INSPECTORS GUIDE

Physical Security Systems

Office of Health, Safety and Security

Office of Security Evaluations
Office of Independent Oversight

November 2007

PHYSICAL SECURITY SYSTEMS

INSPECTORS GUIDE

November 2007

U.S. Department of Energy
Office of Security Evaluations
HS-61
19901 Germantown Road
Germantown, Maryland 20874

User Comments

This reference material will be updated and expanded periodically. Comments from users are appreciated and will be considered for incorporation. This page is provided for your convenience. Please direct all comments to:

U.S. Department of Energy
Office of Security Evaluations
HS-61
DOE-HQ
1000 Independence Avenue SW
Washington, DC 20585-1290
or via email: jeff.mcclure@hq.doe.gov

Foreword

As part of the mission of the Office of Health, Safety and Security, and to enhance the inspection process, the Office of Independent Oversight (HS-60) has prepared the Physical Security Systems Inspectors Guide as one in a series of inspectors guides. The guides incorporate safeguards and security criteria used by the U.S. Department of Energy (DOE) with information gleaned from independent oversight activities to assist inspectors in evaluating safeguards and security protection programs across the DOE complex. Federal and contractor employees may also wish to use the guides to assist in the planning and conduct of surveys and self-assessments. However, an inspectors guide does not represent DOE safeguards and security program implementation policy. Therefore, applicable DOE directives, as well as approved local procedures, must be used to evaluate DOE/National Nuclear Security Administration safeguards and security programs. Users of the guides must also remember that changes can occur in DOE safeguards and security directives that will outpace efforts to maintain the currency of the references listed in a guide, and care must be taken to be knowledgeable of current requirements. A loose-leaf notebook format is used so that sections can be easily removed and copied.

This page intentionally left blank

Contents

Contents (continued)

Contents (continued)

This page intentionally left blank

Acronyms

AC	Alternating Current
ASSESS	Analytical System and Software for Evaluating Safeguards and Security
ATLAS	Adversary Timeline Analysis System
BMS	Balanced Magnetic Switch
CAS	Central Alarm Station
CCTV	Closed Circuit Television
DOE	U.S. Department of Energy
ECS	Entry Control System
EOC	Emergency Operations Center
FBI	Federal Bureau of Investigation
GSA	General Services Administration
HRP	High-Power Rifle
HS-60	Office of Independent Oversight
HS-61	Office of Security Evaluations
IDS	Intrusion Detection System
ISSM	Integrated Safeguards and Security Management
LA	Limited Area
LLEA	Local Law Enforcement Agency
MAA	Material Access Area
MC&A	Material Control & Accessibility
NNSA	National Nuclear Security Administration
PA	Protected Area
PIDAS	Perimeter Detection and Assignment System
PIN	Personal Identification Number
PSS	Physical Security Systems
PTZ	Pan-tilt-zoom
SAS	Secondary Alarm System
SCIF	Sensitive Compartmented Information Facility
SNM	Special Nuclear Material
SPO	Security Police Officer
SRT	Special Response Team
SSSP	Site Safeguards and Security Plan
TID	Tamper-Indicating Device
UPS	Uninterruptible Power Source
VA	Vulnerability Assessment

This page intentionally left blank

Section 1

INTRODUCTION

Contents

Purpose

The Physical Security Systems Inspectors Guide provides the inspector with a set of detailed tools and references that can be used to plan, conduct, and close out an inspection of physical security systems (PSS). These tools serve to promote consistency, assure thoroughness, and enhance the quality of the inspection process.

The guide is intended to be useful for both novices and experienced inspectors. For the experienced inspector, information is organized to allow easy reference and to serve as a reminder when conducting inspection activities. For the novice inspector, the information can serve as a valuable training tool. With the assistance of an experienced inspector, the novice inspector should be able to use the tools and reference materials to collect and interpret data more efficiently and effectively.

Organization

This introductory section (Section 1) describes the inspection tools and outlines their use. Sections 2 through 9 provide detailed guidance for inspecting each major PSS subtopic:

- Section 2—Intrusion Detection and Assessment
- Section 3—Entry and Search Control
- Section 4—Badges, Passes, and Credentials
- Section 5—Barriers, Locks, and Keys
- Section 6—Communications
- Section 7—Testing and Maintenance
- Section 8—Support Systems
- Section 9—Systems Management

Section 10 (Interfaces) contains guidelines to help inspectors coordinate their activities both within subtopics and with other topic teams. Information is provided on the integration process, which allows topic teams to align their efforts and benefit from the knowledge and experience of other topic teams. The section provides some of the common areas of interface for the PSS team, and explains how the integration effort greatly contributes to the quality and validity of inspection results.

Section 11 (Analyzing Data and Interpreting Results) contains guidelines on how to organize and analyze data collected during inspection activities. These guidelines include possible impacts of specific information on other topics or subtopics, and some experience-based information on the interpretation of potential deficiencies.

Appendix A provides procedures for testing the various systems and items of equipment that are commonly used in DOE facilities, with guidelines for evaluating test results.

Appendix A (Intrusion Detection Systems Performance Tests) includes performance tests for testing a variety of intrusion-detection systems:

- Exterior Perimeter Sensors
- Interior Sensors
- Perimeter Closed Circuit Television (CCTV)
- Interior CCTV
- Alarm Processing and Display.

Part 1 (Access Control Systems Performance Tests) contains tests related to the effectiveness of entry control and detection equipment.

Part 2 (Communications Equipment Performance Tests) contains performance tests on radio equipment and duress alarms.

Part 3 (Support Systems Performance Tests) addresses the testing of equipment associated with power sources and tamper protection.

Part 4 (Personnel and Procedures Performance Tests) provides guidelines for designing and conducting site-specific tests of personnel and procedures. Candidate procedures, sample scenarios, and an example test plan are included.

General Considerations

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

The information in this guide does not repeat all of the detailed information in DOE orders. Rather, it is intended to complement the orders by providing practical guidance for planning, collecting, and analyzing inspection data. Inspectors should refer to this guide, as well as DOE orders and other guidance, at all stages of the inspection process.

One purpose in developing the inspectors guides was to provide a repository for the collective knowledge of Office of Security Evaluations' (HS-61) most experienced inspectors that can be enhanced and updated as inspection methods improve and inspection experience accumulates. Every attempt has been made to develop specific guidelines that offer maximum utility to both novice and experienced inspectors. In addition to guidelines for collecting information, guidelines are provided for prioritizing and selecting activities, then analyzing and interpreting results. These guidelines should be viewed as suggestions rather than requirements. The specific guidelines should be critically examined and interpreted in light of inspection-specific and site-specific factors.

Using the Topic-Specific Tools

Sections 2 through 9, organized around the PSS subtopics, provide topic-specific information intended to help the inspectors collect and analyze inspection data. Each subtopic section is further divided into the following standard format:

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

References

The references include DOE orders and manuals that apply to the subtopic, as well as other relevant documents, such as:

- Executive Orders
- Site Safeguards and Security Plans (SSSPs)
- Implementation memoranda
- Memoranda of agreement
- Procedural guides.

These references are used as the basis for evaluating the inspected program and for assigning findings. It is useful to refer to the applicable references, particularly DOE guidance, 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 to help inspectors focus on the unique features and problems associated with the subtopic. It identifies the different approaches that a facility might use to accomplish an objective and provides typical examples.

Common Deficiencies/ Potential Concerns

This section addresses common deficiencies and concerns that HS-61 has noted on previous inspections, along with a short discussion giving more detail. Information in this section is intended to help the inspector further focus inspection activities. By reviewing the list of common deficiencies and potential concerns before gathering data, inspectors can be alert for these elements at the inspected facility during interviews, tours, and other data-gathering activities. Also, where appropriate, general guidelines are provided to help the inspector identify site-specific factors that may indicate whether a particular deficiency is likely to be present.

Planning Activities

This section identifies activities normally conducted during inspection planning. If applicable, specific activities or information available to inspectors is identified for all planning phases. These planning activities include document reviews and interviews with the facility PSS managers. The detailed information in the Planning Activities section is intended to help ensure systematic data collection, and to ensure that critical elements are not overlooked. Typically, the thoroughness of the planning effort directly affects the success of the inspection.

Performance Tests

General guidelines are provided to help the inspector identify site-specific factors that may indicate which specific performance tests may be particularly important. The details of PSS performance tests are provided in Appendices A through E.

Data Collection Activities

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

Inspectors do not normally perform every activity on every inspection. The activities and performance tests to be accomplished are normally selected during the planning effort. The listed activities are those that are most often conducted, and they reflect as much HS-61 data-collection experience and expertise as possible. The activities are identified by alphabetical letter for easy reference.

Using the Tools in Each Inspection Phase

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

In the **planning phase**, inspectors:

- Use the General Information section under each subtopic to characterize the program and focus the review.
- Perform the activities identified under Planning Activities to gather the information necessary to further characterize the program and focus the review.
- Review Common Deficiencies/Potential Concerns to determine whether any of the deficiencies are apparent, and to identify site-specific features that may indicate that more emphasis should be placed on selected activities.
- Assign specific tasks to individual inspectors (or small teams of inspectors) by selecting performance tests and specific items from the Data Collection Activities section. The assignments should be made to optimize efficiency and to ensure that all high-priority activities are accomplished.
- Review the guidelines under Section 10 (Interfaces) of the guide, to be considered when assigning tasks to ensure that efforts are not duplicated.
- Prioritize and schedule data collection activities to optimize efficiency and to ensure that high-priority activities are conducted early in the process. A careful prioritization of these activities provides the opportunity to determine whether the available personnel resources and inspection time periods are sufficient to adequately evaluate the inspected topic.
- Review the applicable policy supplements to ensure that they are current with all applicable policy revisions, updates, and clarifications.

In the **conduct phase**, inspectors:

- Use the detailed information in the Data Collection Activities section to guide interviews and tours. Inspectors may choose to make notes directly on photocopies of the applicable sections.
- Review Common Deficiencies/Potential Concerns after completing each data-collection activity to determine whether any of the identified deficiencies are apparent at the facility. If so, inspectors should then determine whether subsequent activities should be reprioritized.
- Review Section 11 (Analyzing Data and Interpreting Results) after completing each data collection activity to aid in evaluation and analysis of the data, and to determine whether additional data are needed to evaluate the program. If additional activities are needed, inspectors should then determine whether subsequent activities should be reprioritized.

In the **closure phase**, inspectors:

- Determine whether the facility is complying with all applicable requirements.
- Use the Analyzing Data and Interpreting Results section to help analyze the collected data and assess the impacts of identified deficiencies. This will aid inspectors in determining the significance of findings, if any, and in writing the inspection report.

Performance Testing

Appendices A through E provide a set of commonly used performance tests that may be used directly or modified to address site-specific conditions or procedures. Since performance testing is one of the most important data-collection activities used in evaluating PSS, the information on testing is rather extensive. Performance tests applicable to each subtopic are referenced in the subtopic section.

Performance testing differs from other data-collection tools in several important ways. First, performance testing is the most labor- and time-intensive of all the data-collection activities. Second, performance testing places the greatest demands on the resources of the inspected site and requires the highest degree of coordination and planning. Third, performance testing offers the greatest potential for generating safety or security problems. In some cases, data can be

gathered using simpler data-collection tools, and extensive performance tests are not necessary. Performance tests must be carefully planned and coordinated before arriving on site in order to ensure the most efficient use of time and resources. This planning and coordination process continues up to the moment the test is administered.

The tests performed by the PSS topic team may involve equipment, personnel, procedures, or any combination of these. The ideal performance test stresses the system under examination up to the established limits of the site-specific threat. It should simulate realistic conditions and provide conclusive evidence about the effectiveness of the security system.

Equipment performance testing is designed to determine whether equipment is functional, has adequate sensitivity, and meets its design and performance objectives. It is not sufficient for a component to meet the manufacturer's standards if the component proves ineffective during testing.

Personnel performance tests are intended to determine whether procedures are effective, whether personnel know and follow procedures, and whether personnel and equipment interact effectively.

Performance tests must always be coordinated with appropriate facility personnel. Some performance tests require that personnel being tested remain unaware that a test is being conducted. Particular care must be exercised to ensure that these types of tests are well coordinated and safety factors carefully considered.

Unfortunately, realistic conditions are frequently difficult to simulate due to safety concerns, time and resource constraints, and the heightened security posture that results whenever an inspection is under way.

Determining which PSS to test is usually based on information uncovered during document reviews, interviews, and data collection activities. If this information leads the inspectors to think that a weakness may exist along a particular adversary path, or if the maintenance history of a system indicates a potential weakness, the systems identified with these weaknesses should be tested. When testing, it is important not to concentrate on one aspect or component of a system at the expense of the overall system. Also, it is usually not necessary to test all component parts of a system to determine whether the system is effective. For example, if several doors installed in the same barrier wall are equipped with an identical alarm system, testing a few doors rather than all doors is normally sufficient.

Validation

Validation is the process used to verify, with site representatives or points of contact, the accuracy of the information that HS-61 inspectors obtain during data collection. It is also particularly important that the site representatives or points of contact understand what is being validated. These procedures, discussed in the HS-61 Appraisal Guide, include on-the-spot validations, daily validations, and summary validations. On-the-spot validations verify the data at the time of collection. On-the-spot validations are particularly important during performance testing because there may be a number of people present and it is frequently difficult to reassemble these same people for the daily and summary validations. All on-the-spot validations should be validated during daily validations, which are normally conducted at the end of the day during the data-collection phase of the inspection. The summary validation is usually conducted at the end of the data-collection phase of the inspection. It is important for team members to keep track of the information covered in on-the-spot and daily validations so that it can be reiterated during the summary validation.

Characterization of the Physical Security Systems Topic

Physical security is defined as the use of intrusion detection and assessment, entry and search control, barriers and locks, communications, testing and maintenance, and support systems and interfaces to deter, detect, annunciate, assess,

delay, and communicate an unauthorized activity. An effective PSS program employs a complementary combination of these components (see Figure 1), augmented by practices and procedures specific to each location.

All DOE security assets, both tangible and intangible, are protected from theft, diversion, sabotage, espionage, and compromise that might adversely affect national security, program continuity, the environment, or the health and safety of employees or the public. There are four basic asset groups:

- Special nuclear material (SNM) and vital equipment
- Classified information
- Unclassified sensitive information
- Property and unclassified facilities.

SNM is defined and categorized according to quantity, composition, and attractiveness to adversaries. Each category of SNM requires specific protection measures during storage, transit, and use. Most of these measures are discussed in DOE Order 470.4, *Physical Protection Program*, and DOE Manual 470.4-2 Ch1, *Physical Protection Program Manual*.

Vital equipment is defined as "equipment, systems, or components whose failure or destruction would cause unacceptable interruption to a national security program or an unacceptable impact on the health and safety of the public." Site offices are responsible for identifying the vital equipment located at facilities under their purview.

The level of protection afforded classified matter depends upon the level of classification or category assigned: Top Secret, Secret, or Confidential. Classified matter can be information, documents, parts, components, or other material.

Increased levels of protection are provided to high-consequence assets. The most significant protection efforts center on nuclear weapons and Category I SNM. Also, intrusion detection and entry control systems that protect classified communications centers and computer centers are of concern to the PSS topic.

Protection standards are specific to the type of security interest, as well as to specific targets. Consequently, various levels of sophistication are applied to protect different assets. The design of a system requires an engineering perspective, incorporating site-specific requirements determined by vulnerability assessments and resulting in a level of protection consistent with DOE guidance. Levels of protection for particular safeguards and security interests are provided in a graded fashion in accordance with the potential risks.

.

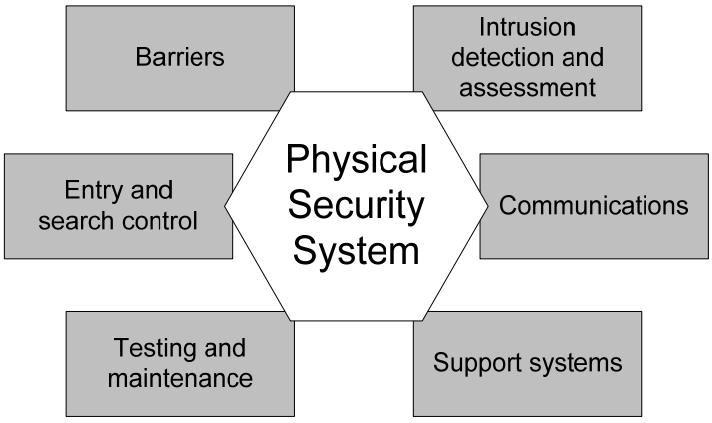

Figure 1. Physical security systems components

PSS provide protection along adversary penetration paths where force, deceit, or stealth tactics may be employed to defeat the system (see Figure 2, an example of layered protection of SNM). Force, deceit, and stealth are characterized as:

- **Force:** Adversary actions directed at overcoming elements of the physical protection system by overt aggressive activities, which the adversary expects to be detected. The adversary is therefore prepared to forcefully defend against the response.
- **Deceit:** Adversary actions directed at overcoming elements of the physical protection system by normal submission to an element with the expectation that unauthorized conditions, such as a fake badge or shielded material, will not be detected.
- **Stealth:** Adversary actions directed at overcoming elements of the physical protection system by avoiding or deactivating these elements in an attempt to prevent detection.

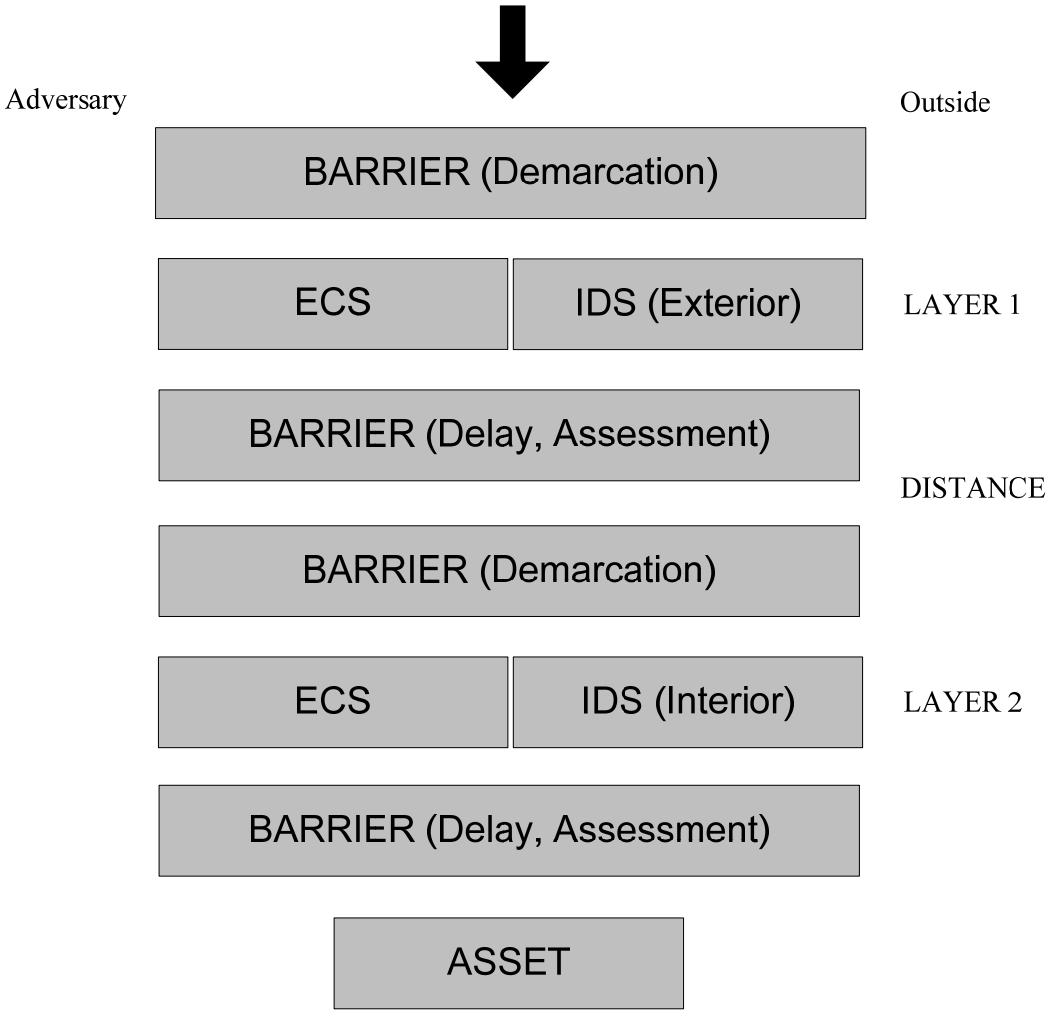

Figure 2. Schematic Adversary Path to an SNM Asset

One approach in determining whether assets are at risk is to identify the existing adversary paths leading into and out of the target area. This is perhaps best visualized by color-coding a large site map and highlighting the layers of protection afforded the various assets. This process identifies the various components of a typical PSS (that is, barrier systems, entry control systems, and interior and exterior intrusion-detection systems). A color-coded map helps the inspectors visualize the overall methodology used by the site and allows evaluation of system weaknesses. Also, this will aid in the selection of performance tests. This characterization can be aided by using a series of tools.

The completed site map, marked to indicate the various layers of protection comprising the PSS, should be compared with a verified listing of assets to ensure that all assets are afforded appropriate protection.

The inspector should then begin to identify and describe the component parts of the PSS.

Data Collection Guidelines

This section provides general data collection guidelines for briefings, document reviews, limited-scope performance tests, facility tours, and interviews. More specific guidance is included in the individual subtopic sections.

Data collection begins as soon as a site is selected and continues throughout the planning and conduct phases of the inspection. An integral part of the inspection planning process involves collection, review, and analysis of data relative to the site. Knowledge of the site-specific assets and the protective methods used provides insight into the site's mission, operations, and processes.

Briefings

During the **planning phase**, briefings are presented by the site office and contractor representative to provide the PSS inspection team with a broad understanding of the site mission. This information is supplemented by a review of documents and interviews with site representatives.

The **conduct phase** begins with an onsite meeting between the inspection team and the DOE site office point of contact to:

- Review follow-up items from planning activities.
- Work out details of the inspection schedule (for example, specific points of contact for each activity).
- Discuss any issues that may have developed subsequent to planning activities.

Document Reviews

To focus the inspection process and ensure that inspection resources are expended appropriately, during the planning phase the PSS inspection team compiles a listing of site assets described in the SSSP, grouping them into appropriate categories. As the inspection progresses, assets should be confirmed with topic teams dealing with material control and accountability (MC&A) and classified matter protection and control. Inspectors can draw certain conclusions and inferences based on the consequence of loss of these assets and, in so doing can further focus inspection efforts.

Document reviews are an important part of the evaluation of PSS effectiveness. Document reviews begin during the planning phase with the review of the SSSP, survey and inspection reports, and other documents. These documents reveal the physical protection philosophy and approach taken to implement the safeguards and security requirements mandated by DOE orders.

Information obtained from document reviews establishes the inspection baseline for:

- Verifying information received from briefings, tours, and interviews
- Determining the site-specific threat
- Identifying site/facility assets
- Implementing PSS corrective actions
- Establishing the response posture and protection strategy
- Detailing standard operating procedures.

Basic documents to be reviewed include:

- Organization charts
- SSSP
- Site security plans
- Security plans for temporary material access areas
- Decontamination and decommissioning plans
- Listing of waivers and exceptions
- Past survey reports and HS-61 inspection reports
- Facility asset list
- Maps/drawings showing security areas, buildings, security posts, vital equipment areas, and SNM storage areas.

Vulnerability assessments are reviewed to clarify the facility's evaluation of all potential pathways leading from outside the security area into target areas and their characterization of those pathways in terms of the delay and detection accumulated by the adversary en route to the target. The overall delay for each pathway is calculated and compared to protective force response times to determine the protective force's probability of interrupting the adversaries before they can access the target. By reviewing these assessments, inspectors can better identify which systems the facility considers to be most essential to asset protection. The following are some considerations for review of vulnerability assessments:

- Priority of site-specific threats
- Identification of "worst-case" (lowest probability of detection and/or shortest amount of delay) pathways into a facility
- Identification of systems (detection, assessment, delay) that are most critical in providing protection for DOE assets
- Determination of the assumed detection probabilities for each system
- Determination of the credit taken by the facility for assessment (immediate assessment vs. delayed assessment)
- Identification of the last possible point at which an adversary must be detected to allow adequate response/adversary interruption by the facility protective force
- Graded protection and defense-in-depth
- Comparison of vulnerabilities against findings and resolution of past HS-61 inspections and operations office surveys.

Records and procedures are also reviewed. **Records** include operations logs; test records; PSS maintenance, testing, and repair records; trend analysis information; occurrence reports; force-on-force after-action reports; and other records identified during the course of the inspection. **Procedures** include protective force post orders, maintenance procedures, MC&A procedures, and facility operating procedures. The inspection team reviews these items to determine whether:

- Required PSS records are kept.
- System tests are performed and documented as required.
- System maintenance is performed as required.
- PSS procedures are comprehensive and effective.
- Anomaly resolution is timely and effective.
- The overall protection afforded DOE assets has been considered.

Limited-Scope Performance Tests

The selection of limited-scope performance tests is based largely on the analysis performed during the planning phase of the inspection and on information derived from facility tours and interviews with operations office and contractor representatives. Typical test measures verify whether:

- PSSs are accurately characterized in vulnerability assessments and security plans.
- Response times are consistent with those identified in security plans.

- Equipment is tested and calibrated according to traceable specifications.
- Procedures are complete and describe the actual methods of operation.
- Personnel adhere to procedures in performing their activities.
- Personnel are knowledgeable of their duties and responsibilities.
- Equipment is in good repair.

Facility Tours

The inspection team generally tours the facility as early as possible. More detailed tours of key areas are scheduled as needed.

Although inspectors are likely to examine facility drawings and analyze potential adversary paths, facility tours are essential to gain the level of understanding required by the inspection team. The purposes of these tours are to:

- Become familiar with the site and facility layout.
- Observe the actual layout of the overall PSS and individual elements of the system.
- Verify that the documentation previously examined accurately reflects the current conditions and configurations at the site.
- Ensure that the systems described in documentation are implemented and operational.
- Identify anomalies or deficiencies that require further investigation.
- Select specific areas or components as candidates for performance testing.

Tours provide the opportunity to place the PSS documentation and briefings into perspective, because the inspectors can witness the operating environment and note the intangibles that affect system design and operation. To obtain maximum benefit from the tour, the topic team should:

- Minimize unnecessary inconvenience to tour guides and facility operations and personnel.
- Try to observe procedures during normal operations (e.g., observe vehicle search procedures while testing equipment at a post).
- Have the people who normally work in the area demonstrate the procedures rather than having a supervisor demonstrate how they think the procedure is performed.
- Take notes on areas that may require further review (e.g., vault thickness, protection against penetrations into vaults).
- Ensure that tour logistics are carefully arranged.

During the initial tours, inspectors should verify:

- Locations and boundaries of material access areas (MAAs) and Protected Areas (PAs)
- Category designation of MAAs and PAs
- Locations of MAA and PA access portals
- Locations of normal transfer points and paths between MAAs
- Locations and types of security equipment installed
- Location of the alarm stations.

Additionally, inspectors should confirm:

- General quality and condition of the physical barriers
- Entry control procedures and methods employed at access portals (contraband detection equipment and procedures, badge checks, badge exchanges, card readers, biometrics)
- Type of storage areas (vaults, vault-type rooms, alarmed rooms, safes, locked filing cabinets, locked rooms)
- Location of emergency exits
- Types and approximate quantities of SNM in use or being processed.

Interviews

Interviews clarify impressions and allow insight into facility operating procedures. Interviews with personnel at all organizational levels are

recommended. Frequently, discussions with personnel involved in "hands-on" operations reveal whether management's policies and directives are effectively communicated and implemented, and whether the systems actually function as described in the documentation.

Personnel to consider interviewing include DOE and contractor security managers, facility managers and staff, vault/vault-type room custodians, security police officers (SPOs), security technicians/specialists, PSS maintenance personnel, systems engineers and programmers, and central alarm station (CAS) and secondary alarm station (SAS) operators. Other personnel may be interviewed as needed. Interviews are not necessarily formal, and often take the form of discussions during facility tours or performance testing.

Integrated Safeguards and Security Management

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

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

The seven guiding principles of ISSM are:

- Individual responsibility and participation
- Line management responsibility for safe-guards and security
- Clear roles and responsibilities
- Competence commensurate with responsibilities
- Balanced priorities
- Identification of safeguards and security standards and requirements
- Tailoring of protection strategies to work being performed.

The five core functions of ISSM are:

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

For the purposes of this inspectors guide, HS-61 has established four general categories that encompass the concepts embodied in the guiding principles and core functions of ISSM:

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

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

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

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

It is important to note that the categories above are only used to organize information in a way that will help inspectors gather data about management performance in a structured and consistent manner. HS-61 has identified general categories of information that would be expected in an integrated ISSM program.

