both perimeter and interior). If compensatory measures are used instead 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 should be examined.

Section 6: Special Programs

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

Section 7: Interfaces

Integration

Integration is the process of assessment team members working together to achieve a better understanding of the overall protection programs used at DOE facilities. In this context, integration includes all the associated attributes: coordinating, cooperating, interfacing, and assimilating 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. Integration also results in a more effective and organized assessment effort, a refinement of assessment techniques, and a more comprehensive assessment report. Lastly, the integration effort significantly contributes to EA's ability to provide an accurate, in-depth evaluation of protection programs throughout the DOE complex.

No assessment topic team operates in a vacuum. The primary objective of a comprehensive assessment is to provide a meaningful, management-level evaluation of the overall status of safeguards and security at the assessed facility. To ensure this objective is achieved, the CMPC team and all other topic teams must work closely together throughout every phase of the assessment 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 to prioritize the efforts of the various topic teams, assign particular issues for investigation to particular teams, and mobilize special assessment team elements to examine issues that transcend topic boundaries.

No more than nine or ten days are available for data collection during a typical comprehensive assessment. During this time, the various topic teams collect a massive quantity of data pertaining to their particular subject matter areas. A careful delineation of each team's assessment 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 identified issues 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 the relevant team members from other topic teams. More formal integration takes place during the assessment planning meeting and during daily coordination sessions involving the assessment team lead and the topic team leads. During the data collection phase of the assessment, a formal team meeting is scheduled on a daily basis (typically at 5 p.m.), which provides a forum for the exchange of information between the topic teams.

The integration process should reflect that the fundamental DOE protection policy is based on the concept of protection in depth (i.e., 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 the protection elements within each layer. In this sense, integration is the basic process through which EA 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 assessed 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 CMPC assessors coordinate their activities with other topic teams. Classified matter protection

is pervasive in nature, intersecting with a number of the other assessment areas. This interdependence requires close coordination with other topic teams, particularly protective force, PSS, personnel security, cyber security (if on the assessment), and 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 if required by the SSSP or SSP), whereas the protective force team conducts detailed reviews of all aspects of protective force activities. Other interfaces with physical protection are addressed in Sections 3.7 and 4.7.

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

- 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.

When reviewing the above items during the assessment, physical protection concerns identified by the CMPC team should be communicated to the PSS or protective force team as soon as practical so that their significance can be evaluated. For example, if the sensors in a vault-type room appear 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:

- 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 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 only if the PSS are not being assessed and if previous assessments indicate some alarm system deficiencies. Here, however, it is essential that the team include at least one member with the requisite PSS skills if highly technical or specialized PSS areas are to be assessed in depth. The addition of a PSS technical expert may also be required if a large number of vaults and vault-type rooms are assessed.

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 assessment 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.

Visitor control, including in particular foreign visits and/or assignments, and security termination procedures also fall under the personnel security topic. Deficiencies concerning either visitor control or security terminations can directly impact the CMPC topic because of potential unauthorized access to classified matter. Assessors looking at the "review and use" element pertaining to 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, Sigma) and have the personnel security team verify that those persons do have the required authorizations listed in their personnel security files.

Protection Program Management

Frequently, the PPM topical area is assessed in addition to assessing the management topic in CMPC. If assessors 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, the CMPC team should communicate to the PPM team such weaknesses in the CMPC program as failure to provide policies and procedures for generation, preparation, review, and use of classified matter; questionable physical protection of classified matter; lack of fully documented and approved vulnerability assessments for classified assets residing in nonconforming open storage; and failure of self-assessments or surveys to detect and address existing problems in this area.

Likewise, coordination with the PPM team may be warranted if the CMPC team uncovers evidence that Federal oversight of 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 appropriate security managers have had adequate input into the planning and design of the protection strategy for special programs, as well as whether they conduct ample ongoing oversight of those programs.