Section 2

INTRUSION DETECTION AND ASSESSMENT

Contents

General Information

DOE Order 470.4 stipulates that intrusion detection systems and/or visual observation by protective force personnel be utilized to detect unauthorized entry and/or presence in security areas that require protection. Typically, the procedures to meet these requirements are documented in approved site security plans.

Specific elements covered in this section are:

- Alarm annunciation, monitoring, and control systems
- Exterior and interior sensors
- Power supply
- Assessment and response
- Lighting.

The testing and maintenance program is addressed in Section 7.

To ensure compliance with DOE requirements, intrusion alarms and detection devices must perform within certain detection specifications. Balanced magnetic switches (BMSs), volumetric detectors, and alarm connections to local law enforcement agencies (LLEAs) are also required to meet the applicable requirements.

In addition to patrols and visual surveillance provided by the protective force, alarm and detection devices are fundamental PSS components. To be effective, alarms must be clearly audible. Alarm displays must be clearly visible and must identify the location and type of alarm, and the operator interface must allow for alarm recognition by the operator. Alarm lines and other detection devices require continuous supervision to preclude any covert attempt to bypass the alarm system, and to ensure an appropriate and timely response. To achieve an acceptable degree of assurance that the PSS works properly, it is incumbent on facility management to provide for adequate equipment, an effective testing and maintenance program, and a sufficient number of trained personnel to operate the alarm and assessment equipment.

Intrusion detection systems consist of both an alarm and an assessment system, and are usually layered for both interior and exterior applications. Exterior systems are designed to provide the earliest possible detection of an unauthorized intrusion, as far away from the security interests as possible. The interior intrusion detection system may be even further divided into layers according to the configuration of security areas and the required levels of protection.

At SNM facilities, the outermost layer of the exterior systems is usually the perimeter intrusion detection and assessment system (PIDAS). It typically consists of multiple and complementary electronic sensors, such as:

- Microwave
- Infrared
- Electric field sensors
- Fence disturbance detectors
- Seismic sensors.

Exterior systems must be capable of withstanding the environmental conditions in which they are deployed. Properly designed systems generally use two or more types of complementary sensors, depending on the operating environment and design parameters. Typically, the PIDAS also includes fixed-position CCTV coverage for timely assessment of alarms generated in the PIDAS bed. PIDAS alarms normally annunciate

in the CAS and SAS, where the alarm console operators can acknowledge the alarm, assess its cause, and direct a response as necessary.

Although design characteristics differ depending on the systems in use, the intent of the exterior sensors is to provide assurance that a person crossing the perimeter will be detected whether walking, running, jumping, crawling, rolling, or climbing at any point in the detection zone, under specified weight and speed limits. Sensor systems are required to have adequate coverage in all weather and light conditions, overlap to eliminate dead areas, and be wide enough to deter bridging. Also, it is essential that detection zones contain no dips, high ground, or obstructions that could provide a pathway for an individual to avoid detection.

CCTV systems used in conjunction with alarm and detection systems are most effective when they have the capability to automatically call the operator's attention to an alarm-associated camera display, and the camera's picture quality, field of view, and image size is such that the operator can easily recognize human presence. Tamper protection and loss-of-video alarm annunciation are essential characteristics of the system if the cameras serve as the primary means of alarm assessment. Video recorders, when used with the CCTV system and when initiated by alarm signals, are most useful when they operate automatically and are rapid enough to accurately record an intrusion. Video capture systems, if used, provide pre-alarm, alarm, and post-alarm video images of the alarmed zone.

Interior intrusion detection systems are normally designed to protect specific security areas, such as:

- PAs
- Limited Areas (LAs)
- MAAs
- Vaults
- Vault-type rooms.

These systems employ various technologies that detect:

- Physical movement
- Heat
- Movement related to time
- Cable tension
- Vibration
- Pressure
- Capacitance.

Assessment measures range from the deployment of protective forces to the use of multiple auto-focus camera systems equipped with pan/tilt and auto-zoom features.

The field device network is the array of sensors and data transmission equipment that communicates to the primary and secondary host computers. As required by DOE Manual 470.4-2 Ch1, communication between the host computers and field devices of the system should be redundant and independently routed. Field devices consist of local processors, input/output panels, and multiplexing units, depending on manufacturer's system configuration. The field device network should provide randomly polled digital supervision that detects and annunciates communications interruptions or compromised communications between any field device and the host computers.

Since alarms and detection systems require a power source for operation, an auxiliary power source consisting of an uninterruptible power supply (UPS) and generator must be available, and switchover

must be immediate and automatic if the primary power source fails. In most cases, immediate and automatic switchover does not occur if a generator is the only source of backup power; the UPS is needed to handle the immediate switchover, and the generator assumes the role once it reaches full power.

To ensure effective operation of alarms and detection devices, managers must provide for a regular test and maintenance program. Such a program includes the periodic testing of equipment and circuits, and the thorough inspection of equipment and circuits by qualified service personnel. Also, records of these tests are required to include the date of the test, name of the person conducting the test, and the results. Details on inspecting the testing and maintenance program are discussed in Section 7.

Frequently, intrusion detection and entry control systems are separate systems, interfaced to provide information to the system operator. In many systems, normal access control and other work-related activities are processed without operator interaction. Records of such transactions are generally recorded for historical purposes.

The main purpose of an intrusion detection and assessment system is to alert the protective force to an intrusion, aid in alarm assessment, allow the protective force to track intruder progress toward a target, and aid in assessing intruder activity and characteristics (for example, the number of intruders and whether they are armed). Protection systems normally include a suitable means of assessing alarms and provide for an appropriate response. The protective force is usually responsible for monitoring and response. Also, protective force personnel are normally responsible for preparing alarm reports according to DOE or site office specifications and distributing copies as appropriate. Response procedures are usually found in the applicable site security plans.

Lighting is of primary importance in the operation of an effective alarm and detection system. Effective lighting provides a deterrent to adversary intrusion, assists the protective force in locating and assessing alarm initiations, and provides for effective use of CCTV as a surveillance and assessment tool. Lights are required to have a minimum specified luminescence at ground level for specific areas, a regular power source, and an emergency backup lighting capability. Lights should not cause glare or bright spots in CCTV camera images, especially if CCTV is the primary means of assessment.

Common Deficiencies/ Potential Concerns

False and Nuisance Alarms

One of the most common problems with intrusion detection systems is that they may generate an inordinate number of false alarms. Many systems are susceptible to false and nuisance alarms induced by high winds, animals, heavy snow, lightning, vehicular vibration, and wind-blown dust and debris. These systems include:

- Microwave sensors
- Infrared sensors
- Electric field sensors
- Seismic sensors
- Buried sensors.

Improper installation (improper tension or insulation coupling) can also cause unacceptable false alarm rates in electric field sensors. Seismic sensors may produce nuisance alarms if installed too near fences, power poles, guy wires, or roads where vehicles generate heavy ground vibration. Video motion detectors are susceptible to nuisance alarms induced by reflected light, cloud motion, vehicle headlights, and camera vibration due to wind. A high rate of false and/or nuisance alarms may lead the protective force to ignore or improperly assess an intrusion.

Improper Installation, Calibration, or Alignment

Improper installation, calibration, or alignment of sensors may significantly reduce sensitivity, contribute to false alarms, and allow for unauthorized intrusion. For example, insufficient offset may allow intruders to crawl under or jump over a bistatic microwave beam at the crossover point (the point where adjacent zones overlap). Also, video motion detectors require extensive maintenance and calibration for proper operation, and audio detectors must be calibrated carefully to avoid nuisance alarms caused by common background noises. Effective operation of a CCTV system is frequently diminished when the system is not correctly installed or aligned. If the camera is not properly placed or aligned, there may be "holes" in the coverage that permit an intruder to cross the isolation zone unobserved. Additionally, if the field of view of the camera is too long for the camera lens, an intruder at the extreme end of the field of view may not be adequately observed, or the camera's automatic call-up feature may not operate quickly enough to capture adversary activity in the alarm zone.

Tamper Protection for Power Sources

The primary and backup power sources for intrusion-detection systems are susceptible to tampering. Power switches, inverters, and generators should be protected but are often overlooked during protection planning and installation. Exterior fuel tanks and filler points are especially vulnerable. For example, an inoperable filler point or contaminated fuel tank may nullify all backup power sources. If the primary power source fails, the protection systems become inoperable and DOE assets become vulnerable.

Inadequate Testing and Maintenance Program

Most PSS failures are the direct cause of an inadequate testing and maintenance program. Like an automobile, the lack of maintenance and operation (testing) usually results in equipment failure. For this reason, the testing and maintenance program is one of the most important features of any protection system. An effective program normally includes provisions that require facility technicians, augmented by service representatives, to perform all tests, maintenance, calibrations, and repairs necessary to keep the detection and assessment systems operational. An inadequate program that results in frequent system failure, cursory testing procedures, or an inordinate number of items of equipment awaiting repair indicates a lack of management attention. Details of inspecting the testing and maintenance program are discussed in Section 7.

Failure To Properly Assess and Respond

A number of factors may affect assessment and response. For example, a high rate of nuisance and false alarms may degrade operator response to genuine alarm conditions. Failure of a system to adequately identify alarm type and specific location may also degrade response. The latter is usually most evident when systems do not clearly differentiate between tamper-indication, line-supervision, and intrusion alarms, or when multiple sensors are monitored by a single alarm point. For computer-based systems, problems may arise because of erroneous software modifications and system configurations that cause program errors. It is important that the signal received from the detection device provide identifiable evidence of the actual occurrence so operators can properly assess the situation and respond accordingly.

Planning Activities

During inspection planning activities, inspectors review available documents and interview points of contact. Elements to cover include:

- Review of the site mission (obtained from a review of the documents and from interviews with site office personnel and site representatives)
- Review of:
  - Organization charts

  - SSSP
  - Site security plans and procedures
  - Security plans for temporary MAAs
  - Decontamination and decommissioning plans
  - Deviations, both approved and requested
  - Past site office survey reports and HS-61 inspection reports
  - Self-assessment reports
  - Site/facility asset list
  - Site maps/drawings indicating
    - Security areas (LAs, PAs, MAAs, vaults, vault-type rooms)
    - Critical facilities
    - Controlled areas
    - Building definitions
    - Locations of security posts
    - Classified matter areas
    - Vital equipment areas
    - SNM storage areas
    - Transfer routes
    - Lighting diagrams
  - Organization charts
  - Alarm procedures
- Review of lists showing:
  - Types of sensors employed
  - Local alarm reporting devices
  - Data transmission systems
  - Console equipment descriptions
- Review of the assessment methodology employed (CCTV, video, and/or patrol response)
- Review of the vulnerability analysis (VA), including consideration of:
  - Application of the design basis threat
  - Whether the threats identified by the site address local characteristics, including the insider threat
  - Priority of site-specific threats
  - Target definition and locations
  - Graded and defense-in-depth PSSs
  - Pathways providing lowest detection and/or shortest delay
  - Presentation of the VA results in the SSSP
  - Listing of the protective elements identified in the VA for each security interest (review the VA results in the SSSP to determine whether the key VA results are in the SSSP and whether any assumptions in the VA should be validated during the inspection)
  - Comparison of vulnerabilities against findings and resolution of past HS-61 inspections and site office surveys.

- Review of protective methods employed at the location to be inspected
- Determination of the type and location of potential targets (to further focus inspection efforts, compile a list of site assets, group them into appropriate categories, and determine potential impacts related to their loss).

Performance Tests

The following performance tests are recommended for alarms and intrusion detection devices:

- Exterior perimeter sensors (Appendix A, Part 1)
- Interior sensors (Appendix A, Part 2)
- Perimeter CCTV (Appendix A, Part 3)
- Interior CCTV (Appendix A, Part 4)
- Alarm annunciation, monitoring, and control system (Appendix A, Part 5)
- Emergency auxiliary power supplies (Appendix A, Part 1)
- Tamper protection and line supervision (Appendix A, Part 2).

Data-Collection Activities

Alarm Annunciation, Monitoring, and Control System

A. Inspectors should review alarm records to determine false/nuisance alarm rates. This may involve reviewing alarm logs for a specified period (for example, two weeks) and determining the number of alarms during that period. Alternatively, the inspector could review the facility's plots of alarm rates if such plots are maintained. Any abnormally high alarm rates should be identified and the causes discussed with the facility representatives (including measures taken to eliminate false/nuisance alarm sources). The accuracy of alarm records can be investigated by comparing alarm plots against alarm logs or alarm plots/logs against computer records for a specified period. When reviewing alarm records, the inspector should clearly understand the facility's definitions of false alarms and nuisance alarms and how they are assessed. The inspector should also consider interviewing alarm system operators to determine their understanding of false/nuisance alarm rates and make sure that they are consistent with facility definitions. Operators' ability to consistently make judgments as to whether alarms are considered false or nuisance will greatly affect false and nuisance alarm rate calculations.

Exterior and Interior Sensors

B. During inspection of the PIDAS, inspectors should examine the various types of sensors to determine whether they are complementary (that is, whether they consist of different sensor types that cannot be defeated by the same means, not just multiple layers of the same sensor). Inspectors should also confirm the existence of an effective testing and maintenance program for the PIDAS. Inspectors should check the condition of the PIDAS bed for obstructions, mounds and valleys, and other terrain features that an adversary could use to avoid the detectors. Crossover and interface points should also be checked to determine whether there are voids or blind spots in sensor coverage. Particular attention should be given to the identification of PIDAS sectors susceptible to bridging as a result of their close proximity to tall buildings, fences, telephone poles, or light and camera structures. Similar attention needs to be paid to any unsecured/unprotected accessway that tunnels beneath PIDAS sectors.

C. Inspectors should tour the CAS and SAS, visually inspect equipment, interview operators, and verify information gathered during document reviews. Items to be checked include operability of equipment, operators' familiarity with equipment, and measures to protect equipment from tampering. It is important that alarms reported from the field are properly recognized and acknowledged, and that appropriate responses are made. Interviews with station operators will reveal their understanding of their responsibilities.

D. At each exterior security area where a PIDAS is used, inspectors should determine:

- The number and configuration of sensors
- Sensor alarm logic (e.g., 1 of 2, 2 of 3)
- Test frequency and methods
- Preventive maintenance frequency and methods
- Tamper-indicating provisions
- Provisions for repairing component failures.

E. Inspectors should review documents and interview security staff to determine the method used to detect intrusion at each security area. If more than one method of detection is used at a security area (for example, an electronic alarm system and direct observation from guard towers), inspectors should determine:

- How the systems complement each other
- Which is considered the primary means of detection
- Whether the combination (primary and backup) is effective.

F. At selected interior security areas (for example, MAA buildings) and storage areas, inspectors should determine:

- The types of sensors used to protect building perimeters (including doors, windows, and other penetrations)
- Testing and preventive maintenance frequency and methods
- Tamper-indicating provisions
- Conditions for placing a zone portal in access
- Provisions for repairing component failures.

G. Inspectors should determine whether the facility has more than one central electronic alarm system and, if so, the area that each system covers. A facility with two well-defined geographical areas may have a separate alarm system for each. For each separate electronic alarm system, inspectors should determine:

- Whether there are SASs
- Central processing unit switching capability
- Tamper alarm features
- Adequate primary and backup power supply.

This information can be gathered by document reviews or interviews with security staff. However, inspectors may need to interview the responsible system engineers to accurately determine the technical aspects of the system. Conducting such interviews in the CAS/SAS may allow a better understanding of the system and its interfaces.

H. Inspectors should verify that the SSSP identifies means for providing intrusion-detection capability when primary systems are out of service. Implementation of the measures can also be verified, generally by reviewing the CAS or protective force supervisor logs or maintenance records to determine when equipment was out of service and to verify that compensatory measures were implemented during those periods.

Power Supplies

I. Auxiliary power supplies are required for all security systems. Inspectors should validate the operability of these supplies. Power supplies are normally tested concurrently with the PIDAS lighting test (see Appendix A, Part 1, Emergency Generator Test).

Assessment and Response

J. Inspectors should verify complete coverage of the security area perimeter. This activity is particularly applicable at areas with alarmed fence lines that delineate a security area perimeter and that rely on protective force visual observation posts to assess alarms. An effective method of verifying complete coverage is to have one person walk the perimeter along the fence line while inspectors are stationed in the CAS observation posts assigned responsibility for that portion of the perimeter. Each portion of the perimeter can be checked sequentially. In this manner, the inspectors can verify that there are no blind spots along the perimeter that might permit an adversary to breach the boundary without being detected and assessed. This activity can be facilitated with two or more inspectors who "hopscotch" from post to post. The overlap points between zones can also be checked more readily with two or more inspectors in adjacent observation posts.

K. Inspectors should observe CCTV display monitors during a range of conditions, such as at different times of the day and night and under various weather conditions if possible, and by using various testing techniques covered in the PIDAS testing. Alternatively, the inspector may request facilities that have a video recording capability to provide tapes recorded during different weather conditions, if available. Inspectors should review the monitors or recordings to determine whether the CCTV systems provide appropriate data under varying light and weather conditions. Inspectors should also verify that camera and recorded video call-ups are rapid enough to capture adversary activity. This is usually done as part of the PIDAS inspection, once during the day and once at night, following the emergency auxiliary test for PIDAS lighting.

L. Inspectors should interview security staff and review documents to determine the areas where direct visual observation is the primary means of detecting intrusion or assessing alarms. Inspectors should determine the type of post (for example, tower, portal, continuous patrol), assessment aids available to protective force personnel (for example, search lights, night vision devices, binoculars), and the methods used by the facility to test effectiveness and maintain the SPO's level of vigilance. Inspectors should determine:

- The operability of equipment
- Power supplies
- Measures to protect equipment from tampering
- Fields of view
- Adequacy of lighting
- Blind spots or obstructions
- Overlap with adjacent zones.

Lighting

M. Inspectors should interview security staff, review documents, and conduct performance tests to determine:

- Effectiveness of lighting levels at:

  - Portals
  - Security area perimeters
  - Exterior and interior areas that rely on CCTV
- Normal and emergency auxiliary supplies for lighting systems
- Procedures used if lighting fails
- Methods for monitoring lighting systems
- Reporting and replacing burned-out lights and failed equipment.

N. Inspectors should observe the lighting during nighttime tours of the facility while lights are on primary power and then on auxiliary power. The lighting levels should be observed from a variety of locations, including key visual assessment posts (for example, towers). The CCTV monitors in the CAS/SAS and other selected posts (if any) should also be observed to determine the adequacy of lighting. One method of determining the adequacy of lighting is to have one or more persons (dressed in various contrastable color clothing) stand in various areas, as directed by the inspectors who are stationed in visual observation posts or monitoring CCTV cameras in the CAS/SAS. The inspectors should direct the individual to stand in locations where light levels are low or contrast ratios are high. The inspectors should determine whether there are blind spots and whether the lighting is adequate to distinguish between humans and animals at any location in the observation zone. If feasible, the lighting should be observed during a variety of conditions (for example, clear weather and rain or fog). Items to check include:

- Lighting levels
- Light/dark contrast
- Glare
- Shadows
- Inoperative bulbs.

Light meters may be used to check lighting levels and contrast ratios in various areas.

O. Inspectors should determine the vulnerability of lighting systems to sabotage by reviewing lighting circuit and power supply diagrams and touring areas critical to the lighting systems (for example, switchyards, transformers, circuit breakers, power lines, engine generators, uninterruptible power supply). Inspectors should determine:

- Whether all lights at a security area perimeter are on a single circuit (as opposed to having every other light on a second circuit)
- Whether the electric power supplies are vulnerable to single-point failures (for example, a circuit breaker)
- Whether there are provisions for controlling access to areas containing components critical to the lighting system
- Self-testing features
- Methods for modifying system hardware and software
- Whether there are provisions for maintaining assessment capability if the lighting fails.

Section 3

ENTRY AND SEARCH CONTROL

Contents

General Information

Entry and search controls are established to prevent unauthorized access to security areas, removal of SNM, sabotage of vital equipment, and introduction of contraband. These controls may include access identification systems, search procedures, detectors, and barriers.

Security areas are established when the nature or importance of classified matter or security interests is such that access to them cannot be effectively controlled by other internal measures. Access to security areas is limited to persons who possess an appropriate clearance and need-to-know. Access and search controls normally include:

- A personnel identification system
- Positive verification of identity
- A visitor log
- Inspection or search procedures
- Signs indicating that trespassing is prohibited.

A security badge or pass system may be used to ensure that only authorized personnel enter, occupy, or leave a security area, and to indicate the limitations placed on access to classified matter. Badges, passes, and credentials are covered in detail in Section 4 of this guide.

Search systems range from physical and visual search procedures to the use of specialized detection equipment such as SNM and explosive detectors. Since these systems are heavily dependent on personnel actions, inspectors must evaluate the training and capabilities of the individuals operating such equipment. Also, attention must be given to ensuring that search equipment is properly installed. The best-trained SPOs, using state-of-the-art equipment, cannot achieve the desired results if the equipment is not properly installed or maintained.

Subjects covered in this section are:

- CCTV identification systems
- Card-reader systems
- Biometric identifiers
- SNM detectors
- Explosive detectors
- Metal detectors
- X-ray equipment.

A CCTV identification system may be used to provide positive identification of personnel entering security areas as an alternative to protection personnel stationed at the access control point to control access to a security area. CCTV systems allow remotely stationed protective personnel to view a person's face and identification badge. Equally effective access control measures must be in place whenever the CCTV identification system is inoperable.

Card readers and coded credentials may be used to supplement or replace badge checks as a means of access control. These devices are often used to control access to inner security areas and at facility entry and exit portals. Door locks opened by card readers must be designed to relock after

the door has closed to prevent a person from immediately opening the door while it is still in the unlock mode. Card readers at critical locations are usually provided with anti-passback protection. The coded credential technology includes a broad range of intricate applications, including:

- Bar codes
- Weigand effect
- Magnetic stripe
- Proximity
- Smart cards.

These types of cards normally contain all information required for personal identification.

Biometric identifiers verify personal identity on the basis of some unique physical characteristic, such as eye-retinal pattern, hand geometry, voice, or fingerprints. Retinal scan and hand geometry devices are the most commonly used biometric identifiers at DOE facilities. These devices may be used along with other controls, such as card readers or badge checks. Biometric identifiers are sophisticated devices that require proper installation, regular maintenance, and periodic servicing by authorized manufacturer's representatives.

SNM detectors usually include signal processing and annunciation equipment and are configured as portal, handheld, or vehicle devices. These detectors must be properly calibrated and sufficiently sensitive to meet site-specific protection objectives as defined in the SSSP.

Explosives detectors may be used for searching personnel to ensure that explosive components are not introduced into the facility. It is important that protective or other personnel are trained for clearing alarms and for taking appropriate actions if a violation is identified. Backup detectors (swipe) must be available at each location where explosives detector portals are in use to resolve portal alarms and for use in the event of portal failure.

Metal detectors may be used for searching personnel to ensure that explosive components, weapons, or other prohibited metal articles are not introduced without authorization. It is important that protective or other personnel are trained for clearing alarms and for taking appropriate actions if a violation is identified. Backup detectors (handheld) must be available at each location where metal detector portals are in use to resolve portal alarms and for use in the event of portal failure.

X-ray machines are also an acceptable means of searching many types of hand-carried items for concealed contraband or other unauthorized material. These machines must be capable of providing a clear picture of objects contained in packages or briefcases. Personnel operating the x-ray machines must be trained to recognize contraband, to take appropriate action when suspect contraband is detected, and to operate the machine and recognize malfunctions.

Common Deficiencies/ Potential Concerns

Inadequate Monitoring

Inadequate monitoring results when SPOs are inattentive or cannot adequately view the search equipment (e.g., because of poor positioning or post design, or distraction by other duties). These conditions can allow the search equipment to be defeated, leading to unauthorized introduction or removal of material.

CCTV Systems

There are a number of concerns when using CCTV identification systems. Since they may be vulnerable to disguise and false credentials, CCTV systems are usually not suitable for high-security areas, such as an MAA. Also, inattention by protective force personnel is a common problem.

Card-Reader Systems

A card-reader system does not verify the identity of a person; it identifies the coded badge or credential. For this reason, these systems are not acceptable as stand-alone systems for high-security areas and require additional controls, such as:

- Badge checks
- Personal identification number (PIN)
- CCTV identification
- Biometric identification.

Coded credentials are also vulnerable to counterfeiting and decoding. If a lost or stolen badge is not voided in a timely manner, that badge can more easily be used for unauthorized purposes increases. Additionally, if the authorized access lists are not updated frequently, persons who no longer have authorization could gain access to a restricted area.

Biometric Identifiers

Facilities have had problems with biometric identifiers frequently rejecting authorized users. At these sites, alternative verification procedures that provide an acceptable level of identification must be available to avoid adverse impacts on the overall protection program. Conversely, some devices are too tolerant; for example, if the band of acceptance is too large, almost any hand, eye, or fingerprint will be accepted.

SNM Detectors

SNM detectors are sensitive to the rate of speed at which individuals and vehicles pass through the detectors. For example, if an individual runs through the portal detector or items are thrown through, the detection probability can be substantially reduced. In any case, the SNM detector should be under visual surveillance when in use to prevent attempts to "pass around," compromise the detector, or otherwise defeat the device.

Explosives Detectors

Explosives detectors are sensitive to nitrogen-based explosives, so they will also detect some non-explosive materials that contain nitrates, such as fertilizers. The speed at which the person moves through the detector is also a concern. For example, if the individual passes through too quickly, the probability of detection is reduced. For these reasons, the detector should be under visual surveillance during operation to reduce the risk of compromise and circumvention.

Metal Detectors

Metal that is passed through the detector very slowly or rapidly may not be detected. For this reason, procedures are usually in place to monitor personnel and items passing through metal detectors. Individuals assigned to monitor this activity must be properly trained and sufficiently diligent to recognize attempts to defeat metal detection devices. Inspectors should pay particular attention to testing of metal detectors at the floor level (in older detectors) because of the metal used in constructing the floor.

X-Ray Equipment

X-ray equipment should be examined closely to ensure that it is functioning properly to detect metal at the required penetration depths, with sufficient resolution capability to effectively discern prohibited articles. The use of the standard step wedge with the requirement to image a 26-gauge wire at step five has not been uniformly implemented at all sites.

Planning Activities

During inspection planning activities, inspectors interview points of contact and review available documents. Elements to cover include:

- General policies and criteria for access authorization at each security area. Potential criteria include:
  - Personnel recognition
  - Possession of a badge
  - Possession of a badge and inclusion in a badge exchange system
  - Enrollment in a coded credential system (e.g., card reader) and possession of a coded credential
  - Enrollment in a biometric identification system
  - Possession of a key
  - Knowledge of a combination to a lock or keypad
  - Knowledge of a code word

- The methods (e.g., badge check, card reader, badge exchange) of verifying the identity of personnel entering each security area, including:
  - Property Protection Area
  - LA
  - Exclusion area
  - Sensitive compartmented information facility (SCIF)
  - Secure communications center
  - Vital Area
  - PA
  - MAA
  - Vault/vault-type room
  - Classified repository
- Whether more than one method of access control is used at a security area (e.g., badge check and card reader), how the systems complement each other, and which is considered the primary means
- General methods for determining a visitor's authorization and controlling access
- Policies and procedures for vehicle control, including volume of traffic and the authorization process for private vehicles, government-owned vehicles, vendor vehicles, emergency vehicles, and SPO vehicles
- General methods and procedures for conducting entry searches at each security area, especially each PA. (It should be noted that, absent dramatic improvement in technology, the only way that a vehicle can be effectively searched for weapons and/or explosives is by dismantlement of major components. Alternatively, vehicles may be escorted inside the protected area by the protective force.)
- General methods and procedures for conducting exit searches at each security area, especially each MAA
- General information about each security area, including:
  - Normal operational hours (e.g., day shift Monday through Friday, or 24 hours a day and seven days a week)
  - Variations in normal operational hours
  - Approximate number of people assigned to the area
  - Approximate number of people with permanent access authorization to the area (including SPOs, fire squad, and other support groups)
  - Number of personnel portals and approximate throughput
  - Number of vehicle portals and approximate throughput.

Performance Tests

- Personnel Access Control Equipment (Appendix A, Part 1)
- SNM Detectors (Appendix A, Part 2)
- Metal Detectors (Appendix A, Part 3)
- X-Ray Machines (Appendix A, Part 4)
- Emergency Auxiliary Supplies (Appendix A, Part 1)
- Tamper Protection (Appendix A, Part 2).

Data Collection Activities

Policies and Procedures

A. Inspectors should determine whether policies are in place that provide procedures on access control. These policies may cover personnel recognition, badge requirements, coded credentials and card readers, biometric identification systems, key control systems, combination lock or keypad requirements, or other access control measures.

B. Inspectors should determine whether there are policies and procedures for vehicle control, including private vehicles, government-owned vehicles, vendor vehicles, emergency vehicles, and SPO vehicles. Inspectors should determine

which vehicles are authorized to enter security areas, how authorization is indicated (for example, sticker pass, government license plate), and how such indicators are requested, issued, and controlled. Inspectors should determine whether procedures are in place to handle special or blanket authorizations for various types of vehicles, such as:

- Protective force
- Fire
- Maintenance
- Ambulance
- Local law enforcement vehicles.

Inspectors should review:

- Protective force post orders
- Standard operating procedures
- Health physics policies
- CAS procedures
- Other relevant documents to determine whether they are complete, current, and consistent with site-specific policies.

C. Inspectors should revire enrollment and de-enrollment procedures by asking the facility to print the enrollment list for one or more areas and then verifying the names on the list by comparing the computer listing to other lists or by interviewing supervisors. Inspectors should determine whether all persons on the list are authorized, whether persons who recently transferred or terminated were removed in a timely manner, and whether the lists are consistent with the information available to SPOs at portals.

D. Inspectors should:

- Review search system policies, procedures, and calibration specifications for both personnel and vehicle searches.
- Interview personnel who:
  - Calibrate, test, and maintain search equipment
  - Monitor and respond to alarms (SPOs).
- Determine the length of time SPOs are required to operate detection equipment.
- Tour areas where searches are conducted.
- Observe search procedures to determine whether:
  - Searches are effective
  - Detection equipment can be bypassed
  - Detectors and x-ray machines are properly calibrated.
- Determine whether backup search equipment is available (for example, handheld metal and SNM detectors) and observe the conduct of searches with that equipment.
- Determine the access authorization policies and procedures for visitors, including cleared, uncleared, and foreign national visitors.
- Review:
  - Visit request initiation, processing, and approval
  - Escort requirements
  - Visitor identity verification
  - Visitor access authorization indication (for example, temporary badge, pass, photo identification, temporary card).
- Review automated entry control system policies to determine whether they are adequate. The review should include special features of the automated systems and the methods used to deter, detect, or prevent tampering.
- Determine whether individuals controlling access ensure that only persons with proper authorization are admitted and that positive verification of identity is established.
- Determine whether more than one method of access control is used at a security area (for example, badge check and card reader), how the systems complement each other, and

which is considered the primary means of access control. Similar to the intrusion-detection systems, these access systems should be complementary, not supplementary. A full understanding of the controls used may enable the inspectors to visualize potential problems and means to defeat the controls.

- Determine whether all vehicles, personnel, and hand-carried items entering and exiting MAAs or PAs encompassing an MAA where Category II SNM is stored outside the MAA are searched in accordance with DOE requirements. PAs that encompass an MAA but do not have Category II SNM present outside the MAA can allow for random searches of vehicles, personnel, and hand carried items at a frequency dictated by the cognizant DOE Authority. Inspectors should also determine whether all items belonging to uncleared personnel going in or out of PAs and MAAs are inspected.

Operations

E. Inspectors should observe operations at selected portals to verify compliance with:

- Site-specific procedures
- Personnel and vehicle entry procedures
- Visitor controls
- Personnel and package searches
- Access logs
- Procedures used to place portals in access or secure mode.

During observation of routine portal activities, it is prudent to request (in advance) that the test and maintenance personnel perform their normal testing and calibration activities.

F. Inspectors should observe operations at selected storage areas such as vaults, vault-type rooms and safes. At these locations, inspectors should check entry procedures, including:

- Requests to put alarm systems in access mode
- Lock and double-lock systems
- Entry logs
- Interfaces with protective force or health physics
- Control methods in the access mode, such as:
  - CCTV
  - SPO posted at door
  - Two-person rule
- Lock-up procedures, including exit searches, lock checks, and procedures to place the alarm system in secure mode.

All of these procedures should be reviewed in light of the possibility of a single insider gaining access to SNM or other security interest. The controls should be structured in such a way that DOE interests are not at risk from a single insider.

G. Inspectors should note that except in the case of an emergency response, protective force personnel should not normally be exempt from the requirements for personnel entering certain security areas. Even though protective force personnel are allowed to take authorized weapons and other duty equipment into a security area, they should not be exempt from routine access controls. Such exemption would be an ideal opportunity for the introduction of contraband or unauthorized material into a security area.

Section 4

BADGES, PASSES, AND CREDENTIALS

Contents

General Information

A security badge or pass system is implemented to ensure that only authorized personnel enter, occupy, or leave a security area, and to indicate limitations placed on access to SNM and classified matter.

Badging systems are normally managed within the facility's security organization. However, the actual badging function is often delegated to other groups at the facility. For example, at some facilities, badges are issued and controlled by the protective force; at other facilities, the employment department may handle some badging functions. At large facilities, a group may be specifically dedicated to badging functions.

How the badge system is implemented varies across DOE facilities, depending on the size and complexity of the site. Sites with only one facility usually have a single office that issues badges and passes to employees and visitors.

Sites with multiple facilities may have more than one badge office or a centralized badge office with a number of satellite activities that perform badging functions. Inspectors must be aware of such satellite locations, their functions, and their interface with the centralized badge activity.

Most sites use computer-generated badges that have a magnetic stripe coded for access control. SPOs or other security personnel may use these badges as a stand-alone measure for controlling access to security areas, or in conjunction with a badge check. Although the PSS topic team usually inspects the technical aspects of the coded systems, the personnel security topic team may review procedures for enrolling/deleting personnel in the automated access control system and for issuing and controlling coded badges. Likewise, the cyber security topic team may review procedures for the establishment of access controls for the computers that house the automated access control system (e.g., passwords, firewalls) Because computer-generated badges can be duplicated to near-perfect visual and tactile quality, the review of the facility's program for encoding data on the badges is particularly important at facilities that use those badges as a stand-alone measure to control access to security areas.

The use of integrated systems gives rise to interfaces with badging systems and access control systems. These interfaces constitute a field device network of sorts, which requires protection at the same level as the interests they protect.

Common Deficiencies/ Potential Concerns

Improper Badge Accountability Procedures

Records documenting the disposition of all badges may lack the required information: date of issue, description and serial number of badge, organization, destruction date, and name of holder.

Improper Storage of Unissued Badges and Passes

Facilities do not always adequately protect unissued badges and passes against loss, theft, or unauthorized use. Unissued badges may be improperly stored in an unlocked drawer or file cabinet in a badge office or reception area, and left unattended or uncontrolled at times (for example, when the person issuing badges takes a break or leaves to perform other duties). Improper storage can result in the loss of unissued badges and the potential for unauthorized access, which can be a serious problem if the badges are already coded or if access authorization is controlled by a security officer.

Ineffective Badge Recovery and Untimely Access Termination

Badges of terminated employees are not always promptly recovered before their departure from the site. Recovery of badges issued to long-term visitors, student workers, construction workers, or temporary employees can be a particular problem since such persons do not always follow normal termination procedures when leaving the site. Recovery of badges of employees terminated for cause or misconduct and timely revocation of their access via the automated access control system is particularly important to prevent further access to the site and eliminate the possibility of misconduct by disgruntled employees.

Failure To Update Badge Photos

If employees do not have a new picture taken when their appearance changes significantly, their badges will not reflect their current appearance. Supervisors, security officials, and protective force officers are responsible for ensuring that the badge pictures are current by reporting to the badging authority any employee exhibiting a significant change in facial appearance.

Incomplete Handling of Lost Badges

When badges are reported lost, all personnel responsible for controlling access to security areas (usually SPOs) must be informed so that they are able to prevent unauthorized personnel from using the lost badge to gain area access. However, badge offices do not always inform the protective force (or other groups responsible for access control) about lost badges. Even if the protective force is informed, the procedures for getting that information to the security posts or portals may be ineffective or untimely. Procedures for timely deletion of lost badges from the automated access control system and for notifying other organizations about lost badges are a particular problem. Identifying lost badges at portals is rarely effective since SPOs may not take the time to check the list of lost or stolen badges. Deficiencies in these notifications can lead to unauthorized access.

Insufficient Understanding of Policies and Procedures

A lack of understanding of policies and procedures may be attributable to inadequate training programs or vague, informal, or incomplete procedures.

Insufficient Protection of Field Device Network

The network of devices utilized in the badge-making process should be afforded the same level of protection as the interests they grant access to. Transmission lines may be routed in and out of security areas and thus may not be given the required level of protection. In some cases, the interconnections of these systems may not be in an appropriate security area. The ability to access these systems remotely may also be considered a weakness.

Planning Activities

During the planning meeting, inspectors should interview points of contact and review available documentation and procedures (for example, SSSPs, personnel security operating procedures, badge system policies, automated access control policies, and visitor control policies) to characterize the badge system policies and implementation. Elements to cover include:

- A general description of all badging systems and the interface systems used at the facility, including those implemented by the operations office or contractors

- The organizations responsible for managing and implementing badging functions, including:
  - Enrollment/deletion of personnel in the automated access control program
  - Issuance of employee and visitor badges
  - Control and physical protection
  - Accountability of badges and stocks of inserts
  - Recovery of expired/terminated badges
- Whether any of the badge offices have satellite offices that may perform badging functions
- Procedures for issuing temporary badges to employees who have forgotten them
- General procedures for obtaining a visitor badge or temporary badge
- General procedures for issuing badges to cleared and uncleared foreign nationals
- General procedures for recovering badges from visitors, temporary employees, and terminating employees
- General procedures for escorting uncleared personnel and how escort requirements are displayed on the badge
- General methods for protecting badges, passes, and records, including:
  - Storage practices (for example, a safe or locked room within an LA)
  - Control when the storage area is unlocked (for example, continuous surveillance)
  - Protection of computerized access control/badging systems
- Accountability systems for badges or passes
- Locations where badging functions are implemented
- General procedures for notifying affected organizations and for taking appropriate action in the automated access control system when a badge is reported lost
- Whether site office surveys that include inspection of badges, passes, and credentials are available for review, and if so, whether the survey findings were identified and corrected
- Whether the facility has performed any self-assessments of badges, passes, and credentials (if so, arrange to review the self-assessment reports during the inspection).
- System diagrams and drawings showing interface points with other systems, such as Human Resources or other badging offices.

Once the inspectors have a basic understanding of the management and implementation of the badge/access control system, they determine which organizations, central badge offices, satellite badge offices, storage areas, and access control locations will be reviewed in more depth during the inspection. At most facilities, it will be possible to review all organizations, central badge offices, and access control points. However, at large facilities it is not generally feasible to review every satellite badge office and access point. In such cases, a representative sample may be selected for inspection.

Performance Tests

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

- Badge accountability check (selecting samples of badges and records, and verifying their accuracy) (Appendix A, Part 2)
- Portal badge checks (Appendix A, Part 4)
- Badge issuance (Appendix A, Part 2)
- Removal from automated access control system (Appendix A, Part 2).

Based on the review of the interfaces with this system, an inspection of these locations for appropriate security precautions should be conducted.

In addition to tests conducted by the PSS topic team, any performance tests conducted by the protective force, personnel security, or cyber security topic teams that involve badge checks or other aspects of the badge system are directly relevant to this subtopic.

Data Collection Activities

Badge Construction

A. Inspectors should examine badges to determine whether the badge design and construction preclude inserting a replacement picture without detectable damage to the badge. Inspectors should devote particular attention to temporary badges, passes, and visitor badges.

Documentation and Records

B. Inspectors should review badge/pass system policies and procedures to determine whether they are consistent with DOE requirements and whether the implementing procedures are consistent with site-specific policies.

C. Inspectors should interview selected personnel responsible for administering the badge/access control system to determine whether the site policies and procedures are implemented as required by DOE orders and as described in site-specific documentation. Inspectors should determine whether these individuals understand the purpose of the badge/pass system and their responsibilities concerning issuance, disposition, storage, and recovery. Inspectors may wish to have personnel responsible for the badge/access control system explain each step in the badging process. It is valuable to observe these individuals issuing a badge to an employee, a visitor, or a contractor.

D. Inspectors should examine the access control/badge/pass disposition records and the record of lost badges for completeness and accuracy. This determination typically involves reviewing a sample of lost-badge records.

Access Control

E. Inspectors should interview SPOs who implement badge checks at portals and physically observe or test the portal operations to collect information about how the badge policies and procedures are implemented at the site. Alternatively, the PSS team can coordinate efforts with the protective force, personnel security, and cyber security topic teams to collect the required information. At selected portals, inspectors should attempt to determine whether:

- Post orders relating to badge checks are current and consistent with site policies.
- A copy of the list of lost badges is at the post and includes lost badges of other organizations that are accepted by the facility.
- The SPO is familiar with, and implements, the procedures related to checking the list of lost badges.
- The SPO is familiar with the markings and indicators on the badges.
- The SPO devotes sufficient attention to comparing the person's face to the photograph.

Physical Protection

F. At each badge office selected for review, inspectors should determine whether stocks of unissued badges and passes are stored in a way that assures their protection against loss, theft, or unauthorized use. Storage areas, including satellite locations, should be checked to ensure that stocks are being adequately protected. Specific information to determine includes:

- The methods for storing the unissued badges and passes (for example, safes, locked filing cabinets, locked rooms)
- Whether the storage repositories are protected by alarm systems or security patrols or both
- The frequency of protective force patrols during non-operational hours
- The means of controlling access to the badges or inserts when the repository is open (for example, continuous surveillance)
- Which persons have access to the storage repository or automated access control system (for example, who has the combination to locked safes used to store the badges/inserts or who has the password to the automated system that encodes the badges) and whether those persons are appropriately

cleared and have legitimate need to access the repository/computer

- Based on the protection measures in place (for example, the storage practices, alarms, and patrol frequencies), whether storage meets the requirements for storing confidential matter as defined in DOE Manual 470.4-2, Ch1
- Whether the field device network between badging stations, Human Resources, and the access control systems is appropriately protected.

Badge Recovery

G. Inspectors should review badge records and interview personnel in the badge office to determine whether terminating employees are disenrolled from the automated access control system and whether badges and passes are recovered from them before they leave the site. This can be crosschecked by obtaining, from Human Resources or other appropriate facility departments, a list of employees terminated during a suitable time period (for example, the past three months). The names on the list can then be compared with the automated access control system and badge disposition records to determine whether the badges of these terminated employees were recovered and access was rescinded.

H. Inspectors should review visitor logs and badge records and interview personnel in the badge office to determine whether visitors' badges and passes are recovered at the conclusion of the visit. Inspectors should determine what actions are taken if a visitor forgets to turn in a badge.

I. Inspectors should interview personnel in the badge office and review badge/pass documentation and the automated access control system to determine whether foreign nationals are being appropriately badged (e.g., cleared foreign nationals are issued standard DOE badges with the individual's country of citizenship noted on the bottom of the badge and uncleared foreign nationals are issued a site-specific badge colored red).

Badge Reissue Requirements

J. Inspectors should determine whether employee photos are retaken and badges reissued as required. One way to review this requirement is to observe the badge checks at a portal to determine whether badge photographs accurately reflect the facial appearance of the holder. Another way is to interview supervisors and SPOs to determine their level of awareness of the requirement to report to the badge office any employees who exhibit significant changes in facial appearance. A third method is to review records to determine how many employees have had their photographs retaken in a specified time period (for example, one year). A very small number of retaken photographs may indicate that the requirements are not being followed. If that is the case, the protective force topic team should devote additional attention to portal operations to determine whether personnel have current photographs and whether the SPOs report any discrepancies.

This page is intentionally left blank.

Section 5

BARRIERS, LOCKS, and KEYS

Contents

Many of the basic security system elements revolve around barriers, locks, and keys. Therefore, basic guidance regarding inspection activities provided in Section 5 remain apply when inspecting physical facilities. Barriers control, impede, and deny access and effectively direct the flow of personnel and vehicles through designated portals. Locks and keys help enforce compliance with DOE orders. Therefore, the inspection of barriers, locks, and keys help determine whether the physical security system performs adequately.

This page intentionally left blank.

Section 5.1

BARRIERS

Contents

General Information

Physical barriers control, impede, or deny access and effectively direct the flow of personnel and vehicles through designated portals. The evaluation of barrier system effectiveness is based on whether the system complies with DOE orders and whether performance testing indicates that it performs adequately.

Specifically, barriers are designed to:

- Reduce the number of entry and exit paths
- Facilitate effective use of protective force personnel
- Delay the adversary to enable assessment and protective force response
- Protect personnel from hostile actions
- Channel adversaries into pre-planned neutralization zones.

The following subject areas are addressed in this section:

- Fences
- Buildings (walls, ceilings, floors, doors, windows, and unattended openings)
- Security containers
- Denial systems
- Vehicle barriers.

Fencing is normally used to enclose security areas and to designate DOE property boundaries. Depending on the intended level of security, fences require regular patrolling, continuous observation, or an intrusion detection system supported by an assessment capability. DOE requires that fences:

- Meet specific gauge and fabric specifications
- Be topped with particular wire and outrigger configurations
- Include steel posts with bracing
- Meet certain height and location provisions.

Buildings of various types represent the most common barrier used to protect DOE security interests. Construction features vary throughout the DOE complex. However, there are a number of basic requirements to consider when evaluating the walls, ceilings, and floors that enclose security areas. In general, it is important that building materials be solid and offer penetration resistance to, and evidence of, unauthorized entry. DOE orders and manuals provide requirements for a variety of construction elements, including:

- Wire mesh
- Insert panels
- Sound attenuation for rooms in which classified information is to be discussed
- Storage rooms.

There are also specifications for construction hardware (for example, hardware accessible from the outside is required to be peened, brazed, or spot-welded to preclude tampering or removal).

In addition to the criteria for walls, ceilings, and floors, there are requisite construction requirements for doors, windows, and unattended openings. It is important that doors offer resistance to forced entry. When necessary, reinforcement is required for doorjambs, louvers, and baffle plates. Windows, when relied on as physical barriers, must be constructed of shatter-resistant, laminated glass of a minimum thickness, and installed in fixed frames so that the panes are not removable from the outside. It is essential that window frames be securely anchored in the walls, and that windows can be locked from the inside. Unattended openings, under certain conditions, are to be alarmed or equipped with steel wire mesh and steel bars with steel crossbars, which are checked for integrity during patrols.

The GSA establishes standards for security containers. Although classification is the only security factor that determines the degree of protection required for classified matter in storage, other considerations include:

- Strategic importance
- Susceptibility to compromise
- Effect on vital production
- Health and safety
- Replacement costs.

Other DOE requirements address:

- Protective force inspections and patrols
- Transfer of security containers
- Protection of security containers and combinations
- Security repository information
- Repair of containers.

Active denial systems include cold smoke, CO_2, and other dispensable materials, such as sticky foam, rigid foam, sprays, and irritant agents. It is important that these substances be properly maintained and protected against tampering. Other systems may incorporate flickering light or intense sound systems to delay, confuse, or otherwise hamper adversaries.

Passive denial systems include building structures (for example, walls, doors, floors, ceilings, and windows), security bars, and large natural or manmade objects (for example, large boulders or concrete blocks). It is important that the mechanism for moving or method of disengaging passive systems be protected at the same level as the interests they protect.

Vehicle barriers are used to deter penetration into security areas when such access cannot otherwise be controlled. Vehicle barriers may include pop-up barriers, cable, bollard configurations, or natural terrain obstacles (for example, bodies of water, ravines, tank traps, ditches, adler barriers, steep hills, or cliffs).

Common Deficiencies/ Potential Concerns

Fences

To be effective, fencing must be checked and repaired on a regular basis. Frequently, the fence fabric is not properly attached to the support poles and the bottom wire is not secure. Erosion of the ground under the fence often results in gaps or washouts that may allow someone to crawl under the fence. Another common problem is that vegetation is allowed to grow up close to the fence, providing cover to potential adversaries or a possible platform for climbing over the fence.

Buildings

Suspended ceilings and raised floors often create the illusion that they represent the “hard” surfaces of the enclosed space. Inspectors often overlook these configurations. The ceiling and floor panels must be inspected to ensure that the true “hard” walls and surfaces of the building are identified, especially in locations where such walls form a PA, MAA, vault or vault-type room, or SCIF.

Security Containers

Some facilities have requested and received exceptions for the use of non-GSA-approved containers for storing classified documents. Inspectors should not assume that all facilities

have these exceptions. All exceptions received by the inspected facility should be reviewed before the onsite inspection to determine whether they are current.

Denial Systems

A form of denial system used at some DOE facilities consists of an extremely heavy block of concrete placed in front of an access door to protect critical assets. To gain access, a hydraulic vehicle or some other lifting mechanism must be used to move these barriers. Since these vehicles or mechanisms are therefore critical to the effective application of this kind of barrier, they must be afforded an appropriate level of protection. Inspectors should check to ensure that these items of equipment are appropriately protected and properly maintained.

Vehicle Barriers

Vehicle barriers must be effectively monitored, and components must be appropriately located. Barriers should be within an area that is protected by detection sensors.

Active Denial Systems

Adequate measures must be provided to prevent an insider from disabling active denial systems (such as cold smoke or sticky foam). Since most such systems have a single location for firing, that location is vulnerable to insiders unless sufficient protective measures are employed.

Planning Activities

During the planning meeting, inspectors should interview points of contact and review available documentation relative to the presence and use of barriers. This documentation should include building construction drawings, focusing on barrier construction details and heating, ventilation and air-conditioning ducts. Elements to cover include:

- The general types of barrier systems (e.g., fences, standard building materials, reinforced/hardened building materials) in place at each security area, including:
  - Property Protection Area
  - LA
  - Exclusion Area
  - SCIF
  - Secure communications center
  - PA
  - MAA
- The types of barrier systems associated with the various storage/process areas (e.g., vaults, safes, vault-type rooms) used to protect SNM and classified matter. In particular, determine:
  - Whether active denial systems (e.g., smoke, foam) are used
  - Whether items within storage areas (e.g., vaults) are protected by additional controls (e.g., locked compartments, tie-downs)
  - Methods for providing delay when material is in use and when storage areas are in the access mode
  - Interfaces with entry controls and intrusion detection systems
  - Whether airborne denial systems are in place in any areas
- The types and locations of vehicle barrier systems.

Performance Tests

No performance tests are directly relevant to this subtopic. The use of performance test results to identify delay times is discussed under Delay Times in the Data Collection Activities section.

Data Collection Activities

General

A. Inspectors should determine whether barriers at facilities with Category I SNM or classified matter provide sufficient delay to allow the protective force to assess alarms and respond with sufficient force to neutralize the adversaries before they have completed their intended purpose. (This is generally evaluated based partially on a review of vulnerability assessments [VAs].)

B. Inspectors should determine whether barriers are sufficient to ensure that SNM cannot be removed from the area without causing an alarm or immediate visual evidence of tampering.

Also, inspectors should determine whether barriers are sufficient to channel personnel through designated portals or into adversary neutralization zones.

Perimeter Barriers

C. For security areas where a perimeter barrier system is used, inspectors should determine what types of barriers are in use (for example, fences, wire, vehicle barriers, or natural obstacles), whether they meet DOE requirements, and whether all barriers are accurately represented in VAs and in the SSSP. Inspectors should determine whether procedures are in place to prevent transferring contraband or SNM over an exterior perimeter barrier (for example, throwing or slinging items over a fence for later pickup). Preventive measures may include wide isolation zones, extra-high fences or nets, or adequate surveillance by protective force personnel.

D. Inspectors should examine fences to determine whether their condition would allow adversaries to get through or bypass them without being detected. Some items to consider include:

- Erosion in isolation zones or under fences that may allow an adversary to pass undetected
- Unprotected pipes or wires that pass over fences or other perimeter barriers and allow an adversary to pass over the barrier
- Tunnels, underpasses, culverts, or pipelines that pass under the perimeter barriers that are not adequately protected
- Adjacent structures in close proximity to either side of the fence that could facilitate bridging.

Buildings

E. Inspectors should determine whether construction materials are sufficient to provide appropriate delay against a number of adversary penetration methods, including hand tools, power tools, and explosives.

F. Inspectors should examine vaults and vault-type rooms to verify compliance with the construction requirements specified in DOE Order 473.1 and DOE Manual 470.4-2 Ch1. Inspectors may accomplish this by visual examination and by looking at vault construction diagrams.

G. Inspectors should check security containers to verify compliance with construction requirements specified in applicable DOE orders.

H. Inspectors should be prepared to conduct a thorough examination of a building. If only a portion of the building is a security area, inspectors should be prepared to tour the security area perimeter. It may be helpful to carry building floor plans. Other areas that should be checked include:

- Air ducts
- Electrical conduit and pipe penetrations
- Storage areas
- Walls
- Windows
- False ceilings
- Underground pathways.

I. Inspectors should review fixed barriers that protect protective force personnel (for example, towers, portals, alarm stations, and defensive positions) to determine whether they meet the requirements of DOE Order 470.4 and DOE Manual 470.4-2 Ch1. Reviewing documents, interviewing security staff, or conducting visual inspections may accomplish this. A requirement that applies to posts constructed after 1985, designed to protect SNM (Category I or II), is that the exterior walls, windows, and doors must provide bullet resistance equivalent to the "high-power rifle" rating of UL 752. This can be checked by looking for a marking or stamp on the window or structure that indicates High-Power Rifle (HPR), or Level 8 protection. Inspectors should also determine whether procedures are in place to preclude protective force personnel stationed within these posts from activities that could negate the purpose of these hardened posts.

J. Inspectors should review the design of vehicle barriers to determine whether they meet DOE standards in accordance with the applicable Design Basis Threat. This determination may

require interviewing the responsible engineers, reviewing vendor data, or reviewing test results. Inspectors should also review barrier operational procedures to ensure that they are effectively integrated into the protection strategy. Barriers left in the "down" position until identification of a potential threat or during a heightened security event do not prevent penetration by a malevolent vehicle during normal operations. Additionally, if credit is taken for emergency "up" operation of the barrier in the production strategy, testing should be performed to determine whether the speed of barrier activation is adequate to counter the Design Basis Threat.

K. Inspectors should review active denial systems to determine the effectiveness of their activation methods and the conditions and procedures for activation. These systems should be examined to determine whether they are properly installed and in good condition, have effective power and backup power sources, and are tamper-resistant. The operator's familiarity with system activation should also be checked.

Delay Time

L. Inspectors should review documents, interview security staff, review as-built designs, and visually inspect barriers to determine the delay times the facility has estimated for various barriers. These estimates should be reviewed to determine whether they are credible and whether protection is balanced. (For example, a vault door used in a room with transite walls is a case of inappropriate protection, since one barrier is significantly more vulnerable than the other.) Inspectors can also compare delay time estimates with response times and response procedures in order to determine whether response plans are effective and give appropriate consideration to the physical security hardware.

Guidelines for identifying penetration times by reviewing site-specific documents are:

- SSSPs should contain parameters related to barrier delay times or to the minimum delay times required to ensure an effective response. Such delay times may relate to individual components (such as doors) or to the total delay time involved in reaching a target or performing an action. However, most SSSPs do not provide this level of detail. Instead, they usually reference a site security plan or VA that may include delay time information.
- SSSPs may describe barriers, including doors and adjacent barriers. These descriptions may include penetration times for individual barriers or may reference the data source.
- VAs may contain penetration times for individual barriers in one or more locations. The narrative may address individual barriers and may include delay times. Also, computer codes are frequently used to conduct the VA. The input to these codes frequently includes delay times. For example, the Analytical System and Software for Evaluating Safeguards and Security (ASSESS) or ATLAS codes are frequently used when developing VAs at DOE facilities. The input includes delay times for portal entry doors, exit doors, and surfaces. When reviewing computer input to determine the penetration times assumed by the facility, the following points should be considered:
  - The input delay times may be different for different facilities or for different scenarios.
  - The input delay times may assume that the door is secure, whereas there may be scenarios where the door is open or in access mode.
  - If several barriers are in a series, the delay times may be added if the adversaries must pass all barriers to reach a target.
- System requirements documents or design specification documents are an excellent source for determining expected penetration times. Unfortunately, such documents are not always available or are difficult to find. If these documents are available, the responsible security engineering group is the most likely source.
- Penetration times for doors and adjacent barriers can be significantly affected by a number of factors, including the mode and

timing of the adversary attack and the adversary's level of sophistication.

Guidelines for visually inspecting barriers and reviewing as-built diagrams are:

- The construction and materials used in barriers can usually be determined by visual inspection or by a careful review of as-built diagrams. With this information, inspectors can generally make a rough estimate of penetration resistance. The Sandia Access Delay Technology Transfer Manual and other security design manuals may be useful for this purpose.
- During a visual inspection, the inspectors should focus on barrier deficiencies or design flaws that an outsider could exploit, allowing surreptitious penetration of the barrier, or a penetration in less time than estimated that an insider could exploit, allowing defeat of the protection element or allowing the insider to provide assistance to an outside force.

Guidelines for gathering information on penetration times by interviewing security staff or engineers are:

- Discussions with security personnel who conducted the VAs or who are responsible for barrier design may be useful for reviewing site-specific documents.
- If penetration times have been documented, inspectors should interview knowledgeable security personnel to determine how penetration times were developed, what assumptions were made, what modes of attack were considered, and what adversary threat characteristics were assumed.
- If penetration times have not been documented, inspectors should interview knowledgeable security personnel to gather information on the effectiveness of the barrier design. Some potential discussion topics are:
  - Alarm response procedures (in particular, the sufficiency of response time in terms of barrier design)
  - Whether penetration resistance was factored into response plans
  - Design and construction (materials used, use of tamper-resistant hardware, hardening of barriers as part of an upgrade program).