Cyber Security

Cyber security assessments are conducted by the Office of Cyber Assessments (EA-21). A cyber security team may or may not be operating on site at the time of a CMPC topic assessment. If the CMPC assessment team identifies a problem that requires cyber security expertise but no EA-21 team is on site, the CMPC topic lead should coordinate with assessment management to obtain assistance from EA-21.

Cyber security and CMPC are closely related. They have the common goal of protecting classified information, and the efforts of the CMPC and EA-21 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 cyber-related areas, such as protection and destruction of magnetic media. Such deficiencies can often be traced to failure of facility management to assign responsibilities for all required security functions, or too much 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 EA-21, which should then devote more attention to the cyber security training programs. In this manner, the assessment team can better determine whether training resources are a sitewide problem. Similar considerations apply for corrective actions and self-assessment programs.

The CMPC team reviews most aspects of the reproduction and destruction of computer-related items, including hard disks, floppy disks, and other storage media. During the course of an EA-21 review of security plans, this information may be encountered; EA-21 will notify CMPC of unusual procedures or processes encountered during their review.

EA-21 customarily reviews some aspects of the physical protection of computer-related items, including specific need-to-know and access to and proper use and storage of media and printouts. However, when reviewing these areas of document protection, the CMPC team also frequently comes upon classified computing equipment (generally personal computers), facilities, and practices. Items of concern that may require follow-up regarding physical security should be communicated.

EA-21 should be included in the initial planning and data collection phases if any special programs or SCIFs to be assessed 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 coordination will enable the site to respond to requests for topic team access in a timely manner, allowing the assessment to progress smoothly.

Another area for concern is the 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 may indicate that CMPC procedures and plans are also lacking. As the unclassified cyber security program changes to meet new security threats, additional interfaces may be identified between the CMPC and unclassified cyber security programs.

Section 8: Analyzing Data and Interpreting Results

Introduction

This section provides guidelines to help assessors 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, assessors 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 indicate a failure of the entire security system. This is why integration among topic teams is critical. Integration provides 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 includes sorting out and logically grouping all validated data collected for each subtopic during each phase of the assessment (remembering that data is collected during the planning process as well as the conduct phase). Although the topic team is generally aware of most 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 assessment team meeting and during the development of nightly bullets. 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, arranging the data according to positive or negative features is helpful and will aid in clearly identifying strengths, weaknesses, and positive or negative trends. Proper organization and thorough review of all assessment 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 assessment report is disseminated. By recognizing this concept early in the assessment 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 assessment 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 and national drivers' 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.

The analysis is a summary of the salient assessment 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 compensatory 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 findings, weaknesses, deficiencies, or requirements 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 site/field office or contractor management previously knew of the deficiency and, if so, what action was taken
- The importance or significance of 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

Assessment 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 assessment team should determine whether a single rollup finding should be reported to address that requirement. It is 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.

Deficiencies

Deficiencies are elements of the CMPC program that have an impact on the effectiveness of the overall program but are non-systemic. The site will determine whether such deficiencies warrant entry into an issues management system and/or whether they require formal corrective actions.

Opportunities for Improvement

Opportunities for improvement may also be identified. These recommendations are often based on EA's knowledge of successful solutions for common issues at other DOE facilities or industry best practices and should be considered as suggestions for program improvement.

Interpreting Results

Program Management

During an assessment, the management program is not to be reviewed based on any particular view of how a management program should function. Rather, assessors 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 and national drivers. 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 and national policy during the assessment of other CMPC program areas. Additionally, deficiencies identified in the management review may cue assessors to examine corresponding areas more closely. For example, if the management assessment reveals that procedures do not contain recent DOE Headquarters guidance about accountability records, assessors may want to redouble their efforts in examining these records to determine whether they are being completed properly. Conversely, if the results of assessment activities for any requisite document accountability systems indicate that findings identified during the previous assessments have not been adequately addressed, assessors 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, or oversight, 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, assessors should attempt to determine whether the management deficiencies have resulted in possible vulnerabilities in the protection of classified information. Of special importance is the conduct of annual self-assessments that allows the site CMPC Program Manager to identify problems and issues within the program. Additionally, if deficiencies are identified, assessors should attempt to determine whether key managers were adequately informed of the status of tracking and completion of corrective actions.