General guidelines for using performance test results (conducted by HS-61 or others) to identify delay times are:

- HS-61 may conduct performance tests of barriers to determine penetration times. However, such tests frequently involve destructive techniques. It would be rare for HS-61 to conduct destructive tests of barriers for a variety of reasons, including:
  - Safety concerns
  - Cost of replacement
  - Impact on operations and security
  - Difficulty involved.
- Tests involving a significant potential for personal injury (for example, crawling through razor ribbon) are not conducted.
- The types of tests for penetration times that inspectors would typically conduct are simple ones designed to demonstrate potential vulnerabilities. For example, an inspector may conduct a simple test of an adversary's ability to defeat a steel-grate door that has a crash bar on the inside; such a test might involve inserting a bent rod through the steel grate to engage the crash bar. Such tests may demonstrate that the assumed delay times did not consider all credible modes of attack.
- HS-61 inspectors may identify penetration times by reviewing the results of tests on similar barriers that were conducted by the facility, other DOE elements, or outside agencies. Frequently, facilities conduct (or contract others to conduct) tests of barriers prior to their installation. Also, vendors often have penetration time results for selected modes of attack. HS-61 may collect and review such information. However, test results should be reviewed critically, with particular attention to:
  - How the penetration times were determined
  - The modes of attack considered

– The level of adversary sophistication

– The type of results reported.

Other general guidelines to be aware of when dealing with penetration times are:

- Penetration times are significantly influenced by the mode of attack. For example, hardened doors that would take several minutes to penetrate with power tools frequently can be breached via explosives in less than one minute. Inspectors should review the data and determine whether the modes of attack that the site has considered are consistent with the parameters of the approved threat guidance.
- Actions by a well-placed insider can defeat most barriers. For example, an insider can open a door from the inside and allow adversaries to enter, thus reducing the delay provided by the door. Inspectors should look for design features that would make a barrier particularly susceptible to defeat. Inspectors should also look for key insiders who are in a position to defeat multiple layers of protection. The inspection team should identify other protection measures in place to prevent insider tampering (for example, protective force patrols). The fact that well-placed insiders can defeat a barrier does not necessarily make that barrier inadequate, since multiple layers of protection should be afforded SNM. The potential actions of an insider need to be examined in a broader context and considered in light of multiple layers of protection and the parameters of the SSSP.
- There is inherent uncertainty associated with penetration time estimates; they are not precise values. Consequently, any comparison of penetration times is by its very nature a rough comparison. The intent is to determine whether the protection is reasonably balanced and whether the barriers provide sufficient delay to allow effective response. For example, if the penetration time of a door is 1.5 minutes, whereas the penetration time of the adjacent wall is two minutes, this will not normally be cause for concern (assuming that the overall delay time is sufficient to allow an effective response). However, if a Class 5 vault door is installed in a transite wall, this would clearly indicate unbalanced protection. One reference used throughout the DOE community is the Sandia Access Delay Technology Transfer Manual.

This page intentionally left blank.

Section 5.2

LOCKS AND KEYS

Contents

General Information

Locks are an integral part of the physical barrier system and are used to control, impede, or deny access, and effectively direct the flow of personnel and vehicles through designated portals. The effectiveness of security locks is based on compliance with DOE orders and whether performance testing indicates that the system performs adequately. The requirements for security locks are determined in light of the security interest being protected, the identified threat, existing barriers, and other protection measures.

Specifically, locks are designed to:

- Reduce the number of entry and exit paths
- Keep unauthorized personnel from entering areas where they are not allowed
- Control access to assets within areas to individuals with an approved need.

Security keys include mechanical keys, key cards, and access codes. Security keys do not include administrative or privacy lock keys to factory-installed file cabinet locks, desk locks, toolboxes, etc. Because keys are easily duplicated, it is imperative that a strict key control program be developed, implemented and effectively managed.

The following subject areas are addressed in this section:

- Types of locks and specifications
- Levels of protection and requirements
- Storage requirements for locks and keys
- Lock and key control management.

The requirements for security locks must be applied in a graded fashion. Locks used to protect classified matter and Category I and II SNM in GSA-approved security containers, vaults, or vault-type rooms must meet Federal Specifications. (See Federal Specification FF-L-2740A, Locks, Combination.) Key locksets must meet American National Standards Institute (ANSI) Standard A156.2-1996, Grade 1, *Bored and Preassembled Locks and Latches*, or ANSI A156.13-1996, Grade 1, *Mortise Locksets.* DOE Manual 470.4-2, Ch1, provides other specific requirements for these locksets.

Security key padlocks that are considered high-security, must be shrouded-shackle and key-operated and must meet standards in MIL-P-43607, *"Padlock, Key Operated, High Security, Shrouded Shackle.*

Security keys, key blanks, and key cutting codes must be protected in a graded fashion. The same protection considerations that apply to keys also apply to locks: the interest being protected, the identified threat, existing barriers, and other protection measures afforded the asset.

Locks and keys are categorized according to the asset being protected, and an inventory and accountability system must be implemented.

Security locks and keys are divided into four levels, Level I through IV. Level I locks and

keys are used to protect nuclear weapons, weapon components, Category I SNM, Category II SNM that rolls up to a Category I quantity, certain high value government assets, and Top Secret and/or Secret classified matter. Security key blanks must be restricted/proprietary. Security locations such as vaults, vault-type rooms, MAA, SCIFs, and exclusion areas where top secret and/or secret documents are stored require Level I security locks and keys. See DOE Manual 470.4-2, Ch1 for other specific requirements.

Level II security locks and keys are used for building doors, entry control points, gates in PA fences, and exclusion area doors or other barriers or containers that protect Category II and Category III SNM and classified matter, including documents classified at the Confidential level.

Level III security locks and keys are used on buildings, gates in fences, cargo containers, and storage areas for protecting government property.

Level IV locks and keys are typically used for offices where there is no open storage of classified material.

Security locks and keys must be stored in a manner that prevents loss, theft, or unauthorized use. Once Level I locks and keys are put in service inside a PA, they must not leave the PA without authorization. Assembled security locks or cores and Level I security keys must remain under the direct control of a responsible person or must be stored in a GSA-approved repository or vault-type room when not in use for the protection of the assets previously mentioned. Level I keys must be segregated from all other keys on key rings and in key storage cabinets. Keys to storage cabinets must be in the physical possession of an authorized person or locked in a GSA-approved repository.

Level II locks and keys, once put into service, must not leave the facility without authorization. Site specific procedures must be developed for control and accountability of Level III security locks and keys, while Level IV locks and keys have no requirements for control and accountability.

Common Deficiencies/ Potential Concerns

Many of the locks used for security purposes are advertised as "high-security" or "medium-security" locks. However, when examined, these lock specifications often do not meet the required MIL standards or DOE requirements. Inspectors should be aware that the terms "high security" and "medium security," when used commercially, may not have the same implication as they do in DOE orders.

Effective control must be maintained to assure locks and keys are used appropriately. Combinations must be changed at specified times and under specified conditions, and key control procedures must be documented and followed. Appropriate procedures for dealing with lost keys must be established. Additionally, when keys are lost, stolen or otherwise unaccounted for, proper reporting must be completed according to DOE Order 470.4, *Reporting Incidents of Security Concern.*

Other common deficiencies in the lock and key program occur when custodians do not maintain an effective accountability system for security keys and allow obsolete or unusable keys to accumulate without taking appropriate destruction action. Inspectors should review inventory records to assure there is "cradle to grave" accountability for security keys and an adequate destruction process in place. Inspectors should also review the organization's self-assessment program to assure that it adequately addresses the lock and key control program. Additionally, DOE site office survey programs should include the lock and key programs in their annual surveys of contractor organizations.

Planning Activities

The objective for organizations is to reduce the number of keys and move toward a keyless access control technology. This new effort would assure that access is not afforded to any single physical item or object that can be lost or stolen. Inspectors should review plans proposed or in process at each site and DOE site office to determine the status of this initiative.

Recognizing that this is a long-term initiative, inspectors need to review the existing lock and key programs to determine the effectiveness of the system.

Inspectors should review the key control system to determine whether procedures are in place to adequately control keys and locks. Typically, an effective key control system includes procedures that address control and accounting for keys and lock sets (this includes issue, sign-out, inventory, destruction, and the key and lock numbering system), and procedures used when a key is unaccounted for. Other factors that may be included are:

- Criteria for issuing a key or combination to a person (for example, supervisors developing authorized lists and notifying locksmiths in writing)
- Procedures for changing lock combinations (for example, when a person possessing a combination transfers, resigns, is dismissed, or no longer requires access
- Procedures and conditions for changing key locks or lock cores.

It may also be helpful for inspectors to visit the lock shop or interview the locksmith to determine the adequacy of methods used to protect keying and core information. Other factors that should be considered are:

- The procedures for notifying the locksmith that locks or combinations need to be changed, and the time required to accomplish these changes. Inspectors may identify these items by reviewing records. For example, when locks are changed because of a lost key, inspectors should be able to locate the records indicating when the key was reported lost, when the custodian reported the loss to the locksmith, when a work order was issued, and when the work was completed.
- The methods for numbering keys and locks, and whether the numbering methods unwittingly reveal information about the master-keyed system.
- The procedures for periodically changing combinations and lock cores.
- The procedures for maintaining locks, particularly locks that are exposed to severe weather conditions.

Performance Tests

Performance tests validate the effectiveness of implemented requirements and inspectors should conduct performance testing of the lock and key program as necessary. The following performance tests are suggested but are not inclusive. Inspectors should develop and conduct other performance tests as appropriate.

- Randomly select Level IV keys using lock and key records. Physically verify that these keys only access offices where no government assets are located and where there is no open storage of classified matter.
- Randomly select Level I and II keys using lock and key records. Physically locate the keys to determine whether they are or have been removed from the PA (Level I) or facility (Level II).
- Randomly select Level I, II, and III keys using lock and key records and physically locate the keys to verify accountability.

Data Collection Activities

A. Inspectors should determine whether the organization is moving forward on the keyless access control initiative by reviewing project plans, budget documentation, milestones, etc. Inspectors should also determine the effectiveness of the existing lock and key control program by gathering data to answer the following questions:

- Have locks and keys have been correctly characterized using a graded approach based on the asset being protected?
- Are locks, keys, and other access control devices protected according to DOE Manual 470.4-2 Ch 1?
- Have procedures been developed and implemented that define the administration

and management of the lock and key program, including roles and responsibilities?

- Has an effective incident reporting system been developed that includes lost, stolen, and unaccounted-for Level I, II, and III keys?
- Is the number of keys and access control devices limited to the absolute minimum required for mission completion?
- Are master keys strictly limited?
- Are keys restricted from leaving security areas and facilities as required by DOE Manual 470.4-2 Ch 1?
- Are all keys accounted for, and is there a current inventory on file?
- Is lock and key control management included in the contractor self-assessment program and the site office survey program?
- Is there strict accountability of keys using either an automated or hard-copy issuance record?
- Has an effective database been developed to account for and track all Level I, II, and III keys?

Section 6

COMMUNICATIONS

Contents

General Information

Physical security systems cannot operate independently of the human element, and since some sites are quite spacious, there must be a method for communicating quickly, clearly, and reliably. Telephone, radio, and duress alarms provide the necessary communication links among the alarm stations, mobile and fixed posts, response forces, and LLEAs. The effectiveness of communications equipment is based on compliance with DOE orders and performance during equipment testing and performance tests.

DOE policy requires that communications equipment allow the effective protection of safeguards and security interests by providing rapid, reliable, and protected information exchange between onsite protective personnel and the CAS and SAS.

The design of communication systems must be such that no single event can disable all modes of communication between the CAS and fixed posts or between the alarm stations and LLEAs. Communications equipment and systems are required to be tested daily for operability, and alternate communications capabilities are required to be available immediately upon failure of the primary system. Records of the failure and repair of all communications equipment are required to be maintained in a form suitable for compilation by type of failure, unit serial number, and equipment type.

The following subjects are covered in this section:

- Radios
- Telephones
- Duress alarms
- Intercoms, public address, pagers
- Audio recording systems.

Radios are used for voice communications among members of the protective force and alarm stations, and with DOE managers and other participants, when required. Additionally, radios are used to communicate with LLEAs who participate in exercises or respond to emergencies. In order to provide the flexibility necessary for all participants who may be required to participate in radio communications, it is important to have a number of frequencies available, especially during emergency conditions—for example, one frequency for members of the protective force, one for Special Response Teams (SRTs), and one for communicating with LLEAs. Also, it is critical that radios be readily available in sufficient quantities to equip protective force personnel and to facilitate the performance of their duties.

When repeaters are used to increase radio communications range and clarity, it is important that these devices (antennas and other exterior components) be protected from tampering or sabotage. Also, a good radio system usually has an effective preventive maintenance program in place to ensure that radios and radio components remain functional.

Although alarm stations and radio communication centers should have both radio and telephone channels of communication with LLEAs, the telephone is normally the primary means of communication between protective forces and LLEAs, and between the site and DOE Headquarters or the DOE Emergency Operations Center (EOC).

Telephone systems are the primary means of communication at most DOE facilities. Although the telephone is often taken for granted, it is important that the telephone system that is used for security purposes be protected (alarmed, buried cable, or line in a conduit) and have backup provisions, especially when used for direct-line communication between the CAS/SAS and guard posts. It is also important that a good preventive maintenance system be in place to ensure that the system remains reliable and operates at peak performance.

Duress alarms are primarily used to alert protective forces to emergency or duress conditions. It is important that the alarm be activated in an unobtrusive manner and that it not annunciate at the post initiating the alarm. Usually these alarms are hardwired devices that are protected from tampering. Radios also may include a duress feature. All duress systems should have procedures in place that provide for maintenance and testing to ensure that they remain in good working condition.

Intercommunication (intercom) and public address systems are normally used to provide information or instructions to selected organizations or individuals, or to the general facility population. Pagers and/or cellular phones may be used for contacting individuals or sending messages, and they are often issued to key security, safety, and management personnel who must be notified in case of an emergency. All of these devices are especially important during emergency situations when speed is critical and when instructions must be disseminated to as many people as possible.

A continuous electronic recording system is used to record all security radio traffic. This will usually include all protective force radio transmissions and duress alarms, and transmissions going into and out of the CAS or operations center. Sometimes, telephone conversations conducted over security channels are also recorded.

Common Deficiencies/ Potential Concerns

Radios

Although radios are required to provide a multichannel capability, some radio systems used at DOE sites do not have enough channels (radio frequencies) available to provide effective communications for all who need to use the radio. If too few frequencies are available, the primary frequency becomes cluttered with radio traffic. It then becomes difficult to transmit messages, transmissions are confusing, and the probability of losing important information increases. This problem is intensified during emergencies, when radio traffic normally increases. Also, an insufficient number of frequencies limits the use of the radio when adversaries deliberately jam the primary frequency. When there is an insufficient number of frequencies, inspectors should determine how the site manages the available frequencies and whether it provides alternate means of communication.

When encrypted radios are in use, the procedures for installing encryption codes or for switching to the secure mode are often inadequate. Inspectors should determine whether problems with encrypting codes are present and what procedures, if any, are in place for installing codes, changing data encryption keys, and switching to a secure mode. Also, radios issued to SRTs often do not have voice privacy or an encryption mode of operation.

Frequently, sites have not conducted a formal, systematic study of radio transmission and attenuation to identify dead spots and range limitations, or to determine what effect inclement weather has on the radio system. This is particularly important in facilities constructed with reinforced concrete. If such a study has been completed, inspectors should examine the results to determine what action was taken to correct or mitigate any deficiencies.

Often, there are inadequate protective measures, or no protection at all, for radio antennas, repeaters, or other exterior radio components to preclude tampering or sabotage.

Telephones

Frequently, onsite telephone lines and switches are not protected against tampering or sabotage.

Duress Alarms

On occasion, hardwired alarms, switches, and junction boxes are not protected from tampering. Duress alarm capabilities should be provided emergency or auxiliary power for continued operation during commercial power outages.

Intercoms, Public Address, Pagers

Frequently, public address or paging systems are not provided with backup power and/or are not appropriately protected even when they are critical elements of the security communications network.

Intercoms and public address systems are not adequate for use in contacting the majority of facility individuals in case of an emergency.

Key security, safety, and management personnel are not normally provided pagers or cellular phones.

Audio Recording Systems

Frequently, recording system tapes are not kept or stored as part of the alarm station historical data. This media should be treated the same as an alarm log or record and should be maintained for a predetermined length of time.

Planning Activities

Inspectors review documents and interview points of contact. Elements to cover include:

- Description of the basic communication systems, local transmitters and repeaters, and duress systems
- Types of communication equipment used in the CAS, the SAS, protective force posts, the EOC, and patrol vehicles
- Types of communication equipment issued to each SPO and SPO supervisor
- Reports documenting site performance tests of communications equipment and system administrator trends and analyses.

Performance Tests

- Radio Equipment (Appendix A, Part 1)
- Duress Alarms (Appendix A, Part 2)
- Auxiliary Power Supplies Test(Appendix A, Part 1).

Data Collection Activities

A. Inspectors should tour selected areas, visually inspect equipment, and verify information gathered in interviews and document reviews. Equipment in the CAS and SAS should always be inspected. Selected fixed and mobile protective force posts should also be reviewed for operability and familiarity with communications equipment, primary and auxiliary power supplies, protection against tampering and sabotage, and ease of operations.

Radio Systems

B. Inspectors should review documents and interview security staff to determine whether an adequate number of radios and radio frequencies are available to the protective force, SRTs, managers, and other participants in routine and emergency conditions. If an encryption system is used, inspectors should determine whether procedures are in place that adequately explain how to install encryption codes, when and how to change encryption keys, and when and how to switch to the secure operating mode.

C. By interviewing security staff, inspectors can often determine whether there are transmission problems due to dead spots, range, interference, or severe weather conditions. If these problems exist, inspectors should determine what has been done to mitigate these problems.

D. During the inspection of entry portals, vaults, and the PIDAS, inspectors should observe the effectiveness and clarity of communications. This information can assist in properly evaluating the routine use of various communication systems used by security personnel.

E. Inspectors should determine whether antennas, repeaters, or other exterior radio components are protected from tampering or sabotage. Also, inspectors should identify the measures used to provide reliable communications in the event of sabotage, including the primary and backup power sources.

F. Inspectors should determine whether there are procedures for testing radios and, if so, how often the tests take place and what actions are taken when deficiencies are found.

G. Inspectors should examine preventive maintenance procedures to determine whether there are provisions for maintaining base, mobile, and handheld radios and for battery replacement and charging. Inspectors should also determine whether there are alternate methods or compensatory measures when radio equipment is unavailable.

Telephones

H. Inspectors should review telephones and telephone equipment to determine whether telephone lines and switches are protected from tampering or sabotage and whether operational features (for example, simplex or duplex, sound powered, or automatic ringdown) are adequate for all contingencies.

I. Inspectors should determine what measures are in place to provide backup communications, especially for emergency conditions, in the event that the telephone system fails.

Duress Alarms

J. Inspectors should determine whether protective force posts are equipped with hardwired duress alarms and, if so, whether they are protected against tampering (for example tamper switches, junction boxes, and line supervision). If handheld radios do not include a duress feature, inspectors should determine whether there are alternate means of indicating a duress condition. Also, inspectors should identify the primary and secondary locations where duress alarms are monitored to determine whether alarm annunciation is adequate and whether protective personnel can easily identify it. Further, the auxiliary power provisions (for example, battery or generators) should be identified to determine whether they are adequate for all duress alarm systems, including radios.

K. Inspectors should determine the method and frequency for testing duress alarms, including hardwired and radio. These tests can be observed at the primary monitoring station or at the individual guard posts. Also, the operator logs at the CAS and SAS can be examined to verify that tests are performed at the required frequency.

Intercoms, Public Address, Pagers

L. Inspectors should review documentation and interview security staff to determine how these systems, if any, are used in communicating security information to the facility population. Some elements to consider include:

- When and how pagers/cellular phones are used for security purposes
- Provisions for use in high-noise areas or electrical interference environments.

M. Inspectors should verify operability by observing equipment being used or by conducting operability tests.

Audio Recording Systems

N. Inspectors should interview security staff to determine whether audio recording systems record all security radio traffic, and whether duress alarms and telephone conversations are recorded. Also, inspectors should determine whether recordings are appropriately maintained. Further, inspectors can determine by listening to recordings whether radio checks and testing are performed as required, and whether radio transmissions are clear during a range of conditions. This involves listening to recordings selected from various times of the day and under different weather

conditions, including periods of severe weather (such as thunderstorms). Inspectors should determine whether anyone reviews the recordings on a routine basis and whether any action is taken on the information taken from the recordings. Inspectors should review that the DOE Headquarters Chief Information Officer's permission letter for recording is available.

This page intentionally left blank.

Section 7

TESTING AND MAINTENANCE

Contents

General Information

All physical security systems require the support of a comprehensive testing and maintenance program in order to ensure that each component remains functional and reliable. If properly conducted, testing and maintenance can minimize equipment failures, forecast impending operational problems, identify functional weaknesses, and guide in future upgrades and improvements.

DOE orders require that security-related systems and components have a regularly applied test and maintenance program to ensure operability. If a system fails, compensatory measures must be implemented. Further, the people who test, maintain, or service alarm systems are required to have clearances consistent with the highest classification level being protected, unless such testing and maintenance activities are performed as bench services away from the protected location or under the supervision of a cleared and knowledgeable custodian, and the systems/components are rigorously tested prior to being placed in service.

The following subject areas are covered in this section:

- Performance testing
  - Operability testing
  - Effectiveness testing
- Corrective maintenance
- Preventive maintenance
- Record keeping.

Performance testing is divided into two levels: operability tests that provide a simple measure of integrity on a frequent basis, and effectiveness tests that provide comprehensive assurance of integrity on an infrequent basis.

Operability testing is a continuing evaluation process that tests access control devices, intrusion-detection systems, communications equipment, auxiliary systems (power sources and lighting), and other critical systems, such as activated barriers.

The operational effectiveness and protection threat levels determine effectiveness testing frequency, including performance testing of protective force personnel.

Details on testing personnel and procedures are provided in Appendix A. Effectiveness testing usually covers the range of performance parameters required in the facility's approved SSSP and includes the number of tests specified in the Performance Test Program Plan.

Corrective maintenance must be initiated within 24 hours of the detection of a malfunction of site-determined critical system elements at facilities where Category I and II quantities of SNM, vital equipment, or Top Secret matter is protected. For critical systems, compensatory measures must be initiated immediately to provide equivalent protection to those critical components that are out of service. Such measures will continue until maintenance is complete. These measures should be documented.

Preventive maintenance must be performed on all safeguards and security-related subsystems and components. The frequency of such maintenance is to be documented in the SSSP or security plan. All of the following elements are required to be included in a preventive maintenance program:

- Intrusion-detection systems
- CAS/SAS alarm, assessment, surveillance, and communication systems
- Advanced systems technologies (e.g., forward looking infrared [FLIR], remotely operated weapons systems [ROWS], and video motion detection [VMD]
- Communications equipment
- Personnel access control and inspection equipment
- Package and material inspection equipment
- Vehicle inspection equipment
- Security lighting
- Emergency power or auxiliary power supplies
- Keys and locks
- Protective force equipment (not including personal issued equipment and vehicles).

The results of both operability and effectiveness tests are to be recorded and kept on file.

Common Deficiencies/ Potential Concerns

An effective testing program normally includes written procedures that ensure consistency and are comprehensive enough to provide for continuity if the individuals who regularly perform testing are absent. The level of detail should be such that a competent technician can perform the required testing without significant prior knowledge of the system.

Occasionally, when the program is administered by people who have been around for a long time, testing becomes routine, based on memory and experience rather than up-to-date written procedures. In this situation, inspectors should examine the program documentation to determine whether it is complete and whether it provides enough detail to ensure continued program effectiveness.

Frequently, protective personnel are improperly or inadequately trained to test the systems for which they are responsible. Many times, members of the protective force perform the required tests without any in-depth knowledge of the system or comprehension of why the test is performed. For example, they may know that if they walk through a metal detector wearing all of their service equipment, the detector should generate an alarm; however, they do not realize what they have just tested. This lack of knowledge may also apply to the many test objects used for testing other search equipment on which SPOs routinely rely.

Sometimes the compensatory measures that are put in place when critical components are out of service are not adequate to ensure equivalent protection.

The preventive maintenance program may not be routinely comprehensive enough to properly maintain all safeguards and security-related subsystems and components, or may not reflect the maintenance required by the SSSP or security plan.

Records reflecting the results of both operability and effectiveness tests may not be complete.

Planning Activities

Inspectors should review documents and interview security staff to determine the organizations and individuals responsible for testing, calibrating, and repairing each type of security-related system or component used by the facility. Items to consider include:

- More than one organization may be involved with testing equipment. For example, SPOs may conduct an operability test of metal detectors once per shift, and security technicians may perform a functional test once per week.

- More than one organization may have responsibility for a system or component. For example, SPOs may perform routine tests of SNM detectors, MC&A technicians may be responsible for calibration, and security department technicians may be responsible for repair.

Elements to cover include:

- Testing and maintenance procedures for all security-related systems
- Frequency of testing for security-related equipment, including emergency generators, security lighting, and battery backup systems
- Type of records maintained, the record-keeping responsibilities of each organization, and the locations where records are stored
- Performance of trend analyses on maintenance requests to identify aging or problematic equipment or equipment types.

Performance Tests

All performance tests cited in the appendices may be relevant to assessment of the testing and maintenance subtopic.

Data Collection Activities

Organizational Considerations

A. Inspectors should identify the method of communicating requests for testing or maintenance from one department to another to determine whether the method is timely and responsive. A reasonable approach is to select several completed work requests and track their progress through the system. Inspectors should ask such questions as who originated the request, how and when the request got to the maintenance department, how it was scheduled, and who verified that the work was accomplished.

B. Inspectors should determine the role of vendors or outside companies in the maintenance and repair of security-related components, especially central processing units or other complex equipment. It is important that formal procedures be in place for tests, maintenance, calibrations, troubleshooting, and repairs. Typically, quality assurance (QA) features are in place to ensure that maintenance is performed properly and security concerns are covered, such as the two-person rule being enforced during tests or maintenance. Normally, an organization is tasked to conduct independent audits to ensure compliance with site-specific and DOE requirements. Inspectors should examine these audit results to determine whether they are comprehensive and what action is taken when deficiencies are found.

C. At facilities with Category I or II SNM or vital equipment, inspectors should review the DOE-approved security plans to determine the site-specific requirements for tests and maintenance. Document review and interviews should reveal whether these requirements are being met and, if not, the reasons for non-compliance.

D. At facilities with classified matter in LAs (or other security areas), inspectors should review the DOE-approved security plans to determine whether site-specific requirements for testing and maintenance of alarm systems are followed, and whether compensatory measures are used when security-related subsystems or components are not in service.

Procedures and Operations

E. Typically, inspectors should review test, maintenance, calibration, and repair procedures to determine whether:

- Procedures are clear and complete.
- They have been reviewed and approved.
- Appropriate test tools are used.
- All organizations have procedures specific to their duties (for example protective force and security technicians).

F. Inspectors should observe facility technicians conducting tests, maintenance, calibrations, and repairs to determine whether site personnel have and use the procedures consistent with site policies. These observations may be accomplished separately or in conjunction with performance tests.

G. Inspectors should review reports developed as part of the QA program. These may include audits, assessments, and independent reviews. The type and extent of the QA program should be determined, and inspectors should note how the facility resolves findings, issues, or deficiencies noted during QA reviews. Occasionally, the resolution process fails to adequately correct problems and results in a superficial treatment rather than an in-depth remedy.

H. Inspectors should determine whether testing and maintenance are performed in a timely manner. Testing or maintenance that is not performed or is performed late (e.g., equipment awaits repair for an extended period) may indicate inadequate staff or lack of management attention. Testing and maintenance should also be reviewed to determine whether security managers can direct and prioritize the activities of test and maintenance personnel (for example, whether they are dedicated to the security department or take their direction from other departments, such as facility engineering). If security technicians do not report directly to security managers, inspectors should determine how the security managers control and prioritize activities—in particular, how items that need immediate attention are handled.

Training and Qualification

I. Inspectors should review the training and qualifications of security technicians by reviewing resumes and records of formal training and determining how in-house training is handled.

Equipment Performance

J. Inspectors should examine performance test results to evaluate equipment performance, which is the best indicator of the quality of the testing and maintenance program. If equipment performs well during performance testing, it is a good indication that the testing and maintenance program is adequate.

Records Review

K. Inspectors should review records of tests, scheduled maintenance, and calibration to verify that these activities are conducted as scheduled and that records are maintained as required. Typically, inspectors review records of three or four components (for example, perimeter sensors, metal detectors, and SNM detectors). If more than one organization has a major role in the testing and maintenance program, inspectors should review selected records of each organization to ensure that all such records are in order. One way to facilitate the record review is to select a specific time frame and review the records of the tests and maintenance conducted during that period. The time frame selected should include six to eight test periods. For example, if a component is tested weekly, a period of two months is appropriate, and if a component is tested monthly, a period of six months may be necessary. During the record review, inspectors should determine whether:

- Tests are conducted as scheduled.
- Maintenance and calibrations are conducted as scheduled.
- Records are complete.
- Documentation is legible and consistent with site-specific procedures and requirements.
- Deficiencies noted during tests or maintenance are promptly reported and appropriate action is initiated (that is, compensatory measures or work orders). Often, inspectors can verify that maintenance action was initiated by listing deficiencies and dates noted on test records, then checking maintenance logs or work order requests to verify that action was taken and to determine time frames for corrective actions. Iinspectors can also verify that compensatory measures were initiated as required by checking the protective force supervisor's or CAS operator's logs.

L. Inspectors should review records of equipment repair, replacement, and corrective maintenance. One way of conducting this review is to select a sample of repair records and trace the documentation back to the initial report of failure (or vice versa). This process typically involves reviewing records of:

- Equipment failures reported by SPOs or other organizations
- Tests that indicate deficiencies requiring maintenance
- Communication of either of the above items to a supervisor or other person who develops a maintenance request
- Assignment of maintenance responsibility (work order) and dates that work was initiated
- Dates that work was completed and names of personnel accomplishing task
- Verification that work was completed and closeout tests were conducted.

With this process, inspectors can determine:

- Whether records are complete
- Time frames for initiating and completing repair
- Whether documentation is complete
- Whether site-specific policies and procedures are followed. (For example, if a two-person rule is in effect, were two qualified individuals assigned to the task?)

This page intentionally left blank.

Section 8

SUPPORT SYSTEMS

Contents

General Information

Although not an independent subtopic of the PSS topic, support systems include a number of interrelated subjects of interest to inspectors examining this topic. Support systems are normally inspected along with the traditional subtopics, but they merit separate discussion to ensure that they are adequately addressed during the inspection process. Support systems include power supplies, tamper protection, and regulatory warning signs.

For the purposes of security systems, auxiliary power is defined as a backup power system (battery and/or engine-driven system) that provides emergency electrical power to security systems when normal power is lost. In the event that the primary power source fails, DOE requires that transfer to auxiliary power must be automatic without affecting the security system or device being protected. Both the CAS and the SAS must receive an alarm indicating failure of any power source and transfer to auxiliary power. Auxiliary power supply configurations vary widely throughout the DOE complex depending upon the system, the equipment, and the manufacturer.

The reason for evaluating auxiliary power supplies is to determine whether they are adequate to power all alarm systems and critical equipment long enough to permit restoration of normal power.

Batteries are also a means of auxiliary power, and a number of provisions are related to their use. When rechargeable batteries are used, they should be kept fully charged or subject to automatic recharging whenever the voltage drops to a specified level. Non-rechargeable batteries should be replaced whenever their voltage drops 20 percent below the rated voltage. An alarm signal should be activated to indicate this condition.

There are various methods for preventing and detecting attempts to tamper with security systems. Tamper protection is covered in detail in Appendix A, which provides information on testing the components that are used to indicate that detection devices or transmission lines to annunciators have failed or been tampered with. If operational or process control information (for example, low rates, pressure readings, or airborne radiation levels) is relied on for security purposes, these systems should be checked for tamper resistance.

Tamper and line supervision tests are usually conducted in conjunction with related tests of CCTV equipment and the intrusion detection and access control systems to increase the efficiency of data gathering.

The posting of signs listing regulations and penalties is provided for by the Atomic Energy Act of 1954. Typically, these signs list prohibited activities, such as unauthorized entry onto DOE property, and the fines or imprisonment that violators may receive if convicted. Signs are normally posted at entrances and at intervals along the perimeter of the property. Signs posted

at entrances normally list prohibited articles, such as firearms, explosives, privately owned recording and electronic equipment, cellular telephones, computers, and controlled substances. Notification of the date of posting, relocation, or removal of posting, or other changes should be furnished to the local office of the Federal Bureau of Investigation (FBI) exercising investigative responsibility over the property.

Common Deficiencies/ Potential Concerns

Often, supporting devices associated with auxiliary power sources are not afforded adequate tamper protection. These may include:

- Batteries
- Inverters
- Power switches
- Fuel supplies.

When one or more of these items are disabled, the auxiliary power source may be effectively neutralized. For example, a fuel tank may furnish fuel to a generator that is the primary backup power source for a particular security system. If the fuel tank is contaminated or destroyed, the backup power source is effectively eliminated, even though the generator itself may be adequately protected.

Since batteries can be hazardous (battery acid can burn or be extremely corrosive, and batteries do occasionally explode), routine servicing and testing are important. Sometimes, inspectors will find batteries left unattended and in poor condition. Some associated problems can be identified early in the inspection by checking testing and maintenance procedures.

The most significant concern in the area of tamper protection is the frequent failure by DOE facilities to provide complete tamper indication and line supervision for all security system elements and devices requiring protection. Tamper devices may include magnetic switches, plungers, and closure contacts. These devices should be inaccessible, located inside a protected space, or otherwise protected.

Frequently, line supervision fails to include the entire circuit to be protected (that is, the sensor itself, local wiring to a control device, the transmission medium, and the final signal processing annunciation equipment). In this case, the destruction or failure of the unprotected component could result in the failure of the whole system.

In some cases, multiple tamper devices are included on a single alarm circuit to reduce wiring and signal processing requirements. This can be a significant weakness since the actual type and location of the alarm, and the number of affected devices, may not be apparent from the information displayed at the alarm console.

Planning Activities

Inspectors review documentation and interview facility representatives to gather information on auxiliary systems, including power supplies and tamper alarms. If vital or security-related equipment relies on cooling water (for example, reactor coolant pumps) or fuel supplies (for example, engine generators), inspectors should determine methods used by the facility to ensure the reliability of such systems.

Performance Tests

All performance tests cited in the appendices may be relevant to assessment of support systems, especially those pertaining to auxiliary power supplies and tamper alarms (Appendix A).

Data Collection Activities

Power Supplies

A. Inspectors should interview security staff and review documents to determine:

- What security-related components are supplied auxiliary power by batteries, a UPS, or other means
- How long the UPS can maintain operation at full load, and procedures for load shedding
- Number and location of diesel generators
- Security-related components that are supplied auxiliary power by engine generators

- How long diesel generators can maintain load until the fuel supply is exhausted
- Frequency and methods of testing and maintaining diesel generators (for example, full load tests, test of switching devices)
- Frequency and methods of testing and maintaining system batteries or the UPS
- Frequency and methods of testing and maintaining batteries that power individual components (for example, sensors)
- Replacement frequency for non-rechargeable batteries
- Indications received in CAS/SAS when normal or auxiliary power fails
- Source of offsite electric power, including number of feeds
- How the systems are tested (are they turned on, brought up to speed, and load-switched, or does the test actually simulate power loss?).

B. Inspectors should tour areas where components critical to providing auxiliary power are located and verify information gathered during document reviews and interviews. Items of interest include fuel supply reservoirs, switching equipment, batteries, and power-generating equipment. All of these elements should be given adequate physical protection, including tamper protection and shielding from inclement weather. For example, the switching equipment for the commercial-to-auxiliary power transfer should not be installed on the outside of a security area where access is unrestricted and tampering could go undetected.

Tamper Protection

C. Inspectors should review the methods in place to prevent and detect attempts to tamper with security-related systems, including the use and inspection frequency of tamper-resistant hardware and tamper-indicating devices (TIDs). Also, inspectors should review the general installation techniques for security sensors (that is, the use of epoxy over screws or bolts, security seals, or deformation of threads on attachment hardware). If operational or process information is used for security purposes, this equipment should have many of the same physical protection features as security equipment. The use of TIDs and security hardware should also be reviewed, including the level of confidence or response placed on this type of alarm (that is, does the protective force initiate a full-blown response or is an SPO dispatched to investigate the alarm?).

Signs

D. Inspectors should determine whether the required signs are appropriately placed and in good repair as required by the DOE orders and site security plans. Signs should include, at a minimum:

- Atomic Energy Commission
- Prohibited articles
- Limited Area
- Vehicle and personal searches
- Surveillance in use.

This page intentionally left blank.

Section 9

SYSTEMS MANAGEMENT

Contents

General Information

Like support systems, systems management is not considered an independent subtopic of the PSS topic. Nevertheless, systems management is important and merits separate discussion to ensure that sufficient management planning, direction, and control processes are established and are adequately addressed during the inspection.

Management has the responsibility to ensure that security interests are adequately protected and that the levels of protection for particular interests are provided in a graded fashion in accordance with potential risks. 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 physical protection
- Developing and implementing procedures and policies, considering site-specific conditions, that fulfill DOE requirements
- Providing adequate resources to include 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.

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 commit limited/ competing resources or to implement physical security measures that are inconvenient or that would impact production. While some reluctance is understandable, minimum protection requirements must be met. An appropriate balance between security, operations, and production must be attained. Without the support of senior managers, the security organization may not have the assets necessary to operate effectively and thus may be unable to maintain adequate protection levels. It is incumbent on senior managers and personnel responsible for oversight activities to assure that a lack of management support does not adversely impact the effectiveness of security programs.

Lack of a Suitable Organizational Structure. Occasionally, inspectors encounter an organizational structure where the person or group responsible for policy and procedures is not positioned high enough in the organization to

ensure compliance. This problem most often occurs when one organizational element is responsible for policy development, while personnel responsible for implementation work for different elements. The situation gets worse when the management element common to the two groups is at too high an organizational level to deal with day-to-day issues effectively. Similarly, inspectors may encounter situations where the security organization has little control or influence over engineering and/or maintenance personnel responsible for PSS design or functioning. In such cases, the operations and production managers to whom these personnel report may place a low priority on security issues and, in extreme cases, simply ignore the security organization's needs.

Responsibilities Not Specifically Assigned. Frequently, facilities fail to document the organizations and persons responsible for PSS operations. Less commonly, they may simply fail to assign responsibility for some aspects of the operations. Not documenting responsibilities assignments inevitably results in some operational functions "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 organization.

Inadequate Staffing. Some facilities simply do not have enough staff to support PSS requirements. A related problem occurs when a facility's manager cannot effectively manage the program, either because there are too many people to supervise (excessive span of control), or because the manager has other duties that deflects attention from physical protection responsibilities. In some cases, the site may have adequate numbers of staff, but may have a non-optimal skill mix, resulting in shortages in certain areas and/or delays in performing certain functions.

Personnel Competence and Training

Inadequate Training. Many PSS-related deficiencies found in DOE are attributable to inadequate training. Some organizations do not provide any formal training, relying instead on an unstructured form of on-the-job training. They expect persons with security responsibilities to learn from other, more experienced individuals. Often, however, the experienced individuals themselves lack adequate training, so improper practices continue. In some cases, organizations make attempts at training, but develop and administer it using individuals unfamiliar with proper training techniques. This practice also results in inadequately trained persons performing key duties. Few organizations evaluate the competency of individuals with security 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. If a training program exists, inspectors should focus on reviewing its effectiveness. If no training program exists, inspectors should devote additional attention to activities designed to determine the knowledge level of individuals who perform security functions (for example, interviews or knowledge tests).

Comprehensive Requirements

Inadequate Planning. Frequently, during physical security planning, management does not give adequate consideration to, or overlooks, potential threats and/or adversary approaches that may be regarded as unconventional. As a result, concerns that would otherwise be identified are often not adequately dealt with and are not addressed in the appropriate planning documents (for example, the SSSP and supporting VAs for Category I SNM facilities). During planning, it is important that managers consider the impact of such adversary approaches as non-traditional ingress points (e.g., airborne intrusion) and thoroughly review the consequences of insider activity, with emphasis on the potential for single-point failures.

Inadequate Implementation of Requirements. More often than not, facilities develop policies and procedures that provide adequate guidance and direction for the protection of identified security interests. However, inadequate implementation of the requirements delineated in those documents frequently results in protection levels that are less than intended. The impact of

inadequate requirements implementation is more crucial in some areas than in others. For example, deviations from protection policies involving the protection of high-value non-classified equipment are less important than those involving SNM. Areas where inadequate implementation is common and where resultant impacts can be significant include material surveillance, SNM transfers, emergency operations, protective force operations, and alarm response.

Feedback and Improvement

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

Inadequate Corrective Action Plans. Inadequacies in corrective action plans are fairly common and potentially serious, and they can result in deficiencies not being corrected. Organizations often do not:

- Analyze root causes and cost effectiveness and, on that basis, prioritize deficiencies so that resources can be used to correct the most serious problems first.
- Establish a corrective action schedule with milestones so that progress can be monitored and slippages identified early.
- Assign responsibility for completion to specific organizations and individuals.
- Continually update the plan as known deficiencies are corrected and new ones are identified.
- Ensure that adequate resources are applied to correcting deficiencies.

Frequently, facility managers devote their resources to correcting the most recently identified deficiency instead of the most serious, and habitually correcting the 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. Tracking system problems can result in deficiencies not being corrected in a timely manner, or not being corrected at all. The two most common problems found in tracking systems are incompleteness and inaccuracy. Often, the system is incomplete because supervisors or operators fail to list all deficiencies. They are inaccurate when corrective actions are shown as complete when they are not, or when corrective actions have not adequately dealt with the problem. Occasionally, inappropriate corrective action based on inaccurate tracking data creates new problems.

No Root Cause Analysis of Deficiencies. Another potentially serious management deficiency is the failure of organizations to determine the underlying cause of deficiencies. Insufficient root cause analysis usually results in recurrence of the same deficiencies because corrective actions address only the surface problem or symptom rather than the root cause. If performed correctly, root cause analysis may reveal the causes of errors (e.g., ambiguous procedures or insufficient training). Unless management accurately determines the root cause of identified deficiencies, it is likely that similar deficiencies will recur.

Planning Activities

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

- Determine the 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.

- Review organizational charts and identify the names of all persons with PSS supervisory and management authority.
- Determine how PSS policy and procedures are promulgated and distributed.
- Determine how the self-assessment program functions, including:
  - Frequency of self-assessments
  - Who has overall authority for the program
  - Who actually performs the self-assessments.
- Focus on determining whether the self-assessment program provides independent oversight of PSS or whether it is conducted by the same persons who operate the programs being assessed.

Once inspectors understand the structure of the program, they should determine which organizations and program elements will be reviewed in more depth during the inspection, and which individuals will be interviewed. At large facilities, it is not practical to inspect all systems in the same depth or to interview all individuals who perform systems-related duties. In such cases, a representative sample may be selected for evaluation. For reasons of efficiency, the review of systems management is normally performed by inspectors who are also inspecting other PSS subtopics. Consequently, the inspection team should consider a variety of factors when selecting organizations to review. It is usually advisable to interview first-line managers with responsibility for the systems that are selected for performance tests; this ensures that the impact of any deficiencies identified during the reviews can be covered with managers during the management interviews. In addition, the information gathered during the first few days of the inspection often influences the selection of managers to be interviewed. As program strengths and weaknesses are noted, the inspectors should modify their planned activities appropriately.

Inspectors review basic documentation and interview facility security and protective force representatives to determine how the protective force implements security-related procedures. Areas to review include:

- Patrols
- Repository checks
- Alarm responses
- SNM transfers
- Emergency response
- Training.

Such reviews should be closely coordinated with the protective force topic team. The PSS team normally focuses on the protective force interface with security systems and does not attempt to evaluate the tactical capabilities of the protective force (for example, weapons-related skills or the ability to use cover and concealment).

Data Collection Activities

Line Management Responsibility for Safeguards and Security

A. Inspectors should review the applicable planning documents that cover PSS (for example, SSSPs or other planning documents). Particular attention should be devoted to determining:

- Whether the planning documents are current
- Whether they appropriately identify
  - Goals
  - Objectives
  - Responsibilities
  - Overall policies for all aspects of physical security systems
- Whether they address all applicable security interests.

B. Inspectors should identify any special conditions or unique features of the site that are covered by exceptions or alternative approaches to determine whether the facility has documented the justification for the exceptions.

C. Inspectors should interview security managers, including design and testing/maintenance supervisors, and review

resource plans and budget documents. Elements to cover include:

- Whether goals and objectives are clearly defined
- Whether needs identified in the corrective action plan and strategic plan (if one exists) are reflected in budget documents
- How the PSS budgeting process functions
- Whether staffing plans are consistent with budget requests.

D. Inspectors should determine whether the organizational structure facilitates efficient communication and positive working relationships between the various organizational elements, and between persons who deal with PSSs. The functional relationships between the various organizational elements should be clearly defined, formally documented, communicated, and understood by all persons. One method useful for investigating the adequacy of the communications and interactions between organizational elements is to determine how the organizations interact with one another (for example, protective force and MC&A) when facility conditions change (for example, during material transfers between security areas).

E. Inspectors should determine whether the persons responsible for PSS are in a position to ensure compliance. This may involve reviewing the facility's policies and procedures to determine whether the safeguards and security manager has the authority to enforce compliance and resolve issues identified during self-assessments or other similar activities.

F. Inspectors should interview managers in the security department and operations and production departments to determine whether the security organization has any problems getting operations or production personnel to implement required procedures. If initial interviews indicate questions about the operations or production organization's commitment to implementing required security measures, inspectors may elect to conduct more detailed interviews (e.g., with individual vice managers) and document reviews to determine whether problems exist. This detailed review may involve examining findings identified in self-assessments, surveys, and inspections to determine whether corrective actions were implemented in a timely manner, or whether repeated memoranda from the security organization are necessary before operations or production personnel take 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").

G. Inspectors should determine how management communicates its goals and objectives and stresses the importance of PSS. Inspectors should determine what incentives are used to encourage good performance.

Personnel Competence and Training

H. Inspectors may elect to review a sample of position descriptions for specific individuals who have responsibilities for PSS to verify that responsibilities are actually reflected at the individual's level. Inspectors can also review individual position descriptions and performance goals of technicians or other persons in the operations and production departments who conduct performance tests or perform maintenance functions to determine whether they are held accountable for their performance and whether good performance in PSS-related areas is specified in these documents.

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

J. Inspectors should review training plans, course materials, and training needs analyses. Interviews with security staff, operations/production supervisors, and custodians should be conducted. Inspectors should observe

training classes that address any aspect of security-related functions, such as:

- SPOs
- Custodians
- Operators
- Health physics staff
- Other personnel who perform security-related functions.

Training reviews indicate whether operations and field personnel understand the security concerns underlying their operations (not only the security practice, but the reason for the practice). For example, the SPO responsible for monitoring a metal detector may have been given orders that all incoming personnel must clear the metal detector, but no orders regarding outgoing personnel. If the SPO does not fully understand the purpose of the metal detector (to prohibit the introduction of weapons and contraband and to prevent removal of SNM or DOE property), the SPO may fail to ensure that outgoing personnel clear the metal detector.

K. Inspectors should review training records and test scores and interview personnel who have received training to verify that training has been conducted as scheduled and that personnel have attended courses as required. During interviews, inspectors should ask facility personnel questions taken from facility tests as a means of determining the effectiveness of the training program. Inspectors may also ask personnel to perform the functions for which they have been trained (for example, test an alarm sensor, apply a TID, operate a handheld SNM detector). In this manner, inspectors can observe each individual's knowledge and skills and verify the training program effectiveness.

Comprehensive Requirements

L. Planning – Airborne Protection. Inspectors should review the SSSP to determine whether airborne assault is considered in the site-specific threat. Document reviews and interviews should reveal whether an airborne threat is appropriate for the site (for example, if the only security interest at the site is a single piece of SNM weighing two tons buried in a solid piece of concrete 15 feet thick, the airborne threat may not be applicable). However, if the security interests are more attractive (smaller, more valuable, and more vulnerable), the inspection team should evaluate all airborne denial barriers and detection equipment.

If an airborne threat is credible, inspectors should review documents and interview security staff to determine the level of protection against airborne intruders. Items to check include whether:

- The airborne threat is addressed in the SSSP.
- Helicopter barriers (for example, poles and rope systems) have been installed to protect priority targets.
- An electronic detection system is used (for example, acoustic detectors or radar). If so, the methods for testing effectiveness should be reviewed.
- Other means of detecting airborne intrusion are available (for example, patrols, orSPOs in exterior posts).

Inspectors should also tour areas to determine the degree of protection against airborne threats. Items to note include:

- Potential landing sites that could be used by helicopters, gliders, parachutists, or fixed-wing aircraft
- Factors affecting thelikelihood of detecting airborne intrusion, such as:
  - The size of the area
  - Visual detection capability from guard posts
  - Frequency of patrols
  - General level of activity in the area
- Effectiveness of any aircraft denial barriers, including susceptibility to defeat by covert means.

M. Planning – Insider Analysis. Inspectors should determine the vulnerability of high-security facilities (for example, those with

Category I SNM or vital equipment) to possible compromise by insiders, including:

- SPOs
- CAS operators
- Custodians
- Operators
- Supervisors
- Security technicians
- Maintenance personnel
- Health physics technicians
- Emergency response personnel (for example, firefighters).

Vulnerability to insiders can be determined by reviewing VAs, interviewing personnel in various job categories, and systematically examining the job duties, responsibilities, and "privileges" of personnel in selected job categories (for example, possession of master keys, access to safe combinations, capability to place alarm systems in access mode). Inspectors should pay particular attention to personnel who have access to SNM and who have numerous responsibilities (for example, material custodians who also test alarms, have safe combinations, and enter information into accountability systems). Inspectors should also look for possible single-point failures (for example, areas where the entire safeguards system would be ineffective if one element were to fail) and determine whether the elements possibly involved in such failures are vulnerable to insider sabotage.

N. Requirements Implementation – Material Surveillance Procedures. Inspectors should conduct the following activities:

- Review such documents such as the MC&A plan, operating procedures, and the SSSP.
- Interview security staff, material custodians, operators, and other personnel who use or process SNM.
- Tour process areas to determine what methods are used to provide surveillance of material that is not in secure storage.

Material surveillance of SNM must be maintained within use and process areas. A two-person rule is a common method of implementing material surveillance at Category I or II areas. Custodial and administrative controls are generally used in Category III or IV areas.

The inspection team should pay particular attention to the means of providing material surveillance for SNM that is kept in process storage or staging areas. Inspectors should ensure that all practices are consistent with MC&A plan provisions and are effectively implemented.

The effectiveness of the two-person rule should be determined by reviewing and observing procedures. Inspectors should verify that procedures are developed for all areas and distributed to all personnel who must implement them. The procedures should clearly specify what is required (for example, constant visual contact, two persons in same room, or two persons in same vault). The means of enforcement of a two-person rule at MAAs or vault entrances can also be reviewed. Card-reader systems, SPO procedures, and double-lock systems are common methods for enforcing a two-person rule. In some areas, inspectors may also review access logs to determine whether the two-person rule is implemented as required. Inspectors should attempt to observe implementation of the two-person rule and interview material handlers or custodians to determine whether they understand and implement the requirements correctly. The PSS team's evaluation of the aforementioned activities should be closely coordinated with the MC&A team as reflected in Section 10.

O. Requirements Implementation – SNM Transfer Procedures. Inspectors should identify:

- The SNM transfer paths, including offsite shipping and receiving and intrasite transfers, and the category and classification of SNM transfers
- Specific portals used for SNM transfers and the controls implemented at those portals by the operations, production, and health physics

staffs, and by the material custodians and the protective force

- Escort procedures, including the number of armed SPOs who accompany Category I shipments
- Vehicles used for shipments, including special security features of vehicles (for example, remote-disable capability, hardened vehicle, locked storage, delay features)
- Methods implemented to assure that SNM is not secreted in non-SNM transfers and/or radioactive waste shipments.

Inspectors should observe SNM transfers to determine protection effectiveness and verify information collected during interviews and document reviews. Procedures at the shipping portal and/or receiving portal should be observed, as well as the transfer route.

Once the inspectors have an operational understanding of the transfer procedures, they should evaluate the procedures for vulnerabilities or weaknesses. One method is "what if" approach: for example, What if the vehicle driver is the insider? Are there procedures that will prevent the driver from driving away with the material?.

P. Requirements Implementation – Emergency Procedures. Inspectors should conduct the following activities:

- Review documents, such as SSSPs, standard operating procedures, emergency plans, post orders, and other documents.
- Interview security managers, protective force supervisors, custodians, and operations/production supervisors.
- Tour use and process areas to identify the methods used to ensure the security of SNM during and following an emergency, including:
  - Evacuation alarms
  - Fire alarms
  - Criticality alarms
  - Medical emergencies
  - Radiation alarms
  - Toxic chemical situations.
- Review requirements and conditions for post-evacuation SNM inventories.
- Identify the methods used to control evacuation, including:
  - SPO response
  - Pre-planned evacuation routes with barriers
  - Post-evacuation personnel accounting
  - Post-evacuation patrols and searches.
- Review relevant procedures, such as protective force procedures (including response plans), custodial procedures, operations/production procedures, and health physics procedures.

Inspectors should verify information about emergency evacuations by observing facility tests or reviewing results of after-action reports (incident reports). For example, if evacuations have occurred, inspectors can usually review incident reports and verify that an inventory was performed as required by site-specific procedures.

Q. Requirements Implementation – Protective Force. Inspectors should interview security staff and protective force supervisors and review security plans and post orders to determine:

- Frequency of patrols of selected areas
- Duties and responsibilities (for example, check locks, check repositories, detect intrusion)
- Documentation of patrols (for example, logs and punch clocks)
- Requirements for repository checks.

Inspectors should review logs on classified repositories to verify that SPOs sign/initial logs as required by site-specific policy.

Inspectors on the PSS team need to know whether facility procedures include support by the protective force to adequately protect DOE assets according to facility plans and accepted risks.

These patrols are normally a part of the security posture agreed to or directed by DOE. The PSS team's evaluation of the aforementioned activities should be closely coordinated with the protective force team as reflected in Section 10.

R. Requirements Implementation – Alarm Response. Inspectors should interview security staff and protective force supervisors and should review security plans and post orders to determine:

- Alarm response plans
- Alarm priorities
- Response times
- Number of responders
- Response actions for various alarms and conditions, including:
  - Exterior intrusion alarms
  - Interior intrusion alarms
  - Tamper or line supervision alarms
  - Duress alarms
  - SNM monitor alarms
  - Evacuation alarms
  - Emergency response (for example, fire)
  - Visual sighting of intruder
- Methods for assessing, recording, and documenting alarms and/or response actions
- Tests conducted by the facility to verify response times or effectiveness.

Inspectors should review logs and/or incident reports to verify response times and actions. Such logs are usually maintained by the CAS and the protective force supervisors.

Inspectors should observe response procedures during routine activities or during facility tests and verify appropriate response actions.

Inspectors should validate the alarm response times to assure that the VA models accurately reflect the required delay times and security responses, and that security interests are adequately protected.

Feedback and Improvement

S. Most organizations have some type of central, integrated system to identify and follow the status of deficiencies identified during self-assessments, site office surveys, and inspections. Inspectors should determine what system or systems are being used. Some sites have a comprehensive system that includes all safeguards and security-related deficiencies, while at others, each area, including physical security, has a separate tracking system. Self-assessment programs are the key to effective management oversight.

T. Inspectors should review the self-assessment program in detail to determine whether self-assessments are performed regularly and whether they review all aspects of the physical security program. Selected self-assessment reports should be reviewed to determine whether root causes are identified when deficiencies are found. It is helpful to compare the results of facility self-assessments to inspection findings or other audit results to learn whether the self-assessments are equally effective.

U. Inspectors should determine who actually performs self-assessments. At the site office, this may be the security survey staff as they perform the annual survey. If the persons who actually perform physical security functions conduct the self-assessments, there should be some form of independent verification or evaluation of the results. Inspectors should determine whether deficiencies identified during self-assessments are entered into a tracking system, and how corrective actions are selected and carried out.

V. Inspectors should determine whether an organization has a tracking system and how it operates. In conjunction with the protection program management (PPM) topic team, they should determine whether the tracking systems have a means of monitoring the status of all inspections, surveys, self-assessments, and other similar activities. Also, inspectors should determine whether there is a formal system for independently verifying that corrective actions have been completed and that the original

problem has been resolved effectively. Inspectors may elect to select a sample of physical security deficiencies from several sources and determine whether they were entered into the tracking system. Finally, they can select a sample of deficiencies indicated as closed to verify that they have in fact been adequately corrected.

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

X. Inspectors should review the role of DOE oversight by interviewing selected DOE security or survey managers to determine how DOE implements its responsibilities. Specific items to cover include how DOE reviews contractor physical security program functions during 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 on the same subjects.

Section 10

INTERFACES

Contents

Introduction

Integration is the coordination and cooperation among inspection team members designed to achieve a more effective and organized inspection effort. It creates a synergism that results in an enhanced knowledge of the inspected site, a strengthening of inspection techniques, and a more comprehensive inspection report. The integration effort significantly contributes to the effectiveness of the HS-61 inspection process and, along with other unique attributes, enhances HS-61's ability to provide an accurate, in-depth evaluation of protection programs throughout the DOE complex.