Control of Secret and Confidential Documents

Review and Use. Deficiencies in procedures and practices for reviewing and using classified matter 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, assessors should investigate further to determine the actual likelihood that classified documents are not being adequately protected.

Deficiencies in out-processing 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 out-processing of persons whose access authorizations have been terminated for cause, or whose employment has been involuntarily terminated.

Physical Protection and Storage. Systemic deficiencies in the physical protection and storage of classified matter that could result in matter 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, assessors 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, assessors 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 self-assessment procedures, lack of adequate training programs, or inadequate resources. If a significant number of physical protection deficiencies are identified, the assessors should consider reviewing the relevant aspects of the management program to determine the root cause.

Document Generation. The lack of or failure to follow appropriate procedures could result in matter not being entered into accountability or not marked at all. Such deficiencies are significant and could result in matter not being adequately protected. If such deficiencies are noted, assessors 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 assessors review large amounts of matter, they often encounter incorrectly marked matter or other procedural errors. Minor discrepancies in markings, page counts, or the use of cover sheets are not easily exploited by adversaries if the matter is properly controlled (including formal accountability, when required) and afforded adequate physical protection. Thus, assessors may conclude that the deficiencies are isolated instances and the impact is minimal if:

- The percentage of incorrectly marked matter 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 self-assessments, lack of adequate training programs, or inadequate resources. If a significant number of errors are 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 matter, assessors should take whatever actions are needed to determine the full extent of the problem. They may need to use additional assessment techniques, including performance testing, observation of additional iterations of applicable procedures, or direct staff interviews. Assessors 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 matter. 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, assessors should determine the full extent of the problem, using additional assessment techniques such as performance testing and management interviews to determine the root cause. Assessors 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 and media 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, assessors 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, assessors should consider reviewing the relevant aspects of the management program to determine the root cause.

Accountability. Though few sitewide classified matter 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 (i.e., the system has not adequately protected them, and they may have been lost, stolen, or compromised).

Missing classified matter or matter not in accountability identified during review of a sample of any accountability system are indicators of similar problems in the entire population of classified matter. 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 the matter 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

Markings and Forms. Significant deficiencies in classified matter marking, such as matter not marked at all or numerous marking errors or omissions, have a detrimental effect on information protection. Occasional minor marking errors may not have a serious impact on information protection. However, Top Secret matter is 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, assessors 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 contributing to the deficiencies.

Receipt and Transmittal. Systemic deficiencies in Top Secret document receipt and transmittal 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 matter and Top Secret matter not receiving adequate protection.

If deficiencies are detected in the receipt and transmittal of Top Secret matter, 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 assessment techniques, such as specially developed performance testing. Additionally, assessors 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 matter, the root cause of the problem must be promptly determined. Additional assessment 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. Assessors 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 matter could result in matter 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, assessors 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 matter. 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.

Control of Classified Materials

Marking. Deficiencies in marking classified material that would result in the inability to identify an item as classified are 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 do 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, the problem is more significant.

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 matter, control of Top Secret matter, and control of classified materials generally apply 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 outside 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 site or field 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.

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. The scenarios provided are not all-inclusive, and other equally useful scenarios 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 assessment guides and can be employed at the majority of sites assessed. 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 the appropriate U.S. Department of Energy (DOE) order, manual, and/or other applicable requirements.

Scenario

The assessment 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 the appropriate DOE order and/or other applicable requirements.

Scenario

To specifically verify the test participant's ability to mark classified documents, the assessment 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 simulated classified 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 and/or other applicable requirements.

Scenario

The assessment team selects a computer-generated random sample of documents listed on the assessed organization's accountability records. Selected documents are then assembled and reviewed at a single, central location or at their storage locations, as appropriate. The assessment 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 requisite items to determine compliance with all applicable requirements. Each repository is also assessed for compliance with applicable 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 assessment 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 all applicable 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

Assessment 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 assessment (most likely obtained sometime during assessment planning). During the assessment of that facility, personnel are asked to produce (1) the documents themselves, (2) their destruction forms, or (3) their transmittal slips.

Intra-site 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 assessment 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 assessors 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 applicable 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 (if packaging is part of the participant's responsibility) or ensure proper packaging (if packaging is another's responsibility), and prepare the appropriate paperwork to send the package 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 assessed, 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 tracking includes receipt by the central mailroom, transfer to Document Control, entry into the accountability system, courier transfers, any Control Station procedures, and custodian receipt, as applicable.

Reproduction

Objective

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

Scenario

The assessment 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, as applicable, at the assessed 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 applicable directives.

Scenario

The assessment 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, and if, to employ degaussing is determined. Requisite 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. Also, as applicable, use a similar scenario, but observe the destruction of classified parts.

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

Assessment team members visit selected locations in which classified matter is stored and/or used. Team members arrange with the appropriate site personnel with 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.]

Variation: In lieu of an actual performance test, simply interview the test participant about the appropriate actions to be taken in the above situation.

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 assessment team obtains a "red" badge for a cleared person, possibly an Office of Enterprise Assessments (EA) administration team member, and has 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.]

Variation: In lieu of an actual performance test, simply interview the test participants about the appropriate actions to be taken in the above situation.

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 assessment team instructs an unauthorized person to request that the facility CAS put security area alarms in access mode, and then determines 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.]

Variation: In lieu of an actual performance test, simply interview the test participants about the appropriate actions to be taken in the above situation.

Emergency/Special Procedures

Objective

To determine whether appropriate site-specific procedures for emergency evacuation of a security area are followed.

Scenario

Assessment 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 a test is being conducted. 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.]

Variation: In lieu of an actual performance test, simply interview the test participant about the appropriate actions to be taken in the above situation.

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.]

Variation: In lieu of an actual performance test, simply interview the test participants about the appropriate actions to be taken in the above situation.

SAMPLE PERFORMANCE TEST PLANS

CMPC

Document Accountability Performance Test Plan – Front Check

DOE San Diego Operations Office (SDO)

Objective

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

System Description

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.

EA team members will select a random sample of 200 documents. Corresponding control tickets will then be examined, and documents reflected on the selected tickets will be used as the assessment 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 document 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 all applicable requirements. Each repository will also be assessed for compliance with requisite storage requirements.

Document Accountability Performance Test Plan – Back Check

DOE SDO

Objective

To determine whether accountable classified documents on hand at DOE 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. EA team members 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

Assessment 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 document will be checked to ensure that it is described in accountability records.

Document Accountability Performance Test Plan – Front Check

NUCO-El Cajon Document Accountability System (DAS)

Objective

To evaluate the accuracy of the NUCO-El Cajon DAS, and to determine whether documents are protected, stored, and marked in accordance with all applicable requirements.

System Description

The DAS is maintained using a computerized barcode system. NUCO-El Cajon personnel state that 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 DAS. EA team members will select a sample of 200 numbers, which will then be used to select specific sample documents from the DAS by matching the random number to the list of document custodians and their respective holdings.

Scenario

The assessment 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 document 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 assessed for compliance with DOE storage requirements.

Document Accountability Performance Test Plan – Back Check

NUCO-El Cajon DAS

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 DAS documents. EA team members will select a 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

Assessment 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 document will be checked to ensure it is properly described and reflected in accountability records.

Document Accountability Performance Test Plan – Front Check

NUCO-El Cajon Non-Destructive Testing (NDT) DAS

Objective

To evaluate the accuracy of the NUCO-El Cajon NDT DAS for the laboratory located in Building 724, and to determine whether classified x-rays are protected, stored, and marked in accordance with requirements.