Because of the interdependency of elements of any security system, integration must continue throughout all phases of the inspection to ensure that all pertinent data has been shared. Integration, facilitated by one or more integration teams, is realized by exchanging information and discussing how information collected by one topic team influences the performance of security system elements observed by other topic teams. The fundamental goal of this effort is to ensure that potential systemic vulnerabilities are clearly identified and analyzed.

In addition to enhancing inspection results, integration has several other major benefits. First, it allows topic teams to align their efforts so that their activities complement rather than detract from one another. It is usually less productive to inspect PSSs at one location, classified matter protection and control (CMPC) at a different location, and the protective force at yet another location. Using this approach, inspectors would accumulate a collection of unrelated facts. Therefore, topic teams must cooperate to make the best choices regarding what should be inspected at which locations. Early and continuing integration helps ensure that the activities of all topic teams are unified and contribute to the overall goal.

A second benefit of integration is that it allows topic teams to benefit from the knowledge, experience, and efforts of other topic teams. Sometimes, ideas developed by one topic team can help another topic team focus inspection activities in a more productive and meaningful direction. For example, the PSS topic team may indicate that its planning effort led to the conclusion that the physical systems at a particular location are weak, resulting in heavy reliance on the protective force. It may therefore

be useful for the protective force topic team to plan to focus on assessing protective force capabilities as they relate to this weakness, in addition to their independently determined areas.

The third benefit of integration is to prevent topic teams from interfering with each other. Often, several topic teams concentrate their activities at the same location, resulting in multiple visits over time or a number of visits at the same time. This causes undue disruption of the facility being inspected. Integration among topic teams can preclude this problem by having one or two topic teams visit a particular location and collect the data for several. All topic teams should be aware of what all other topic teams are doing, where they are doing it, and how it will affect their own activities.

Integration of data collection activities for performance testing is imperative. For example, if the PSS topic team schedules a performance test that results in the activation of the alarm system in a building, and the MC&A topic team schedules a performance test involving an emergency inventory or transfer of material in the same building at the same time, the resulting problem is obvious.

Integration by the Physical Security Systems Topic Team

As an integral part of the overall protection program at any DOE facility, PSS interacts with all other elements of that program. Therefore, the topic cannot be inspected in isolation. Inspection team members must continually keep this in mind in order to determine how well this interaction works. As noted, this requires integration with topic teams responsible for other inspection areas. Information developed by these teams may affect how the results of the PSS team efforts are viewed. Similarly, data gathered by the PSS team may have some bearing on how the results of another team's efforts are viewed.

Figure 3, on the next page, shows the common areas of interface for the PSS topic with other topics.

Protection Program Management

The PSS topic team must consider elements of PPM, as they are mutually supportive. Evaluating the consistency of descriptions contained in the SSSP with the actual system or procedural configurations involves mutual validation between the PPM and PSS topics. Another area of mutual support is the implementation of the DOE ISSM program at a facility and how it supports physical security systems, maintenance, personnel, and management's attention to the resources needed for a successful program.

Classified Matter Protection and Control

The CMPC topic relates to PSS because of requirements for protecting classified information and material. Some areas of interest common to PSS and CMPC are:

- Control and storage of documents
- Physical control of classified parts
- Establishment of security areas for classified information processing, including secure communications centers
- Alarm log printouts, alarm system drawings, and compensatory plans.
- Protective force patrols (also reviewed by the protective force team)
- Badge and pass systems.

Personnel Security

Elements of personnel security must be considered by the PSS topic team when the site places high reliance on the adequacy of the personnel security programs. Implementation of human reliability or personnel security assurance

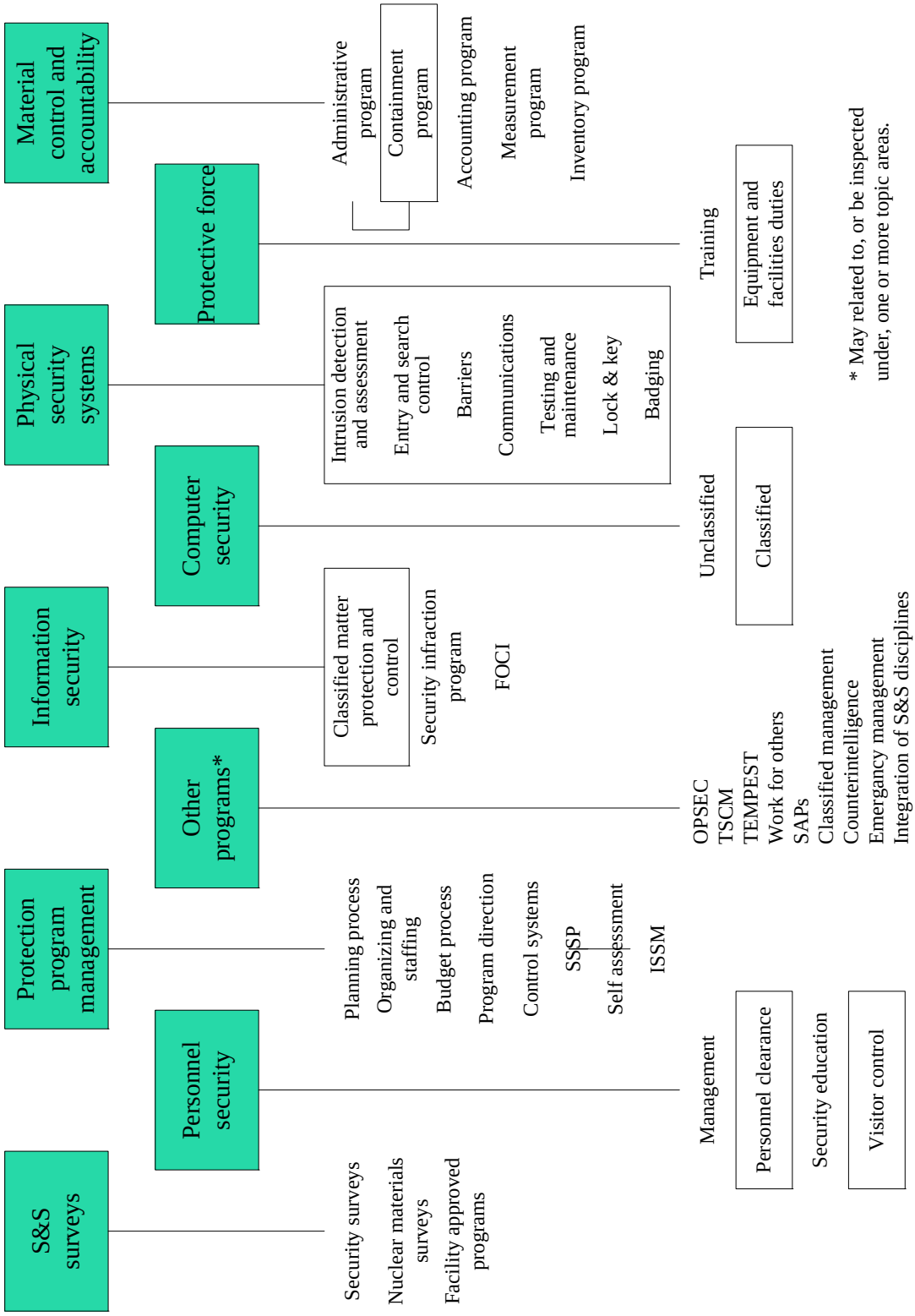

Figure 3. Area of interface most common to physical security systems topic team

programs may directly affect the overall PSS program. Also, PSS may interface with personnel security in the areas of visitor control and escort procedures. Personnel security systems that interface with the PSS should be afforded the same level of protection as the systems they interface with.

Material Control and Accountability

The interface between the inspection of PSS and MC&A is important to ensure that findings are reported in the appropriate topic are and that both inspection teams are aware of potential problem areas impacting their individual conclusions.

DOE orders require that MC&A procedures be compatible with the physical protection and security of the system.

The PSS and MC&A topics overlap in a number of areas, including:

- Surveillance of SNM
- Access controls and records
- MAAs
- Portal monitors
- Material transfers
- Storage of materials
- Detection of unauthorized activity or conditions.

If both topics are inspected at the same facility, any findings involving areas of overlap should be coordinated between the MC&A and PSS topic teams to ensure that findings are reported under the most appropriate topic.

Typical findings of mutual interest include:

- Access controls that do not meet DOE requirements
- Deficiencies in barriers that could allow an insider to divert material out of a security area without detection
- Deficiencies in the intrusion detection system protecting SNM storage repositories or security area perimeters
- Deficiencies in locks, key control, or combination controls that could allow an insider to gain unauthorized access to SNM
- Portal monitor capabilities that are ineffective or inconsistent with the type of material in the MAA
- Inadequate implementation of procedures, such as the two-person rule or vault closing/operating procedures
- Category I quantities of SNM stored outside a vault or vault-type room.

The interface with the MC&A topic team frequently results in identifying locations of special concern due to the category or attractiveness of material in process or storage. This information can significantly redirect the focus of the PSS inspection. For example, if a significant quantity of SNM is identified as being outside the MAA during inspection planning, it may initially be considered a major problem. However, subsequent coordination between the MC&A and PSS teams may reveal that there is no problem due to the condition of the material and the storage method. In this case, both teams can refocus their attention and inspection activities.

Protective Force

Interface with the protective force topic team is very important in performance testing. In addition, the subtopic of badges, passes, and credentials is of interest to a variety of HS-61 inspection teams (typically, personnel security, CMPC, and protective force). Although the PSS team reviews the badge system, the personnel security, protective force, and CMPC topic teams must be kept informed of results, because they

may also review some aspects of the badge system. For example, the personnel security team may review the procedures for issuing badges, and the protective force topic team often observes badge-checking procedures at portals. Performance tests conducted by protective force inspectors also have a bearing on any conclusion drawn by PSS inspectors. Consequently, all of these topic teams must coordinate their efforts both to assure full coverage and to avoid duplication of effort.

The PSS team can increase the efficiency of their data collection efforts by having the protective force team help collect data at the portals. For example, PSS inspectors may provide the protective force inspectors with a short list of information to gather at each post as part of the post checks. Examples of information that might be more efficiently collected by the protective force team include whether SPOs are knowledgeable about policies for accepting badges of other contractors, whether each post has a current list of lost badges, and whether the post orders are consistent with site policies.

Cyber Security

Cyber security inspections are conducted by the Office of Cyber Security and Special Reviews (SP-42), often in conjunction with an HS-61 inspection. The interface with the SP-42 cyber security inspection team routinely involves an evaluation of the effectiveness of security controls implemented on computer systems used to operate automated access controls systems and intrusion detection systems, along with badging and video monitoring systems. This interface is especially important because many facilities do not consider the data processed by these computers to be classified, so these computers are not subject to the same strict security requirements as classified systems. Lower security requirements could lead to falsification of access credentials, unauthorized database manipulation, or, in the worst case, an undetected defeat of intrusion detection for an MAA. Because of the diversity of security alarm system applications, the PSS team must work closely with the cyber security team to determine the required level of protection that the security alarm system is expected to provide, and to evaluate the computer's ability to meet that goal.

This page intentionally left blank.

Section 11

ANALYZING DATA AND INTERPRETING RESULTS

Contents

Introduction

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

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

Inspectors must be aware of the relationships between the various elements of a particular PSS and between one PSS and another. For example, a barrier system might form the first layer of protection for more than a single asset. In one case it may be the only layer of protection, and in another it may be one of several layers. Auxiliary power systems may support several elements within a PSS and between separate system configurations. Recognizing these dual roles precludes duplicative testing efforts and places the particular element in proper perspective.

All elements of a properly designed PSS interface with one another and are interdependent. Entry control, intrusion detection, and barrier systems are directly related. Testing and maintenance is interwoven throughout all system elements. Auxiliary systems, such as auxiliary power generators, play a supportive role in the functioning of the overall PSS.

Analysis of Results

The information collected for each of the PSS subtopics is reviewed to determine whether the PSS complies with the requirements of DOE orders. In addition to compliance, the analysis process involves the critical consideration by topic team members of all inspection results, particularly identified strengths and weaknesses or deficiencies, framed within the parameters of the site mission. Analysis should lead to a logical, supportable conclusion regarding how well PSSs are meeting the required standards and satisfying the intent of DOE requirements.

A workable approach is to first analyze each subtopic individually. The results can then be integrated to determine the effects of the subtopics on each other and, finally, the overall status of the topic. As mentioned before, it is important to weigh the significance of a weakness or deficiency in light of the entire system. For example, if one intrusion detection device is inoperable, is the entire intrusion detection system deficient? What other measures or backup devices compensate for the deficiency? If barriers, other alarm systems, and CCTV cameras are in place, do they ensure that protection needs are being met? Although the deficiency may be worth noting in the report, it may not be significant enough to be a "rating driver" (meaning that it would not cause the subtopic or topic to be rated anything other than Satisfactory).

If there are no deficiencies, or if those that are identified are not rating drivers, the analysis is relatively simple. In this case, the analysis is a summary of the salient inspection results supporting the conclusion that protection needs are being met. If compensatory systems or measures were considered in arriving at the conclusion, these should be discussed in sufficient detail to clearly establish why they counterbalance any identified deficiencies.

If there are negative findings, weaknesses, deficiencies, or standards that are not fully met, the analysis must consider the significance and impact of these factors. The deficiencies must be analyzed both individually and collectively, then balanced against any strengths or mitigating factors to determine their overall impact on the PSS'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 office or contractor management previously knew of the deficiency and, if so, what action was taken
- Mitigating factors, such as the effectiveness of other protection elements that could compensate for the deficiency
- The deficiency's actual or potential effect on mission performance or accomplishment.

Ratings

The conclusions reached through the analysis of PSS inspection results may lead to the assignment of individual ratings in the subtopics or to a single rating for the topic. The topic team is responsible for assigning ratings; however, approval of final ratings rests with the Inspection Chief, the Director of HS-61, and ultimately, the Director of SP-40.

Interpreting Results

PSSs must perform so as to provide the desired level of protection for the asset(s) for which they are deployed. It is not enough that the various individual component parts of a system or systems meet manufacturers' specifications.

The SSSP and supporting documents can provide a link from DOE-wide performance expectations, including the DOE generic threat, orders, and policies, to facility-specific performance expectations.

Exterior Intrusion Detection and Assessment

When the perimeter can be frequently crossed without detection in one or more zones, it is likely that the perimeter sensors are not reliable. This weakness must be analyzed in light of site-

specific protection objectives and complementary systems. On the other hand, when one or more sensors can be defeated but redundancy in the sensor configuration is successful in detecting an intruder, the deficiencies are of lesser concern because the combination of sensors is effective. However, this problem may indicate testing and maintenance deficiencies.

When the facility indicates that a system is correctly calibrated but tests by HS-61 inspectors indicate that the sensors are not reliable, it may be an isolated instance of sensor drift or evidence of deficiencies in the facility's testing and calibration procedures. A large number of sensor deficiencies may indicate problems with the testing and maintenance program or the QA program. In this event, HS-61 inspectors may consider testing a representative sample of sensors in order to determine the extent of the problem..

When tests by both the facility and the inspection team indicate that the sensors are reliable, the system can be considered effective for that particular test; however, the testing parameters must be considered. For example, the system may not have been tested for all contingencies, or the test that was used may not have stressed the system to the limit.

Related tests or activities, such as perimeter barrier inspections, tests of CCTV and video-recording equipment, and tests of tamper and line supervision alarms, are typically conducted concurrent with the sensor tests. During these activities, inspectors need to look at the integrated system as a whole to determine whether it is effective in defeating intruders. Also, when the results of a test of one element are poor, inspectors should determine the impact of that result on the system.

Interior Intrusion Detection and Assessment

Inspectors should be aware that many interior sensor systems rely on redundant or layered protection (that is, a combination of barrier, volumetric, and point protection). If deficiencies are found in any one of these during testing, the results should be closely examined in light of program objectives and the complementary systems.

Entry and Search Control/ Badges, Passes, and Credentials

When entry can be made into the security area through one or more portals without authorization or detection, there is reason to believe that the entry control systems are not reliable.

Deficiencies in the badge system that can result in unauthorized personnel gaining access to classified information, security areas, or vital equipment are significant. Inspectors should pay particular attention to the effectiveness of control over the life cycle of the badge, including procurement, storage, issuance, disposition, and recovery. Other deficiencies in the badging system may include network and operational vulnerabilities.

Significant deficiencies in the badge system may indicate inadequate management attention, training, or resources devoted to administering and maintaining the badge system. All deficiencies should be evaluated to determine whether they result from human error, a systemic procedural problem, or a lack of supervisory emphasis. The root cause of any significant problem should be determined.

Barriers

While barriers cannot absolutely preclude an adversary gaining entry into the area being protected, they should provide delay times and, when properly complemented by intrusion detection systems, notification in the event of an attempted penetration. The lack of effective barriers may affect response times and may place an undue reliance on other systems.

Communications

The absence of adequate communication systems or duress alarms significantly impacts the capabilities of the protective force. One of the most important factors in an effective system is ensuring that the protective force responds to intrusion or duress in a timely and effective manner. To be able to respond appropriately, they must be able to communicate with the alarm stations, guard posts, response forces, and local

law enforcement agencies. Inadequate communication systems may result from budget constraints, lack of planning, or lack of management attention.

Testing and Maintenance

The backbone of any PSS is the testing and maintenance program. Without testing, alarm response and system reliability cannot be measured with any degree of certainty. Without maintenance, the hardware associated with these systems will begin to fail and, ultimately, deteriorate. The lack of an effective testing and maintenance program is a significant deficiency and is usually the root cause of a number of other problems. If this program is deficient, it is likely that there are problems in training, service repair, or management support.

Support Systems

All critical security systems that operate on electrical power must have a backup power source. These systems include:

- Intrusion detection system equipment
- CCTV
- Access controls
- Fixed base station communications equipment
- Alarm annunciation equipment
- Security lighting.

Failures in these backup sources may indicate an isolated mechanical problem or a systemic weakness in the system or in the testing and maintenance program.

If "load shedding" is required because auxiliary power sources are unable to instantaneously accept the full load of security equipment, the rationale for sequencing the load should be assessed. For example, the most critical loads, such as alarms and communications equipment, should be picked up first, followed by the less-critical systems, such as CCTV systems and lighting.

When assessing batteries, it is important to remember that many batteries have a predictable useful life, after which rapid degradation followed by complete failure can be expected. If all batteries were installed at the same time, it is likely that failure will occur in rapid succession throughout the system.

If there are indications that an adversary could defeat tamper protection without being detected in a significant number of attempts, it is likely that the tamper-protection system is not reliable. This situation should be analyzed in light of site-specific protection objectives and the effectiveness of complementary systems.

If there are indications that one or more tamper or line supervision devices are not functioning, it may be an isolated instance of component failure or an indication of systemic deficiencies in the design of the system.

Contractor and DOE Field Element Performance

HS-61 PSS inspectors should consider both contractor performance and DOE field element performance. In evaluating contractor performance, the PSS team should consider:

- Compliance with DOE orders, including the number and significance of findings in site office surveys and HS-61 inspections
- Responsiveness, indicated by procedures and timeliness in addressing and closing out previous findings
- QA program effectiveness, reflected by the quality of documentation, plans, procedures, records, and internal audit programs
- Defense-in-depth, including the number of layers of protection and the deployment of complementary systems
- Use of testing and maintenance records and false and nuisance alarm records to enhance system performance.

In evaluating DOE field element performance, the PSS team should consider whether:

- Surveys addressing PSSs are current.
- Survey ratings are consistent with the survey report narrative and work papers.
- Previous HS-61 PSS inspection concerns have been addressed.
- Survey results have been communicated to the facility operating contractor so that corrective actions can be implemented.
- Survey findings are tracked to completion and resolved in a timely manner.
- Exceptions are appropriate and documented.

Where appropriate, the inspection report should specifically identify weaknesses associated with contractor performance. Similarly, weaknesses specific to DOE line management should be identified as such.

Consideration of ISSM Concepts

As discussed in Section 1, HS-61 does not use the guiding principles or core functions of ISSM directly as a basis for ratings or findings. However, the ISSM concept provides a useful diagnostic framework for analyzing the causes of identified deficiencies. For example, inspectors may find that a required action is not being completed. Upon further investigation, inspectors may determine that the reason is that there has not been clear designation of responsibility for completing the required action. This situation may indicate a weakness related to line management responsibilities. In such cases, the inspectors would cite the deficient condition (i.e., the failure to complete the required action) as the finding and reference the requirement. In the discussion and opportunities for improvement, however, the inspectors may choose to discuss the general problem with assignment of responsibilities as a contributing factor.

As part of the analysis process, PSS inspectors should review the results (both positive aspects and weaknesses/findings) of the review of the PSS topic in the context of the ISSM concept. Using this diagnostic process, inspectors may determine that a number of weaknesses at a site or particular facility may have a common contributing factor that relates to one or more of the management principles. For example, a series of problems in intrusion detection effectiveness could occur if line management has not placed sufficient priority on testing and maintenance and has not provided adequate resources to implement an effective maintenance program. In such cases, the analysis/conclusions section of the PSS report appendix could discuss the weaknesses in management systems as a contributing factor or root cause of identified deficiencies.

APPENDIX A

SYSTEM PERFORMANCE TESTS

CONTENTS

FORMS*

* Each group of forms includes: Checklist–Interview Items, Tour/Visual Inspection Items, and a Data Collection Sheet.

This page intentionally left blank

Part 1
Exterior Perimeter Sensors

This page intentionally left blank

Part 1

Exterior Perimeter Sensors

Introduction

Objective

The objective of these performance tests is to determine the effectiveness of exterior perimeter sensors. The most directly applicable requirements are:

Applicability

	Order Reference
Category I and II SNM, Vital Equipment, PA	DOE Manual 470.4-2 Ch1, Chapter VII, Paragraph 3
Classified Matter, LA	DOE Manual 470.4-2 Ch1, Chapter VII, Paragraph 3
DOE Property and Unclassified Facilities	DOE Manual 470.4-2 Ch1, Chapter VII, Paragraph 3

System Tested

System - Intrusion-detection system

Function - Perimeter-intrusion detection

Component - Exterior sensors, transmission lines, alarm processing equipment, interfaces with CCTV and CAS operation. Testing and maintenance of perimeter sensors.

Scenario

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

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

- At least two zones should be tested. If the zones employ different sensor configurations, or if the sensor configuration at portals is significantly different, the inspectors should consider selecting at least one of each type.
- At least one of each type of sensor should be tested, if possible. This should include sensors on building roofs and sensors (if any) in tunnels under the perimeter.
- If the first few HSS-10 tests do not indicate problems and there is no evidence of exploitable deficiencies, the inspectors should not generally devote extensive time to testing numerous zones and sensors. However, if deficiencies are apparent, the inspectors should collect sufficient data to determine if a deficiency is an isolated instance or evidence of a systemic problem.
- Tests should be conducted for selected zones in which terrain features or questionable installation practices are likely to degrade detection capability.

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

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

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

Evaluation

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

Assessing Sensor Performance

The primary objective in the evaluation of exterior perimeter intrusion-detection sensors is to determine whether the system effectively and reliably detects an intruder crossing the perimeter. Other questions that should be considered in the evaluation are:

- Do the individual sensors detect an individual crossing the sensor detection pattern at varying rates? Typically the slowest rate for testing should be 0.15 m/sec and the fastest rate should be 5 m/sec. However, if patrol frequencies and direct visual observation are considered inadequate to provide reasonable assurance that such attempts would be detected, speed is no longer a factor to consider.
- Are the sensors positioned to allow adversaries to bypass one sensor at a time, or are they positioned such that an adversary attempting to bypass one sensor would be in the detection zone of a second (and possibly a third) type of sensor?

- Does the alarm system annunciate all alarms or does the system incorporate alarm processing logic (for example, one of two, two of three, two of four) that allows one sensor or sensors in different zones to activate without an alarm condition? If so, can adversaries exploit the design, that is, can adversaries cross the perimeter in such a manner that they do not cause an alarm? The inspectors should consider tactics such as zone hopping and defeating one of two complementary sensors.
- Can the adversary exploit the existing barriers (for example, fences, jersey bouncers) as a platform for jumping or as an aid in climbing to avoid detection?
- Have effective measures been taken to protect potential paths under (for example, storm sewers) or over (for example, wires or pipes) the detection zone?
- Are there any seams or bypasses between zones that can be exploited? If so, and there are multiple sensors, can more than one sensor be defeated?
- Are there dips, ditches, humps, or obstructions that could provide a pathway for an individual to avoid detection? If so, can those deficiencies be identified from outside the secure area?
- Are there probable differences in the day and night detection capability due to extremes of heat and cold or effects of sunlight versus darkness?
- Is the detection zone free of snow, ice, standing water, vegetation, or other obstructions that could prevent detection or cause nuisance alarms?
- Are sensors accessible from outside the PA, making them vulnerable to tampering (for example, "nudge" sensors out of alignment; jam multiple infrared or microwave sensors; block CCTV cameras)?
- Are the sensors particularly susceptible to adversaries using tools (for example, ladders, boards, ropes)?

Interpreting Results

The following guidelines are provided to assist the inspectors in interpreting results in the context of system performance.

- A perimeter system is only as good as its weakest link. Tests that indicate that a knowledgeable adversary could frequently cross the perimeter without detection in one or more zones are evidence that the perimeter sensors are not a reliable system. The significance of this finding must be analyzed in the context of the site-specific protection objectives and the effectiveness of other complementary systems.
- In some cases, testing by inspectors indicates that one or more sensors can be defeated but that, because of the degree of redundancy in the sensor configuration, an intruder crossing the perimeter would cause an alarm. In such cases, the identified deficiencies are of lesser concern because the tests indicate the combination of sensors is effective. However, the sensor deficiencies may indicate testing and maintenance problems.
- In some cases, facility tests indicate that the system is correctly calibrated but inspector tests indicate that the sensors can be defeated or do not reliably detect intrusion. In such cases, it is reasonable to conclude that there are deficiencies in the test and calibration procedures and in the quality assurance program.
- Facility tests that indicate that the sensors are calibrated according to specification, in conjunction with tests by inspectors that confirm the sensors are capable of reliably detecting an intruder, usually signify that the tested portion of the system is effective and that test and maintenance procedures are effective. However, the limitations of the tests must be recognized. For example, not all methods of defeat (for example, bridging of microwave sensors) may have been tested and the test may not have stressed the system to the limit.

- Facility tests that indicate that one or more sensors are not calibrated according to specifications may simply be an indication of an isolated instance of sensor drift. On the other hand, this may indicate systemic problems in the test and maintenance program, or problems related to the age and overall condition of the sensor system. If the facility tests indicate sensors are out of calibration, inspectors should consider instructing the facility technicians to test a representative sample of sensors in order to determine the extent of the problem.

Special Considerations

Some types of sensors are sensitive to the size of the intruder (or more accurately, the radar cross-section). Inspectors should request that the facility provide a relatively small person to conduct the crawl tests.

Related tests or activities, such as perimeter barrier inspections, tests of CCTV and video-recording equipment, and tests of tamper and line supervision alarms, are typically conducted concurrent with the sensor tests.

Responsibilities

Inspectors: Select zones and sensors. Direct tests and monitor alarm annunciation. (Typically one inspector will be stationed at the CAS and at least one at the perimeter.)

Facility: Conduct routine tests. Provide security technicians. Provide test devices as necessary (for example, aluminum spheres). Provide SPOs for security during testing, as required. Provide radios for two-way communication. Provide personnel (normally an SPO) to conduct tests (climb, crawl, run, and walk) at the direction of inspectors.

Internal Coordination

Tests should be scheduled to avoid conflicts with other tests involving the protective force.

Security Considerations

Observe all normal security considerations. Normally, an SPO must monitor (directly or via CCTV) the tests to ensure that no unauthorized personnel enter the protected area.

Personnel Assignments

Test Director:

Facility Alarm System Point of Contact:

Facility Protective Force Representative:

Safety Coordinator (if required):

Facility Safety Coordinator (if required):

Logistical Requirements

Personnel:

- Protective force representative
- Alarm technicians
- Tester

Equipment:

- Radio
- Test devices (for example, aluminum sphere for microwave and calibrated punch for fence vibration sensors)

Safety:

- Follow normal operating procedures
- Complete safety plan (if necessary)
- Notify CAS and other alarm monitoring stations before testing
- Station one inspector in CAS
- Arrange to prevent any undesired armed response to alarms

Bistatic Microwave Sensors

General Characteristics: Line-of-sight, freestanding, transmitter/receiver pairs

Intruder-Detection Capabilities: Walking, slow walking, running, crawling, rolling, jumping

Vulnerabilities: Tunneling, trenching, bridging

Concerns

- Even terrain over the length of the detection zone is critical. Ditches, humps, or dips greater than three inches may significantly reduce the capability to detect a crawling intruder.
- Insufficient offset may allow intruders to crawl under or jump over the beam at the crossover point (the point where adjacent zones overlap; typically, 30 feet or more is required).
- Separation distances between transmitter and receiver that are greater than the effective range of the detector (typically 100 meters) may significantly reduce detection capability.
- Microwave sensors are susceptible to nuisance alarms induced by standing water, high winds, blowing debris, snow, animals, lightning, and fencing that is too close to the sensor beam. Properly drained terrain and well-maintained isolation zones (vegetation free and without holes that would allow large animals to enter) can reduce the nuisance alarm rate.
- The accumulation of snow reduces sensor performance.
- Improper alignment may significantly reduce sensitivity and detection width and contribute to false alarms.
- Transmitters or receivers that are mounted too high may not detect someone crawling under the sensor.
- Transmitters or receivers that are mounted close to the ground may not detect someone vaulting over at the crossover point, if there is insufficient overlap between adjacent zones.