System Description

NUCO-El Cajon personnel stated that document accountability is maintained using a series of logbooks, 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. EA team members will select a sample of numbers, which will then be used to select specific logbooks. Sample documents will then be determined by selecting numbers for each selected logbook and identifying the specific accountable holding each number represents.

Scenario

The assessment team will use the random sample of 100 Secret documents listed in the accountability logbook system at the NDT center in Building 724. Selected documents will be reviewed at their storage locations or at a central location, as appropriate. Each document 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 assessed for compliance with DOE storage requirements.

Document Accountability Performance Test Plan – Back Check

NUCO-El Cajon NDT 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

Assessment team members will visit the document storage locations used by the NDT 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 document will be checked to ensure that it is properly described and reflected in accountability records.

Document Accountability Performance Test Plan – 100% Audit

WB Security Incorporated (WB)

Objective

To evaluate the accuracy of the WB DAS, and to determine whether documents are marked in accordance with applicable requirements.

Scenario

The assessment team will review all accountable documents listed in the WB El Cajon accountability system. Documents will be reviewed at their storage locations. Each document 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 applicable requirements. Additionally, each repository will be assessed for compliance with applicable storage requirements, and to ensure that all accountable documents have been entered into the WB accountability system.

Material Accountability Performance Test Plan – Front Check

NUCO-El Cajon Parts System

Objective

To determine whether the NUCO-El Cajon parts accountability system accurately reflects the Secret parts on hand, and to ensure that all classified parts are protected in a manner consistent with all applicable requirements.

System Description

Parts accountability is maintained using a computerized system. NUCO-El Cajon personnel state 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. EA team members will select a 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 and/or protected as required by applicable directives.

Material Accountability Performance Test Plan – Back Check

NUCO-El Cajon Parts System

Objective

To determine whether the NUCO-El Cajon parts accountability system accurately reflects the Secret parts on hand, and to ensure that all classified parts are protected in a manner consistent with all applicable requirements.

Scenario

The assessment 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 part to ensure that it is properly described and reflected in accountability records. Classified parts selected will also be checked for proper markings 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 that all parts are marked and stored and/or protected as required by applicable directives.

Classified Transmittal Performance Test Plan

USPS Receipt/Transmittal

Objective

To determine whether classified matter is transferred to and from 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 USPS Office until it reaches its final custodian within El Cajon. Observation will include receipt from USPS personnel; transportation to El Cajon; delivery to the DOE SDO, NUCO-El Cajon, and WB; entry into the appropriate accountability system; and custodian receipt procedures, as applicable. Should any required actions not occur during the assessment, site personnel will be asked to perform actions on simulated classified matter.

Variation: In lieu of an actual performance test, simply interview the test participant about the appropriate actions to be taken in the above situation.

Classified Transmittal Performance Test Plan

Site Transfers

Objective

To determine whether classified matter is transmitted within the confines of the El Cajon Plant in accordance with applicable requirements, and to determine whether classified information is receipted only to individuals with a valid need to know.

Scenario

Assessment team members will observe NUCO-El Cajon personnel receipting and internally distributing classified matter. Should any required actions not occur during the assessment, site personnel will be asked to perform actions on simulated classified matter.

The assessment team will interview El Cajon Plant employees and review operating procedures to ensure that internal distribution and hand-carry procedures meet applicable requirements. A sampling of procedures for transfer of classified documents will be reviewed and observed as such transactions occur during the assessment. If necessary, simulated documents will be placed in local distribution and tracked to determine site procedures.

Special attention will be given to procedures for hand-carrying classified matter off site. A sample briefing will be requested, local procedures will be reviewed, and records of hand-carry authorization will be assessed.

Classified Document Destruction Performance Test Plan

Objective

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

Scenario

Assessment team members will observe DOE SDO, NUCO-El Cajon, and WB personnel using routine local procedures to destroy classified matter. Should destruction of classified matter not be planned during the assessment, site personnel will be asked to describe procedures or perform actions on simulated classified matter.

Reproduction of Classified Documents Performance Test Plan

Objective

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

Scenario

Personnel normally charged with duplicating classified matter will be interviewed and observed reproducing accountable classified documents. Should the reproduction of accountable classified matter not actually occur during the assessment, site personnel will be asked to perform actions on simulated classified matter.

Facilities authorized for the reproduction of classified matter will also be assessed 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 applicable requirements for the safeguarding of classified information are implemented.

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, security (OPSEC), and the technical surveillance countermeasures program (TSCM).

3. Site safeguards and security plan(s) or site security plans.

4. OPSEC assessments and reviews, and the OPSEC Program Plan.

5. Copies of the sites CMPC training program to include custodians and alternates.

6. Survey reports and status of corrective actions. **

7. Self-assessment reports and subsequent corrective action reports. **

8. Documentation dealing with approved, pending, or requested exceptions relating to the CMPC program. **

9. Number of classified document inventories (Federally, nationally, or locally mandated) performed over the last 24 months.

10. All local policies and procedures regarding access control to vaults and vault-type rooms that contain classified material.

11. Site map showing the locations of all vaults and vault-type rooms in which classified documents and material are stored.

12. Description of alarm systems used to protect the vaults and vault-type rooms.

13. Location and safe number of all classified matter and accountable classified matter, including Sigma.

14. DOE or other national-level requirements under which the site is currently operating by contract.

15. List of all areas where non-conforming or non-standard storage is utilized and any deviations (if relevant).

** Check Safeguards and Security Information Management System database.

For Top Secret document accounts:

1. Description of Top Secret control programs and names of responsible individuals.

2. Location of Top Secret repositories (with map, if possible).

For Secret matter under accountability:

1. Total amount of lost/unaccounted-for classified matter 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.

For TSCM:

1. Copy of local policy and procedures for TSCM team.

2. Copies of training and briefing materials used to train TSCM and site personnel.

3. Have available on site during data collection the following information:

    a. Information concerning the scheduling of TSCM services
    b. Copies of the last five years of TSCM reports of services
    c. Information concerning life-cycle replacement of TSCM equipment.

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 assessment 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 any site visit.

___ Communicate and arrange internal support requirements.

___ Communicate external support requirements to site representatives/point(s) of contact.

___ Prepare and submit assessment guide.

___ Prepare and submit report outline input.

___ Prepare and submit assessment plan/action plan input.

___ Prepare any performance test/safety plans.

___ Prepare and deliver management-briefing input.

SAMPLING METHODOLOGY

Introduction

The Office of Enterprise Assessments (EA) conducts assessments to evaluate the effectiveness of the U.S. Department of Energy (DOE) safeguards and security programs. Confidence in these assessments is influenced by perceptions of consistency, thoroughness, and fairness in conducting the assessments. The use of scientifically valid methods for gathering and interpreting information strengthens the confidence in the results obtained.

In performing assessments 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 are properly accounted for in a facility's inventory. In most cases, 100 percent assessment 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.

EA has developed statistically valid, practical procedures for gathering information during assessments. 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 presents a general sampling methodology that is applicable to most topics, and discusses EA's application of sampling methods to the review of classified document and material accountability.

General Sampling Methodology Considerations

Although EA comprehensive assessments are very broad, there are frequently too many items in a given population to permit a 100 percent assessment because of limited time and other resources available. The tasks that must be addressed in conducting statistical sampling in EA assessments 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 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 assessment 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 assessed 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, which 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 assessors should select as large a sample as possible given the time and resource constraints of the assessment. With large samples, the assessors can develop more reliable estimates of the proportion of defective items.

Selecting Random Samples

If using a formal statistical sampling technique, 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 EA assessment 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 numbers with the population computer file to produce a list of sample items. For example, if the 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 assessment activities, computer programs that will carry out the sample selection process should be prepared or modified before the assessment. Also, the computer programming requirements should be identified during the planning stage of the assessment.