Types of Tests

- Walk Test Across the Zone

  Walk tests or shuffle walk tests are conducted to verify operability and sensitivity, and to determine the width of the detection zone. A shuffle walk involves small slow steps without swinging the arms (steps of five cm or less at 0.15 m/sec). The width of the detection zone can be determined by monitoring alarm annunciation. Sensitivity tests should be conducted at the mid-range of the sensor beam.

- Walk Test Parallel to the Zone

  Walk tests parallel to the zone are conducted to determine whether the sensor is misaligned or mounted too close to the fence. Such tests involve walking parallel to the zone approximately one meter from the fence and verifying that no alarm occurs.

- Run Tests

  Run tests are conducted to verify whether receiver response is fast enough. Run tests involve crossing the detector zone at a fast run (five m/sec). Such tests are performed where the beam is narrow—approximately six meters from the transmitter or receiver or just inside the crossover point (for overlapping sensors).

- Crawl Tests

  Crawl tests are conducted to verify proper detector alignment and sensitivity, and to determine whether terrain irregularities can be exploited. Crawl tests involve crossing the detection zone at selected points while minimizing radar cross section (intruder remains flat, parallel to the beam, head down, with no reflective clothing). Tests should be conducted by a relatively small individual crawling at approximately 0.15 m/sec. Tests should be conducted at various points along the detection zone, including just inside the crossover point, at the mid-range, and wherever terrain features are likely to reduce detection.

- Jump Tests

  Jump tests are conducted to verify adequate detection height. Such tests involve attempting to jump over the beam, and are conducted where the beam is narrowest (that is, near the crossover point). Barriers, buildings at the perimeter, sensor posts, or mountings may be used as platforms for jumping.

Test Guidelines

- All tests listed in the previous section should be conducted on at least two typical zones.
- Zones that are substantially different (different terrain, sensor configuration, portals) should also be considered for testing.
- Areas that appear vulnerable (due to alignment, terrain irregularities, or other concerns) should be tested.
- If an individual sensor can be defeated, that same sensor should be retested to determine whether it can be defeated a second time. Several tests of the same sensor may be required to determine whether an adversary can exploit the sensor.
- If an individual microwave sensor can be defeated by one or more methods (for example, jump, run, and crawl), the microwave sensors in other zones should be tested using the same methods in order to determine the extent of the problem. Inspectors should conduct several (three to five) more tests in different zones. If most of these tests indicate that the sensor can be reliably defeated, there is sufficient evidence to indicate that a systemic problem exists. If no other sensors are defeated, one may conclude that an isolated deficiency was identified. If the results are inconclusive, inspectors should consider testing additional sensors. Only rarely would an inspector test more than 10 to 15 zones.
- If the adversary has the knowledge, time, and equipment, bridging or tunneling can defeat all microwave sensors. Such tests should only be conducted if a zone is particularly vulnerable (for example, due to barrier placement, or if patrol frequencies and direct visual observation are considered inadequate to provide reasonable assurance that such attempts are detected).
- Experience with microwave sensors has shown that the slowly crawling intruder and the intruder jumping over a single stack microwave unit are the most difficult to detect. Therefore, much of the testing effort is devoted to crawl tests and jump tests in microwave zones that appear to have alignment problems or terrain irregularities.

Checklist
Bistatic Microwave Sensors
Exterior Perimeter Intrusion-Detection System
Interview Items

Installation location _____

_____

Operational test frequency _____

_____

Operational test method _____

_____

Sensitivity test frequency _____

_____

Sensitivity test method _____

_____

Acceptance criteria for sensitivity test _____

_____

Procedures for vegetation removal _____

_____

Procedures for snow removal _____

_____

False alarm history/records _____

_____

Make/model _____

_____

Measures to prevent erosion _____

_____

Tamper switches (transmitter, receiver, junction boxes) _____

_____

Tour/Visual Inspection Items

Vegetation present? _____

_____

Deep snow present? _____

_____

Terrain level? _____

_____

Zone length OK? _____

_____

Complements other sensors? _____

_____

Overlap sufficient? _____

_____

Standing water present or likely? _____

_____

Frequency of patrols? _____

_____

Data Collection Sheet
Bistatic Microwave – Exterior Perimeter Intrusion-Detection System

Test Method

	Zone Tested	Zone Number	Walk Across	Walk Shuffle	Walk Parallel	Run	Crawl	Jump
1								
2								
3								
4								
5								
6								
7								
8								
9								
10								
11								
12								
13								
14								
15								
Comments:								

Active Infrared Sensors

General Characteristics:	Line-of-sight, vertical plane, post-mounted, multiple transmitters and receivers
Intruder Detection Capabilities:	Walking, slow walking, running, crawling, rolling, jumping
Vulnerabilities:	Tunneling, trenching, bridging, climbing

Concerns

- Because infrared is a narrow beam line-of-sight detector, there should be no surface depressions of six inches or more, which may permit crawling under the lowest transmitter/receiver pair. The bottom beam should be aligned within six inches of the ground surface.
- The ground under the detection zone should be compacted, graveled, or paved to preclude easy furrowing under the zone (look for loose gravel; this is usually a big problem).
- Close proximity to fences, building walls, CCTV towers or other structures may permit easy bridging or jumping over the narrow vertical detection zone (sensor stacks can, themselves, become climbing aids).
- Infrared sensors are susceptible to nuisance alarms induced by animals, vegetation, fog, snow, and wind-blown dust and debris.
- Heavy snow must be removed to preclude tunneling through the snow to avoid detection.
- In some older model sensors, sunlight and vehicle headlights may cause false alarms.
- Improper alignment may significantly reduce sensitivity and detection width and contribute to false alarms.

Types of Tests

- Walk Test Across the Zone

  Walk tests are conducted to verify operability and sensitivity. These tests should be conducted at mid-range of the sensor beam.

- Run Tests

  Run tests are conducted to verify that receiver response is fast enough. They involve crossing the detector zone at a fast run (5 m/sec).

- Crawl Tests

  Crawl tests are conducted to verify proper detector alignment and sensitivity, and to determine whether terrain irregularities can be exploited. Crawl tests involve crossing the detection zone at selected points while minimizing target cross-section (intruder remains flat, perpendicular to the beam, head down, with no reflective clothing). Tests should be conducted by a relatively small individual moving at approximately 0.15 m/sec (see "Assessing Sensor Performance," page A-4). Tests should be conducted at various points along the detection zone, including the mid-point, and wherever terrain features are likely to reduce detection capability.

- Jump Tests

  Jump tests are conducted to verify adequate detection height. Such tests involve attempting to jump over the beam and are conducted where barriers, buildings, sensor posts, or mountings can be used as jumping platforms.

Advanced technique tests

The advanced technique tests consist of introducing props/ equipment that would assist the performance tester with defeating the sensor system.

- Spoofing tests

  Spoofing techniques are utilized in stealth attempts of bypassing the sensor systems or CCTV. Spoof methods are executed by positioning in an undetected area of the zone and manipulating the sensor system or CCTV using performance testers accessories.

- Multiple-man tests

  The multiple-man test is effective to maximize the ability to jump and run over and through sensors during routine performance testing. This method can be utilized in stacking various zones and generating multiple alarms simultaneously.

Test Guidelines

- All zones should be considered using three methods of testing. Can the performance tester pass above, through, or below the sensor system. These three elements are essential in strategizing potential pathways through the zones.
- All sensor tests are conducted on the first attempt. If the tester fails to defeat the sensor, there are no second chances in that specific zone.
- To ensure performance test accuracy during an execution, all inactive bystanders in the sensor vicinity must remain still.
- During performance tests intervals, allow enough time between iterations for the microwave sensitivity to rebalance
- Central alarm station operators should have effective communications with the inspector's escort to expedite sensor alarm and reset annunciation.
- Prior to PIDAS physical testing each day, inspect all props and testing equipment to ensure a safe and accurate performance test. This includes all personal gear such as harnesses, lanyards, shoelaces, etc. Testing items, planks or ladder system, require a "once over" inspection prior to use.
- Razor ribbon and barbed wire usually appears as a deterrent and in many cases is nothing to attempt to compromise. If the razor-ribbon loops and strands are overlapping and tightly configured, a tester should move to the next zone; however, if the razor-ribbon seems stretched and in single strand, a tester can open a pathway by attaching the razors to the fence fabric. In addition, Razor-ribbon loops act as a climbing element. Outrigger barbed-wire assist testers when climbing or stabilizing on fence top rails.
- Pizza cutters, usually found on microwave support poles, are defeated by creating a wedge or having another tester hold and secure the wheel.
- PIDAS junction boxes usually have tamper protection and should be tested spot-checked frequently
- While reviewing and walking the isolation zone, make sure no essential PIDAS cables and connections are exposed on cable trays or unsecured subsurface boxes.
- Inspector's interests should not overlook sensor overlaps, gates, and buildings attached to the isolation zone.
- Prior to any physical test execution, be sure that all testing participants clearly understand the pathway strategy and guidelines. Team communication enforces team safety.

- The PSS testing team mission statement/ plan of the day should coordinate prior to exploring the field. The pre-testing briefing contains general strategy, location, equipment, and personnel needed to conduct the proposed test.
- The PSS testing team should properly stretch five to ten minutes before physically testing
- Uniforms and gear are essential when exploring and testing outdoors and indoors. Dress appropriately to the weather conditions. Always wear protective leather gloves and proper footwear to support ankles. Knee and elbow pads are recommended. Contact the HSS or on-site safety officer if any questions or concerns should arise.
- All the tests listed in the previous section should be conducted on at least two typical zones.
- Zones that are substantially different (different terrain, sensor configuration, or portals) should also be considered for testing.
- Areas that appear vulnerable (due to structures that aid bridging or jumping, terrain features, or other concerns) should be tested.
- If an individual sensor can be defeated, that same sensor should be tested again to determine whether such defeat can be repeated. Several tests of the same sensor may be required to determine whether an adversary can reliably exploit a sensor deficiency.
- If an individual zone can be defeated by one or more methods (for example, jump, run, crawl) other zones should be tested using the same methods to determine the extent of the problem. The inspectors should conduct several (three to five) more tests in different zones. If most of these tests indicate the sensor can be reliably defeated, it is likely that a systemic problem exists. If no other sensors are defeated, one may conclude that an isolated deficiency was identified. If results are inconclusive, the inspectors should consider testing additional sensors. Only rarely would an inspector test more than 10 to 15 zones using the same methods.
- If the adversary has the knowledge, time, and equipment, bridging or tunneling techniques can defeat all infrared sensors. Since the infrared beam is quite narrow, bridging or tunneling can be accomplished fairly rapidly and easily. Such tests should only be conducted if a zone is particularly vulnerable (for example, due to barrier placement) or if patrol frequencies and direct visual observation (CCTV or guard posts) are considered inadequate to provide reasonable assurance that such attempts are detected.
- Experience with infrared sensors has shown that vaulting the zone at the mounting post is the most likely method of quickly defeating the system. This method, together with the crawl test (where there are depressions in the ground surface), should be used when possible.

Checklist
Active Infrared Sensors
Exterior Perimeter Intrusion-Detection System
Interview Items

Installation location _____

_____

Operational test frequency _____

_____

Operational test method _____

_____

Sensitivity test frequency _____

_____

Sensitivity test method _____

_____

Acceptance criteria for sensitivity test _____

_____

Procedures for vegetation removal _____

_____

Procedures for snow removal _____

_____

False nuisance alarm history/records _____

_____

Make/model _____

_____

Measures to prevent erosion _____

_____

Tamper switches (transmitter, receiver, junction boxes) _____

_____

Tour/Visual Inspection Items

Vegetation present? _____

_____

Deep snow present? _____

_____

Terrain level? _____

_____

Zone length OK? _____

_____

Complements other sensors? _____

_____

Overlap sufficient? _____

_____

Structures adjacent to the zone permitting vaulting/bridging _____

_____

Data Collection Sheet
Active Infrared Sensors – Exterior Perimeter Intrusion-Detection System

Test Method

	Zone Tested	Zone Number	Walk	Run	Crawl	Jump	Bridge
1							
2							
3							
4							
5							
6							
7							
8							
9							
10							
11							
12							
13							
14							
15							
Comments:							

Electric Field Sensors

General Characteristics:	Electric field-generating wire coupled to sensor wire, freestanding or fence-mounted, can follow irregular terrain
Intruder Detection Capabilities:	Walking, slow walk, running, crawling, rolling, jumping
Vulnerabilities:	Tunneling, trenching, bridging

Concerns

- Improper wire/spring tension or improper wire/insulation coupling can cause unacceptable false and nuisance alarms. Careful installation and maintenance are required for proper sensor operation.
- Two-wire (versus three- or four-wire) configurations may permit an intruder to jump between the field wire and sensing wire undetected.
- When more than one section of electric field is installed, adjacent sensors should overlap to overcome the lack of sensitivity around the tension springs and end insulators.
- Electric field sensors are not generally used at fence gates because of the requirement to maintain wire tension, although removable sections can be used. For frequently used gates, active infrared or microwave sensors are normally used. In such cases, there must be sufficient overlap between the gate sensor and the adjacent electric field zone to preclude intrusion between zones of different sensors.
- Electric field sensors are susceptible to nuisance alarms from lightning, high-level electromagnetic noise (for example, transformers) animals, heavy rain, wet snow, and blowing debris.
- Electric field sensitivity is a concern with accepting slow movement/stop approach while the tester is passing through the detection field.
- Request a bystander to time the testers movements through the sensor with a stopwatch.

Types of Tests

- Walk Test Perpendicular to the Zone

  Walk tests are used to verify sensor operability and sensitivity. The zone should alarm when approached at normal walking speed when one is between 1 and .5m from the wire. This test is used for two- and three-wire systems (see "Assessing Sensor Performance," page A-4).

- Shuffle Walk Test Perpendicular to the Zone

  Shuffle tests are conducted by taking slow, small steps without swinging the arms (steps of 5 cm or less at 0.15 m/sec). The system should alarm at a distance of 25 cm or less, and any attempt to climb between the wires should be detected.

- Stoop Test (for four-wire systems)

  This test is conducted by walking to a point near the sensor then facing parallel to the wires. The control unit should be allowed to stabilize, then the individual should stoop or squat down to unbalance the upper and lower zones. An alarm should annunciate.

- Crawl Test Perpendicular to the Zone

  The crawl test consists of an individual crossing the zone at a slow crawl as close to the ground as possible, in zones where the bottom wire is highest (6 inches or more) from the ground or where there is a depression in the zone. An alarm should annunciate.

- Jump Test

  The jump test cannot normally be performed if the electric field sensor is properly installed, due to the height of the detection zone (eight feet or more). However, where there are structures adjacent to the zone it may be possible to jump over the sensor wire, if personal safety can be assured.

- Step-Through Test

  Step-through tests should be conducted if the walk tests, shuffle walk tests, and stoop tests indicate that the electric field sensors are not sufficiently sensitive. The step-through test consists of an individual stepping or jumping between the electric field wires and crossing the detection zone while avoiding contact with the wire. If the zones do not overlap, this test should be conducted at the end of the zone (near tension springs) where sensitivity is lowest, otherwise the test should be conducted at several locations throughout the zone. Some of the older models are more susceptible to penetration.

- Feet first test

  The electric field sensitivity is usually the most vulnerable while first presenting the smallest part of the tester's body into the detection area. During this execution, the tester should gradually introduce the larger portions of the body, monitoring the pace/body-mass equation, and maintain control and steadiness of movements.

Test Guidelines

- The person conducting the tests should remove all metal objects and should not wear steel-toed shoes or wear gloves.
- Walk tests, shuffle walk tests, and stoop tests should be conducted on at least two typical zones.
- If sensitivity is questionable on the initial walk or stoop tests, the step-through tests should be conducted to determine if a person can cross the detection zone undetected.
- Zones that are substantially different (different terrain, sensor configuration, portals) should also be considered for testing.
- Areas that appear vulnerable (due to terrain features or other concerns) should be tested (crawl tests or jump tests).
- If an individual sensor can be bypassed, that same sensor should be tested again to determine if bypassing can be repeated. Several tests of the same sensor may be required to determine if an adversary can reliably exploit the sensor deficiency.
- If an individual electric field zone can be defeated by one or more methods (for example, jumping, running, crawling), other zones should be tested using the same methods to determine the extent of the problem. The inspectors should conduct several more tests (three to five) in different zones. If most of these tests indicate that the sensor can be reliably defeated, it is likely that there is a systemic problem. If no other sensors are defeated, it may be concluded that an isolated deficiency was identified. If the results are inconclusive, additional sensors may be considered for testing. Only rarely would an inspector test more than 10 to 15 zones using the same method.
- If an adversary has the knowledge, time, and equipment, bridging or tunneling can defeat all electric field sensors. Such tests should only be conducted if it appears that a zone is vulnerable, or if patrol frequencies and direct visual observation (CCTV or guard posts) are considered inadequate to provide reasonable assurance that such attempts are detected.

- Experience with electric field sensors has shown that the slow-crawling intruder is the most difficult to detect. Typically, much of the test effort is devoted to crawl tests of zones that appear to have installation or terrain irregularities.
- When activating an alarm, Allow ample time between E-field test intervals to assure sensor sensitivity status is normal.

Checklist
Electric Field Sensors
Exterior Perimeter Intrusion-Detection System
Interview Items

Installation location _____

_____

Operational test frequency _____

_____

Operational test method _____

_____

Sensitivity test frequency _____

_____

Sensitivity test method _____

_____

Acceptance criteria for sensitivity test _____

_____

Procedures for vegetation removal _____

_____

Procedures for snow removal _____

_____

False alarm history/records _____

_____

Make/model _____

_____

Measures to prevent erosion _____

_____

Tamper switches (transmitter, receiver, junction boxes) _____

_____

Tour/Visual Inspection Items

Vegetation present? _____

_____

Deep snow present? _____

_____

Terrain level? _____

_____

Zone length OK? _____

_____

Complements other sensors? _____

_____

Overlap sufficient? _____

_____

Wire tension and terminations satisfactory? _____

_____

Data Collection Sheet
Electric Field Sensors – Exterior Perimeter Intrusion-Detection System

Test Method

	Zone Tested	Zone Number	Walk	Walk Shuffle	Stoop	Crawl	Jump	Step Through
1								
2								
3								
4								
5								
6								
7								
8								
9								
10								
11								
12								
13								
14								
15								
Comments:								

Buried Line Sensors

General Characteristics:	Buried cable(s); seismic, magnetic or electromagnetic coupled field detectors; signal processor unit; cable(s) follow terrain
Intruder-Detection Capabilities:	Varies depending on type; may include walking, running, jumping, crawling, trenching, and tunneling
Vulnerabilities:	Bridging

Note: Due to the varying sensing techniques of buried line sensors, the strengths and weaknesses of various systems differ somewhat. However, the method of testing is the same for each.

Concerns

- Standing water, wind-blown debris, electromagnetic interference, vehicular traffic, lightning, and animals may cause nuisance alarms depending on the type of buried line sensor used.
- Seismic sensors may not function when installed under roadbeds or sidewalks, or when the ground is frozen or under deep snowpack.
- Ported leaky coax is susceptible to nuisance alarms due to running or wind-blown water, moving metallic objects (vehicles), or lightning.
- Seismic sensors may experience nuisance alarms if installed in the vicinity of fences, power poles, guy-wires, or roads (vehicle ground vibration).
- Ground covering the sensor should be maintained in such a manner that the actual location of the sensor is not visually apparent.

Types of Tests

- Walk Tests Across the Zone

  Walk tests should be conducted at a normal walking speed in at least three places within each buried cable zone.

- Run or Jump Tests Across the Zone

  Run tests are conducted to verify prompt sensor response and should be conducted at a fast run (5m/sec) at three locations within a given detection zone. The runner may attempt to jump over the location where the sensor is buried.

- Low–crouch test

  Low-crouch testing is conducted through the volumetric area of the ported-coaxial. The basic design is to create the smallest figure possible and steadily move heel over toes through the detection area.

- Roll Tests to the Zone

  Roll tests consist of an individual slowly rolling across the detection zone with the body oriented parallel to the buried cable(s) with arms held close to the body and legs together. A roll test should be conducted when there is a hard surface road or sidewalk crossing the zone.

Test Guidelines

- All tests listed in previous section should be conducted on at least two typical zones.
- Areas that appear vulnerable (due to the existence of hard surface roads, standing water, sources of seismic interference, or other reasons) should be tested.
- If an individual sensor can be defeated, that same sensor should be tested again to determine whether it can be defeated again. Several tests of the same sensor may be required to determine if an adversary can reliably exploit the sensor.
- If an individual zone can be defeated by one or more methods, the buried line sensors in other zones should be tested using the same methods to determine the extent of the problem. Inspectors should conduct several more tests (three to five) in different zones. If most of these tests indicate that the sensor can be reliably defeated, it is likely that a systemic problem exists. If no other sensors are defeated, one may conclude that an isolated deficiency was identified. If the results are inconclusive, additional testing should be considered. An inspector would rarely test more than 10 to 15 zones using the same methods.
- If the adversary has the knowledge, time, and equipment, bridging techniques can defeat most buried line sensors. Such tests should only be conducted if a zone is particularly vulnerable, or if patrol frequencies and direct visual observation (CCTV or guard posts) are considered inadequate to provide reasonable assurance that such attempts are detected.

Checklist
Buried Line Sensors
Exterior Perimeter Intrusion-Detection System
Interview Items

Installation location _____

_____

Operational test frequency _____

_____

Operational test method _____

_____

Sensitivity test frequency _____

_____

Sensitivity test method _____

_____

Acceptance criteria for sensitivity test _____

_____

Procedures for vegetation removal _____

_____

Procedures for snow removal _____

_____

False alarm history/records _____

_____

Make/model _____

_____

Tamper switches (transmitter, receiver, junction boxes) _____

_____

Tour/Visual Inspection Items

Vegetation present? _____

_____

Deep snow present? _____

_____

Terrain level? _____

_____

Zone length OK? _____

_____

Complements other sensors? _____

_____

Overlap sufficient? _____

_____

Standing water present or likely? _____

_____

Hard surfaced road crosses zone? _____

_____

Power poles, guy wires or other seismic sources exist? _____

_____

Data Collection Sheet
Buried Line – Exterior Perimeter Intrusion-Detection System

Test Method

	Zone Tested	Zone Number	Walk	Run/Jump	Roll
1					
2					
3					
4					
5					
6					
7					
8					
9					
10					
11					
12					
13					
14					
15					
Comments:					

Taut-Wire Sensor Fence

General Characteristics:	Tensioned horizontal wires connected to detector posts, freestanding or fence-mounted
Intruder Detection Capabilities:	Cutting, climbing, or other deflection of sensor wire
Vulnerabilities:	Tunneling, trenching, bridging

Concerns

- Since taut-wire sensors operate on mechanical principles, they are relatively impervious to weather, wind, electromagnetic interference, and other common sources of nuisance alarms.
- Some systems, which have only one sensor switch channel for multiple parallel switches, may be defeated by cutting ungrounded switch leads if the end-of-line resistor and signal cable are not disturbed.
- As with other fence-mounted mechanical (pressure, strain, vibration) sensors, taut-wire systems are susceptible to defeat by tunneling, bridging, or jumping, if no physical contact with the sensing wires occurs.
- Taut-wire sensors are not generally used at fence gates because of the requirement to maintain wire tension. For frequently used gates, active infrared or microwave sensors are often used. In such cases, there must be sufficient overlap between the gate sensor and the adjacent taut-wire zone to preclude intrusion between zones of different sensors.
- Older systems used fewer total wires, allowing inspectors to climb over system or under system if not fence-mounted.

Types of Tests

- Simulated Climb Test (for freestanding taut-wire sensors)

  This test consists of a ladder being placed against the wires and an individual climbing the ladder to a point where sensor activation occurs (usually when the knees are near the top of the fence). Local alarm indication is required to prevent damage to sensor switches.

- Wire Pull Test

  Individual wires are pulled up or down by hand so that a deflection of approximately four inches is achieved. The distance that the wire is pulled before an alarm is generated should be noted.

- Cutting

  No actual cutting of the sensor wires should be performed.

- Jump Tests

  These tests cannot normally be performed if the taut-wire sensor is properly installed, due to the height of the detection zone (eight feet or more). However, structures adjacent to the zone used as platforms may make it possible to jump over the sensor wire, if personal safety can be assured.

Note: During periods of extreme cold weather, it may take some time for the mechanical sensor switches to return to the normal neutral position after activation. This should be taken into account when considering multiple tests of the same zone.

Test Guidelines

- All tests listed in the previous section should be conducted on at least two typical zones.
- Zones that are substantially different (different terrain, sensor configuration, portals) should also be considered for testing.
- Areas that appear vulnerable (due to terrain irregularities or other reasons) should be tested to determine whether a vulnerability exists.
- If an individual sensor can be defeated, that same sensor should be tested again to determine if it can be defeated repeatedly. Several tests of the same sensor may be required to determine whether an adversary can reliably exploit the sensor deficiency.
- If an individual taut-wire zone can be defeated by one or more methods (for example, bridging and climbing), other zones should be tested using the same methods to determine the extent of the problem. Inspectors should conduct several more tests (three to five) in different zones. If most of these tests indicate that the sensor can be reliably defeated, it is likely that a systemic problem exists. If no other sensors are defeated, one may conclude that an isolated deficiency was identified. If results are inconclusive, additional testing should be considered. Only rarely would an inspector test more than 10 to 15 zones using the same methods.
- If the adversary has the knowledge, time, and equipment, bridging or tunneling techniques can defeat all taut-wire sensors. Such tests should be conducted only if a zone is particularly vulnerable (for example, due to barrier placement), or if patrol frequencies and direct visual observation (CCTV or guard posts) are considered inadequate to provide reasonable assurance that such attempts are detected.

Checklist
Taut-Wire Sensor Fence
Exterior Perimeter Intrusion-Detection System
Interview Items

Installation location _____

_____

Frequency of operational test _____

_____

Operational test method _____

_____

Sensitivity test frequency _____

_____

Sensitivity test method _____

_____

Acceptance criteria for sensitivity test _____

_____

Procedures for vegetation removal _____

_____

Procedures for snow removal _____

_____

False alarm history/records _____

_____

Make/model _____

_____

Measures to prevent erosion _____

_____

Tamper switches (junction boxes) _____

_____

Tour/Visual Inspection Items

Vegetation present? _____

_____

Deep snow present? _____

_____

Terrain level? _____

_____

Zone length OK? _____

_____

Complements other sensors? _____

_____

Overlap sufficient? _____

_____

Wire tension and terminations satisfactory? _____

_____

Data Collection Sheet
Taut-Wire Sensor Fence – Exterior Perimeter Intrusion-Detection System

Test Method

	Zone Tested	Zone Number	Simulated Climb	Wire Pull	Cutting	Jump
1						
2						
3						
4						
5						
6						
7						
8						
9						
10						
11						
12						
13						
14						
15						
Comments:						

Video Motion Detector

General Characteristics:	Comparison of digitized camera view, some masking capability, variable scan rates
Intruder Detection Capabilities:	Any intruder motion affecting a sufficient part of the camera's field of view
Vulnerabilities:	Extreme slow motion and an individual wearing clothing that matches the background

Concerns

- Video motion detectors are complex devices requiring extensive maintenance and calibration.
- Due to high detection sensitivity, some systems are highly susceptible to nuisance alarms from reflected light, cloud motion, sunrise and sunset, automobile headlights, wind-blown objects, and animals (if the detector's field of view is wide and encompasses areas outside of the potential space, the greater the potential for nuisance alarms).
- Camera vibration due to wind may create false alarms, as well as improper camera signal synchronization or other video signal disturbance.
- Camera image tube "burn in" caused by a constant view of the same scene may degrade sensitivity of the video motion detector, particularly where extreme changes in light to dark contrast are present.
- Any obstruction that blocks the camera's field of view, or creates strong shadowed areas, may prevent intruder detection.
- If the length of the field of view is too long for the camera lens, an intruder at the extreme end of the field of view may be able to avoid detection.
- If the "refresh rate" (the rate at which one camera scene is compared to the previous scene) is too slow, an intruder may be able to run through the field of view near a camera without detection.
- In the case of digital systems, the zone(s) of detection should be reviewed to ensure proper coverage in the field of view.
- Fog or smoke (grenade) is likely to adversely impact system effectiveness.

Types of Tests

- Walk Test Across the Zone

  Walk tests or shuffle-walk tests are conducted to verify operability and sensitivity, and to determine the width of the detection zone. A shuffle walk involves small slow steps without swinging the arms (steps of 5 cm or less at 0.15 m/sec). Width of the detection zone can be determined by monitoring alarm annunciation. Sensitivity tests should be conducted at the furthermost observable point in the camera's field of view (see "Assessing Sensor Performance," page A-4).