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 truly 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 change 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 to each assessor during the assessment planning process.

Data Entry:

Data collection activities are listed parallel to those outlined in the CMPC Assessment 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 assessment. Each column heading should list the specific program (e.g., site office classified document program, contractor document program, contractor material program, security force document program).

CLASSIFIED MATTER PROTECTION AND CONTROL

PLANNING SHEET

DATA COLLECTION ASSIGNMENTS

DATA COLLECTION ACTIVITY	PERSONNEL ASSIGNMENTS			
	PROGRAM	PROGRAM	PROGRAM	PROGRAM
PROGRAM MANAGEMENT				
Organization and Planning				
CONTROL OF SECRET AND CONFIDENTIAL DOCUMENTS TO INCLUDE ACCOUNTABLE 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				
TECHNICAL SUREVILLANCE COUNTERMEASURES				

DATA COLLECTION ACTIVITY	PERSONNEL ASSIGNMENTS			
	PROGRAM	PROGRAM	PROGRAM	PROGRAM
OTHER AREAS AND ASSIGNMENTS				

LIST OF EXCEPTIONS

Purpose:

Designed to record any exceptions from applicable 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 whether exceptions were granted at an appropriate level.

Data Entry:

Listing the subtopical areas will help assessors quickly identify any exceptions that pertain to the specific programmatic area they are reviewing.

A typical sheet might be filled out as follows:

CLASSIFIED MATTER PROTECTION AND CONTROL

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.	8/9/05	San Diego Operations Office
Physical Protection	Allows for use of locally developed forms versus Standard Forms 700.	12/1/05	DOE/Office of Policy

CLASSIFIED MATTER PROTECTION AND CONTROL

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 assessed. Serves as a quick reference to ensure that the assessment being planned will address all areas of weakness and determine whether 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

PLANNING SHEET

PREVIOUSLY IDENTIFIED DEFICIENCIES

PROGRAM: El Cajon Documents Page 1 of 1

DEFICIENCY	DATE FOUND	FOUND BY	CORRECTIVE ACTION	EST. DATE COMPLETED (EDC)	VALIDATED BY
No unique document numbers	1/14/05	EA	All accountable documents will have a number assigned	11/1/05	No Validation Noted
Destruction residue too large	1/14/05	EA	New shredder ordered	9/30/05	No Validation Noted
Infractions not reported	8/22/05	KCFO	Quarterly reports being submitted	Complete	EA 1/14/05
No accountability system	3/1/05	KCFO	New accountability system adopted site wide	Complete	Kansas City Field Office Survey 8/22/05

(CAUTION: MAY BE CLASSIFIED WHEN FILLED IN)

(CAUTION: MAY BE CLASSIFIED WHEN FILLED IN)

CLASSIFIED MATTER PROTECTION AND CONTROL

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/Express Mail services and the site mail room, operations of the mail room, and internal distribution procedures.

Data Entry:

Space is provided for recording notes on assessment data points applicable to mail room operations pertaining to classified documents. Entries should be self-explanatory.

Ensure proper marking, protection, and handling if completed forms contain any classified information.

CLASSIFIED MATTER PROTECTION AND CONTROL

DATA COLLECTION SHEET

MAIL ROOM

Location: _____ Operated by: _____

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

_____

Accountability (Receipt and Transmittal, Pick-up and Delivery):

_____

_____

Delivery Procedures from the U.S. Post Office:

_____

_____

Delivery Procedures to the U.S. Post Office:

_____

_____

Physical Protection between U.S. Post Office and Site:

_____

_____

Access Controls:

_____

_____

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

_____

_____

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

Physical Protection during internal delivery: Assess the mail delivery vehicle.

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 assessment data points applicable to reproduction of classified documents at such facilities. Entries should be self-explanatory.

Ensure proper marking, protection, and handling if completed forms contain information that would make them classified.

CLASSIFIED MATTER PROTECTION AND CONTROL

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

Purpose:

An abbreviated reminder of points to be covered when reviewing reproduction of classified documents on office copy machines.

Data Entry:

Space is provided for recording notes on assessment data points applicable to reproduction of classified documents on office copy machines. Entries should be self-explanatory.

Ensure proper marking, protection, and handling if completed forms contain any classified information.

CLASSIFIED MATTER PROTECTION AND CONTROL

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 if directed to review security self-assessment programs.

Data Entry:

Space is provided for recording notes on assessment data points applicable to facility security self-assessment programs. Entries should be self-explanatory.

CLASSIFIED MATTER PROTECTION AND CONTROL

DATA COLLECTION SHEET

SELF-ASSESSMENT PROGRAM

Program Procedures:

Program Resources:

Program Scope:

Tracking/Validation of Previous Deficiencies:

Program Findings versus Enterprise Assessment Results:

Program Records:

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 assessment data points applicable to policy, procedures, and facilities pertaining to facility destruction programs. Entries should be self-explanatory.

CLASSIFIED MATTER PROTECTION AND CONTROL

DATA COLLECTION SHEET

DESTRUCTION FACILITY

Location: _____ Responsible Organization: _____

Accountability (Upon Receipt):

Appropriately Cleared Destruction Personnel?

Type of Machinery (Approved?):

What is the method and procedure for destroying hard drives/platters and destruction process for floppy drives?

What is the method and procedures for destroying accountable documents?

What is the method and procedures for destroying non-accountable documents?

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 assessment data points applicable to Top Secret document accounts. Entries should be self-explanatory.

CLASSIFIED MATTER PROTECTION AND CONTROL

DATA COLLECTION SHEET

TOP SECRET DOCUMENTS

Account Size: _____ Number Checked: Front _____ Back _____ Personnel (Control Station, Top Secret Classifier):

Accountability:

Markings/Cover Sheets:

Inventories:

Destruction:

Receipt/Transmittal:

Reproduction:

Other Comments:

Sigma 14 documents and Sigma 20 media

REMINDER: Sigma documents & media follow the same guidelines and assessment points as other accountable documents. Before conducting the review, usually during the planning stage, DOE Headquarters approval for accessing these files must be requested. The request must come from an EA management official to the appropriate "Use Control Officer" within DOE Headquarters for this access.

SUMMARY ANALYSIS WORKSHEET

This worksheet is intended to be used by an assessor, if desired, to help organize conclusions reached during data collection and analysis. If ratings are to be assigned, a checkmark indicating a rating of Effective Performance (E), Needs Improvement (N), or Significant Weakness (W) for each subtopic area reviewed may reveal a picture of the total survey program environment that is not otherwise evident. The worksheet may be completed by an individual assessor or indicate the collective conclusions of all topic team members.

FACILITY ASSESSED: _____ DATE: _____

SUBTOPIC	E	N	W	REMARKS
MANAGEMENT PROGRAM				
Planning				
Security Organization				
Self-Assessment Program				
Foreign Ownership, Control or Influence				
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				

SUBTOPIC	E	N	W	REMARKS
Transmission				
Reporting Problems				
Classification Appraisals				
Conduct				
Records				
Corrective Actions				

TRAINING:

Have all of the employees received the required CMPC training as specified in their duties?

What are the site's required training courses?

- Is the training classroom or computer based?

How is each individual's training tracked?

- Are there consequences if an individual fails to complete the required training?

ACCOUNTABLE MATTER:

Are the primary and alternate custodians appointed in writing?

Has all of the accountable matter been entered into accountability?

Are accountability records complete and accurate (including loans, transfers, etc.)?

- Are all of the data fields included in the tracking system?

How are inventories conducted, by scanner or manually?

- Is each item visually identified during the inventory?

Do the accountable documents meet the marking requirements?