- Run Tests

  Run tests are conducted to determine whether the detector response is fast enough. Run tests consist of an individual crossing the detector zone at a fast run (5 m/sec). Such tests are performed at the nearest and furthermost points in the camera's field of view (see "Assessing Sensor Performance," page A-4).

- Crawl Tests

  Crawl tests are conducted to verify proper detector sensitivity and to determine whether terrain irregularities can be exploited. Crawl tests consist of an individual crossing the detection zone at selected points (intruder remains flat, parallel to the camera field of view, head down, with no reflective clothing). Tests should be conducted by a relatively small individual moving at approximately 0.15 m/sec. Tests should be conducted at various points along the detection zone wherever terrain features are likely to reduce detection and at the furthermost observable point in the camera's field of view (see "Assessing Sensor Performance," page A-4).

Note: Cameras outside the protected area can be manipulated to prevent alarming during intrusion. Special care must be taken when examining a video motion detector system with unprotected cameras.

Test Guidelines

- Tester should be dressed in standard work clothing (e.g., washed denim jeans and jacket).
- Camouflage will assist the tester (snow camouflage in snow or light-colored gravel).
- All tests listed in the previous section should be conducted on at least two typical zones.
- Zones that are substantially different (different terrain, lighting conditions, obstructions) should also be considered for testing.
- Areas that appear vulnerable (due to lighting deficiencies, terrain irregularities, or other reasons) should be tested to determine whether a vulnerability exists.
- If an individual camera's detector can be defeated, that same camera should be tested again to determine whether the deficiency can be repeated. Several tests of the same zone may be required to determine whether an adversary can reliably exploit the deficiency.
- If an individual camera zone can be defeated by one or more methods (run, walk, crawl), the other camera zones should be tested using the same methods to determine the extent of the problem. The inspectors should conduct several more tests (three to five) in different zones. If most of these tests indicate the detector can be reliably defeated, it is likely that there is a systemic problem. If no other zones are defeated, one may conclude that an isolated deficiency was identified. If the results are inconclusive, additional testing should be considered. Rarely would an inspector test more than 10 to 15 zones using the same methods.

Checklist
Video Motion Detector
Exterior Perimeter Intrusion-Detection System
Interview Items

Installation location _____

_____

Operational test frequency _____

_____

Operational test method _____

_____

Sensitivity test frequency _____

_____

Sensitivity test method _____

_____

Acceptance criteria for sensitivity test _____

_____

Procedures for vegetation removal _____

_____

Procedures for snow removal _____

_____

False nuisance alarm history/records _____

_____

Make/model _____

_____

Measures to prevent erosion _____

_____

Tamper switches (transmitter, receiver, junction boxes) _____

_____

Tour/Visual Inspection Items

Vegetation present? _____

_____

Deep snow present? _____

_____

Terrain level? _____

_____

Zone length and field of view OK? _____

_____

Complements other sensors? _____

_____

Overlap sufficient? _____

_____

Obstructions present? _____

_____

Lighting adequate? _____

_____

Data Collection Sheet
Video Motion Detection – Exterior Perimeter Intrusion-Detection System

Test Method

	Zone Tested	Functional Test	Walk	Run	Crawl
1					
2					
3					
4					
5					
6					
7					
8					
9					
10					
11					
12					
13					
14					
15					
Comments:					

Monostatic Microwave Sensors

General Characteristics:	Volumetric coverage; transmitter/receiver unit; typically mounted pointing at a building to provide coverage of approaches; also used on rooftops or gates
Intruder Detection Capabilities:	Walking, slow walk, running, crawling, rolling, jumping
Vulnerabilities:	Tunneling, trenching, bridging

Concerns

- Microwave sensors are susceptible to false alarms induced by standing water, high winds, snow, animals, lightning, and fencing that is too close to the sensor beam. Properly drained terrain and well-maintained isolation zones (vegetation free and without holes that would allow large animals to enter) can reduce the false alarm rate.
- Optimum coverage requires direct line of sight. Obstructions such as columns, beams, air-conditioning units, or other large objects may prevent detection.
- Sensor transceivers and control units are subject to physical damage and tampering if they are readily accessible or are not covered by another sensor's detection pattern.
- Sensors are susceptible to false alarms due to moving objects, electromagnetic radiation, air movement, seismic vibration, fluorescent lighting, and background noise.
- Proper overlap and coverage must be considered to ensure that an intruder cannot cross over, around, or under the sensor's pattern of coverage.
- The microwave detection beam can easily penetrate glass, wood, wallboard, and plastic (including downspouts and drainpipes), creating false alarms from moving objects outside the protected space.
- A sensor is most sensitive to a target moving directly toward or away from the transceiver.
- Inspector should check to see if sensor could be deliberately misaligned. It will reset itself regardless of position (i.e., point at the sky)—insider or outsider.

Types of Tests

- Sensitivity Walk Test

  Walk tests are used to verify operation and sensitivity of the sensor. This test is performed by slowly walking (1 ft/sec) toward microwave sensors until an alarm is received. This test should establish the far end of the sensor coverage pattern.

- Crossing Walk Test

  This test verifies the ability of the sensor to detect motion along the least sensitive axis of the detection pattern. After the end of the sensor coverage pattern is determined from a sensitivity walk test, a crossing test should be performed by walking across the far end of a microwave zone from various points outside the detection zone. Detection should occur before the tester enters the defined protected space or reaches the protected asset.

- Avoidance Walk Test

  Based on the sensor coverage pattern (oval, wedge, or circle), the inspector should attempt to enter the target zone by walking around the sensor's zone of coverage. This test should verify adequate sensor coverage and overlap to provide detection for the protected space or target/object.

- Crawl test—as close to sensor head as possible.

Test Guidelines

- The person conducting the tests should remove all metal objects and should not wear steel-toed shoes. Observers should be requested to stand away from the area being tested in order to reduce confusion.
- Testing should be conducted on at least two typical zones.
- Any zones that have potential vulnerabilities caused by obstructions or other sources of interference should be tested to determine whether they can be exploited.
- If there are apparent weaknesses in zone coverage or sensor overlap, these should be tested to determine whether sensor coverage could be circumvented.
- Experience indicates that monostatic microwave sensors are most vulnerable to a very slowly moving target entering the detection zone on the least sensitive axis (across the zone for microwave sensors).
- Many sensors have alarm indicator lights built into the sensor head. The inspectors may observe these indicators to facilitate testing the coverage pattern or sensor sensitivity. However, the inspectors should also verify that an alarm is received in the alarm stations to ensure that the alarm circuit is functional from sensor to annunciation point.
- If an individual sensor can be defeated, that same sensor should be tested again to determine whether the deficiency can be repeated. Several tests of the same sensor may be required to determine if an adversary can reliably exploit the sensor deficiency.
- If an individual microwave sensor or zone can be defeated, the microwave sensors in other zones should be tested using the same methods to determine the extent of the problem. The inspectors should conduct several more tests (three to five) in different zones. If most of these tests indicate that the sensor can be reliably defeated, it is likely that a systemic problem exists. If no other sensors are defeated, one may conclude that an isolated deficiency was identified. If results are inconclusive, additional testing should be considered.

Checklist
Monostatic Microwave Sensors
Exterior Perimeter Intrusion-Detection System
Interview Items

Installation location _____

_____

Operational test frequency _____

_____

Operational test method _____

_____

Sensitivity test frequency _____

_____

Sensitivity test method _____

_____

Acceptance criteria for sensitivity test _____

_____

Procedures for vegetation removal _____

_____

False alarm history/records _____

_____

Make/model _____

_____

Tamper switches (transmitter, receiver, junction boxes) _____

_____

Tour/Visual Inspection Items

Vegetation present? _____

_____

Complements other sensors? _____

_____

Overlap sufficient? _____

_____

Standing water present or likely? _____

_____

Obstructions present? _____

_____

Data Collection Sheet
Monostatic Microwave Sensors – Exterior Perimeter Intrusion-Detection System

Test Method

	Zone Tested	Sensitivity Walk	Crossing Walk	Avoidance Walk	Crawl
1					
2					
3					
4					
5					
6					
7					
8					
9					
10					
11					
12					
13					
14					
15					
Comments:					

Fence Disturbance Sensors

General Characteristics:	Sensing wires/cables attached to or woven through fence, sonic capacitance, or piezoelectric technologies
Intruder Detection Capabilities:	Cutting, climbing, or other vibration/deflection of sensor wire or fence
Vulnerabilities:	Tunneling, trenching, bridging

Concerns

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

Types of Tests

- Unaided Climb Test

  The test consists of an individual (preferably a small individual) climbing the fence at various locations to verify that detection occurs. Attempts should be made near fence posts, especially corners/posts.

- Ladder Climb Test

  A ladder is placed against the fence. An individual climbs the ladder to the point of sensor activation.

- Cutting Attack

  No actual cutting of the sensor wires or fence fabric should be performed.

- Jump Tests

  These tests cannot normally be conducted if a fence disturbance sensor is properly installed, due to the height of the detection zone (eight feet or more). However, adjacent structures used as platforms may permit an individual to jump over the fence/sensor wire, if personal safety can be ensured.

Test Guidelines

- All the unaided climb tests should be conducted on several fence posts in at least two typical zones.
- Zones that are substantially different (gates or different sensor configuration) should also be considered for testing.
- Areas that appear vulnerable to jumping should be tested to determine whether a vulnerability exists. Safety concerns should be addressed.
- If an individual sensor can be defeated, that same sensor should be tested again to determine whether the deficiency can be repeated. Several tests of the same sensor may be required to determine whether an adversary can reliably exploit the sensor deficiency.

- If an individual zone can be defeated, other zones should be tested using the same methods to determine the extent of the problem. The inspectors should conduct several (three to five) more tests in different zones. If most of these tests indicate that the sensors can be reliably defeated, it is likely that there is a systemic problem. If no other sensors are defeated, one may conclude that an isolated deficiency was identified. If the results are inconclusive, additional testing should be considered. Rarely would an inspector test more than 10 to 15 zones using the same methods.
- If the adversary has sufficient knowledge, time, and equipment, bridging or tunneling techniques can defeat all fence disturbance sensors. Such tests should only be conducted if a zone is particularly vulnerable (for example, due to barrier placement), or if patrol frequencies and direct visual observation (CCTV or from guard posts) are considered inadequate to provide reasonable assurance that such attempts are detected.

Checklist
Fence Disturbance Sensors
Exterior Perimeter Intrusion-Detection System
Interview Items

Installation location _____

_____

Operational test frequency _____

_____

Operational test method _____

_____

Sensitivity test frequency _____

_____

Sensitivity test method _____

_____

Acceptance criteria for sensitivity test _____

_____

False alarm history/records _____

_____

Make/model _____

_____

Measures to prevent erosion _____

_____

Tamper switches (transmitter, receiver, junction boxes) _____

_____

Tour/Visual Inspection Items

Vegetation present? _____

_____

Zone length OK? _____

_____

Complements other sensors? _____

_____

Overlap sufficient? _____

_____

Data Collection Sheet
Fence Disturbance Sensors – Exterior Perimeter Intrusion-Detection System

Test Method

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

This page intentionally left blank.

Part 2
Interior Sensors

This page is intentionally left blank

Part 2
Interior Sensors

Objective

The objective is to test the effectiveness of interior sensors in detecting adversary intrusion. The most directly applicable DOE requirements are given below.

Applicability	Order Reference
Category I and II SNM, Vital Equipment, Vital Areas, MAAs	DOE Manual 470.4-2 Ch1 Chapter VII, Paragraph 2
Classified Matter	DOE Manual 470.4-2 Ch1 Chapter VII, Paragraph 2
DOE Property and Unclassified Facilities	DOE Manual 470.4-2 Ch1 Chapter VII, Paragraph 2

System Tested

System - Intrusion-detection system

Functional Element - Interior intrusion detection

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

Scenario

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

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

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

ceilings, floors, windows, doors, and penetrations (for example, ductwork and cable chases).

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

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

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

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

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

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

Evaluation

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

Assessing Sensor Performance

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

- Do volumetric sensors detect an individual moving at a rate of 1 ft/sec or faster? (See "Assessing Sensor Performance," page A-4.)
- Do BMS sensors initiate an alarm when exposed to an external magnetic field or when the switch is moved one inch from the magnet housing?
- Does the sensor layout allow adversaries to circumvent any sensor(s) because of alignment, obstructions, or environmental interference?
- Are there any temporary entry points or penetrations to barriers that could allow undetected intrusion?

Interpreting Results

The following guidelines are provided to assist the inspector in interpreting evaluation results.

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

Special Considerations

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

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

Responsibilities

Inspectors: Select areas and sensors for testing. Direct tests and monitor alarm annunciation. Typically, one inspector will be located at the CAS/SAS and one will be with the test team.

Facility: Conduct routine tests. Provide security technicians. Provide test devices and aids, as required. Provide SPOs for security and radios for two-way communication. Provide personnel to conduct testing at the direction of inspectors.

Internal Coordination

Testing should be coordinated to minimize the impact on facility operations and should not result in undue exposure of test personnel to radiological or other health hazards. Testing should also be scheduled to avoid conflicts with other tests involving other topic teams (for example, the protective force topic team).

Security Considerations

All normal security precautions should be taken. Normally, an SPO should be present or observe testing to ensure there is no unauthorized access or activity at the protected location to be tested. In many cases, special security arrangements must be made before opening vaults or alarmed doors. These arrangements should be coordinated in advance to avoid delays during the testing.

Personnel Assignments

Test Director:

Facility Alarm System Point of Contact:

Facility Protective Force Representative:

Safety Coordinator:

Facility Safety Coordinator:

Logistical Requirements

Personnel:

- Protective force representative
- Alarm technician
- Testers
- SPOs to provide security during tests, as necessary

Equipment:

- Radios
- Test devices (for example, infrared target simulator, glass-break detector, audio source)

Safety:

- Follow normal operating procedures
- Complete a safety plan
- Notify the CAS/SAS before testing is conducted
- Station one inspector in the CAS/SAS
- Coordinate to prevent any undesired armed response to alarms by the protective force

Barrier Penetration Sensors

System Description:	BMS sensors, capacitance sensors, vibration sensors, and audio detectors; surface-mounted and coupled to a control device
Intruder Detection Capabilities:	Various, including physical proximity, forced opening, and physical attack using tools
Vulnerabilities:	Bypassing, tampering, substitution

Concerns

BMS Sensors:

- BMS sensors should have the switch mounted to a fixed surface, with the magnet mounted on the movable surface (door or window); capture or substitution of the magnet should be precluded.
- BMS sensors installed in areas posing a potential health hazard (for example, in radiation zones) should have self-checking test circuitry to eliminate the need for personnel to enter the hazardous area to check devices.
- BMS sensors should always be installed on the protected side of the barrier to preclude tampering.
- BMS sensors should be mounted with tamper-resistant hardware to reduce the potential for surreptitious removal.

Capacitance Sensors:

- The capacitance sensor wire or "blanket" should not make contact with any grounded object or surface. Other grounded objects in the vicinity of the protected barrier, or in the presence of liquids on floors or other nearby surfaces, can drastically alter sensor capacitance.
- Control units for capacitance sensors should be located within the protected space to preclude tampering.

Vibration Sensors:

- Vibration sensors should be mounted within or on the protected inner surface of the protected barrier.
- Because there are several types of vibration sensors (piezoelectric, coaxial cable, wire tension, and others), the particular manufacturer's specifications must be consulted to determine sensor detection capabilities and weaknesses.

Audio Detectors:

- Audio detectors must be calibrated carefully to avoid nuisance alarms caused by common background noises (for example, machinery, vehicles, and other alarm signals).
- Audio glass-break detectors should be positioned to face the window(s) they protect.

Types of Tests

- BMS Sensors

  BMS sensors should be tested by opening the protected portal (door, hatch, or window) sufficiently to create an alarm. In general, an opening of one inch or less should generate an alarm. A second test should be conducted by placing a magnet near the BMS. This should also create an alarm since the switch's magnetic field is being disturbed.

- Capacitance Sensors

  Capacitance sensors are tested by approaching the protected surface and making physical contact. An alarm should occur either upon near contact or actual physical contact with the surface.

- Vibration and Audio Detectors

  Because various technologies are employed, the particular manufacturer's performance testing procedures should be followed, and any specified testing devices should be used.

Test Guidelines

- At least two typical zones should be tested.
- Any zones that have potential vulnerabilities because of sensor configuration, location, or environmental or structural concerns should be tested to reveal any exploitable deficiencies.

Checklist
Barrier Penetration Sensors
Interior Sensors
Interview Items

Installation location _____

_____

Operational test frequency _____

_____

Operational test method _____

_____

Sensitivity test frequency _____

_____

Sensitivity test method _____

_____

Acceptance criteria for sensitivity test _____

_____

False alarm history/records _____

_____

Make/model _____

_____

Tamper switches (transceivers, control units, junction boxes) _____

_____

Tour/Visual Inspection Items

Unprotected/vulnerable entry points present? _____

_____

Sensor location adequate? _____

_____

Sensor coverage adequate? _____

_____

Sensor overlap sufficient? _____

_____

Sensor compatible with structural materials? _____

_____

Sensors compatible (if multiple sensors used)? _____

_____

Obstructions or nuisance alarm sources present? _____

_____

Control unit protected? _____

_____

Data Collection Sheet
Barrier Penetration Sensors – Interior Sensors

Test Method

	Zone Tested	Functional Test	Sensor Type	Alarm Generation Method
1 **2** **3** **4** **5** **6** **7** **8** **9** **10** **11** **12** **13** **14** **15**				
Comments:				

Area Motion Sensors

System Description:	Ultrasonic, microwave, or passive infrared sensor; wall- or ceiling-mounted; coupled to control device; volumetric coverage pattern
Intruder Detection Capabilities:	Walking, slow walking, or running
Vulnerabilities:	Bypassing coverage pattern, target masking, extremely slow movement

Concerns

General:

- Optimum coverage requires direct line of sight. Obstructions such as columns, beams, storage racks, or bins, furniture, or other large objects may prevent detection.
- Sensor transceivers and control units are subject to physical damage and tampering if they are not mounted to be inaccessible or are not covered by another sensor's detection pattern.
- Depending on the type used, sensors are susceptible to false alarms caused by moving objects (for example, fans), electromagnetic radiation, rapid temperature changes, air movement, seismic vibration, and background noise.
- Different sensor types have different coverage patterns (generally fan- or wedge-shaped). Proper overlap and coverage must be considered to ensure that an intruder cannot go over, around, or under the sensor's pattern of coverage.

Ultrasonic Sensors:

- Telephones, public address systems, alarm bells or sirens, and other loud sound sources can create nuisance alarms.
- Moving objects such as machinery, fans, venetian blinds or curtains, and wind-blown paper can create nuisance alarms.
- The sensor is less sensitive to a target moving across the detection zone.

Microwave Sensors:

- Moving objects such as machinery, fans, and venetian blinds or curtains can create nuisance alarms.
- The microwave detection beam can easily penetrate glass, wood, wallboard, and plastic (including water and drainpipes) creating false alarms from moving objects outside the protected space.
- Fluorescent light fixtures in the detection zone can create nuisance alarms.
- The sensor is less sensitive to a target moving across the detection zone, as opposed to moving toward or away from the sensor.
- The sensor is susceptible to masking (insider).

Infrared Sensors:

- Infrared will not penetrate any solid object, including glass. Movement in the area behind any objects in the detection pattern cannot be detected.
- Heat sources such as radiators, electrical motors, and direct sunlight can create nuisance alarms.
- Lights in the vicinity of the transceiver may attract insects thereby creating nuisance alarms.
- The sensor is less sensitive to a target moving toward or away from the sensor.
- The sensor is susceptible to masking (insider).

Video Motion Detection Cameras:

- Detection effectiveness will decrease if minimum light levels are not maintained. Lighting is necessary even when the area is unoccupied.
- The lighting for a video motion detection system must be on an emergency power supply to be effective during a power failure.
- Some video motion cameras allow the CAS operator to define the detection zone. If the defined zone is too small, detection probability may be decreased.
- Video motion detection cameras frequently have difficulty detecting slow-moving objects.
- Video motion detection cameras require direct line-of-sight with no obstruction. If the detection capability is not verified when placed in secure mode, the video motion sensors can be rendered ineffective by blocking the field of view or covering the lens when the system is in access mode.
- Camera can be manipulated to mask intrusions.

Types of Tests

- Sensitivity Walk Test

  Walk tests are used to verify operability and sensitivity of the sensor. This test is performed by slowly walking (1 ft/sec) toward ultrasonic and microwave sensors until an alarm is received. For infrared sensors, the inspector walks slowly across the detection pattern, starting at a point outside the detection zone and proceeding inward until an alarm is received. This test should establish the far end of the sensor coverage pattern (see "Assessing Sensor Performance," page A-4).

- Crossing Walk Test

  This test verifies the ability of the sensor to detect motion along the least sensitive axis of the detection pattern. After the end of the sensor coverage pattern is determined from a sensitivity walk test, a crossing test should be performed by walking across the far end of an ultrasonic or microwave zone and by slowly walking toward the infrared sensor from various points outside the detection zone. Detection should occur before the tester enters the defined protected space or reaches the protected target/object.

- Avoidance Walk Test

  Based on the sensor coverage pattern (oval, wedge, or circle), the inspector should attempt to enter the target zone from a likely entry point (for example, from a doorway, a heating/ventilation/air-conditioning duct, or other weak point in the barrier system) or by walking around the sensor's zone of coverage. This test should verify adequate sensor coverage and overlap to detect movement in the protected space or movement of the target/object.

- Crawl test may be useful, depending on location of detector.

Test Guidelines

- All sensor tests are conducted on the first attempt. If the tester fails to defeat the sensor, there are no second chances in that specific zone.
- To ensure performance test accuracy during an execution, all inactive bystanders in the sensor vicinity must remain still.
- During performance tests intervals, allow enough time between iterations for the sensitivity to rebalance
- Central alarm station operators should have effective communications with the inspector's escort to expedite sensor alarm and reset annunciation.
- Upon entering the room to be tested, and prior to testing, sufficient time should be allowed to pass for room temperature and airflow to normalize. Observers should be requested to stand away from the area being tested in order to reduce confusion.
- Testing should be conducted on at least two typical zones.
- Any zones that have potential vulnerabilities caused by obstructions or other sources of interference (for example, lighting, moving objects, noise, vibration, or heat sources) should be tested to determine whether exploitable deficiencies exist.
- If there are apparent weaknesses in zone coverage or sensor overlap, these should be tested to determine whether sensor coverage can be circumvented.
- Experience indicates that interior volumetric sensors are most vulnerable to a very slowly moving target entering the detection zone on the least sensitive axis (across the zones for ultrasonic and microwave sensors, and toward or away from infrared sensors).
- Many sensors have alarm indicator lights built into the sensor head. The inspectors may observe these indicators to facilitate testing the coverage patterns or sensor sensitivity. However, the inspectors should also verify that an alarm is received in the CAS/SAS to ensure that the alarm circuit is functional from sensor to annunciation point.

Checklist
Area Motion Sensors
Interior Sensors
Interview Items

Installation location _____

_____

Operational test frequency _____

_____

Operational test method _____

_____

Sensitivity test frequency _____

_____

Sensitivity test method _____

_____

Acceptance criteria for sensitivity test _____

_____

False alarm history/records _____

_____

Make/model _____

_____

Tamper switches (transceivers, control units, junction boxes) _____

_____

Tour/Visual Inspection Items

Unprotected/vulnerable entry points present? _____

_____

Sensor location adequate? _____

_____

Sensor coverage adequate? _____

_____

Sensor overlap sufficient? _____

_____

Sensor compatible with structural materials? _____

_____

Sensors compatible (if multiple sensors used)? _____

_____

Obstructions or nuisance alarm sources present? _____

_____

Control unit protected? _____

_____

Data Collection Sheet
Area Motion Sensors – Interior Sensors

Test Method

	Zone Tested	Zone Number	Sensitivity Walk	Crossing Walk	Avoidance Walk	Crawl
1						
2						
3						
4						
5						
6						
7						
8						
9						
10						
11						
12						
13						
14						
15						
Comments:						

Proximity Sensors

System Description:	Capacitance tuned circuit, point or proximity sensor, blanket or cable and contact configuration
Intruder Detection Capabilities:	Proximity/physical contact
Vulnerabilities:	Tampering with control unit

Concerns

- Some sensors experience "drift" in capacitance sensitivity over time and require regular sensitivity calibration.
- Sensors may be less effective at low temperatures and low sensitivity settings. Sensors are most reliable under temperature-controlled conditions.
- The capacitance sensor wire or "blanket" should not make contact with any grounded object or room surface. Other grounded objects close to the protected items, or liquids on the floor, may drastically alter the capacitance of the sensor.
- Control units for capacitance sensors should be located within the protected room or space to preclude tampering with sensitivity settings.

Types of Tests

- Capacitance sensors are tested by slowly approaching and physically touching the protected object with the hands. In an attempt to simulate an attempted compromise of this system, gloves should be worn to realistically desensitize the system. An alarm should be generated when in proximity to the object or upon physical contact.

Test Guidelines

- The person conducting the tests should remove all metal objects (radios, watch, coins, or a pocketknife) and should not wear steel-toed shoes. Gloves should be worn.
- Testing should be conducted on at least two typical zones.
- Any zones that have potential vulnerabilities (for example, extreme low temperature, surface water, or unprotected metal objects near the protected target) should be tested to reveal any exploitable deficiencies.

Checklist
Proximity Sensors
Interior Sensors
Interview Items

Installation location _____

_____

Operational test frequency _____

_____

Operational test method _____

_____

Sensitivity test frequency _____

_____

Sensitivity test method _____

_____

Acceptance criteria for sensitivity test _____

_____

False alarm history/records _____

_____

Make/model _____

_____

Tamper switches (transceivers, control units, junction boxes) _____

_____

Tour/Visual Inspection Items

Sensor location adequate? _____

_____

Standing water present? _____

_____

Grounded objects in proximity to protected object? _____

_____

Control unit protected? _____

_____

Complements other sensors? _____

_____

Data Collection Sheet
Proximity Sensors – Interior Sensors

Test Method

	Zone Tested	Zone Number	Approach and Touch
1 **2** **3** **4** **5** **6** **7** **8** **9** **10** **11** **12** **13** **14** **15**			
Comments:			

This page is intentionally left blank

Part 3

Perimeter CCTV

This page is intentionally left blank

Part 3:
Perimeter CCTV

Objective

The objective is to test the effectiveness of perimeter CCTV systems for providing surveillance and assessment of ground-based intrusions. The most directly applicable requirements are:

Applicability	Order Reference
Category I and II SNM, Vital Equipment, PAs	DOE Manual 470.4-2 Ch1 Chapter V, Paragraph 3
Classified Matter, LAs	DOE Manual 470.4-2 Ch1 Chapter V, Paragraph 3
DOE Property and Unclassified Facilities	DOE Manual 470.4-2 Ch1 Chapter V, Paragraph 3

System Tested

System - Assessment system

Functional Element - Perimeter/exterior CCTV

Components - CCTV cameras, enclosures, towers, transmission lines, interface with intrusion-detection system, and CAS/SAS switching and displays, testing and maintenance of exterior CCTV, lighting

Scenario

During an initial site tour, inspectors should select various CCTV zones for testing, usually in conjunction with the exterior intrusion-detection system test. Zone selection is based on a number of factors, including CCTV layout, fence line and intrusion-detection system layout, perimeter lighting, visual obstructions such as buildings and manmade structures, terrain and vegetation, and system operating history. The objective of the site tour is to identify potential problems created by irregular terrain (ditches, humps, dips), obstructions that block the view of a camera or create strong shadow effects, poor security lighting, poor camera placement or alignment, or improper integration of camera zones with intrusion-detection system zones.

The inspectors should observe the facility's CCTV technicians and SPOs conducting routine operational and calibration tests of CCTV cameras and associated equipment, if possible. Cameras are identified for testing based on the number, type, configuration, and operating history. Test, calibration, and maintenance procedures are observed to determine whether they are consistent with DOE orders and approved SSSPs and if they are an effective means of verifying proper system operation. Although it is desirable to observe these activities to determine system status and test and maintenance effectiveness, such tests should not be required if they are not part of the normally scheduled system checks.

The inspectors should conduct individual camera testing during both daylight and darkness and, if practicable, at either sunset or sunrise. This is important to verify that the cameras function properly

throughout the full range of lighting conditions. Testing generally consists of run tests across the isolation zone between the outer and inner perimeter fence lines to determine whether the automatic camera call-up, following intrusion-detection system activation, is rapid enough to allow observation of an intruder within the camera field of view. In addition, testing is conducted at the far end of the field of view to verify that camera lens selection provides a discernable image at the maximum viewing distance. Other tests are conducted where features of terrain, obstruction, or lighting indicate that CCTV coverage may not be effective. The purpose of these tests is to determine whether an adversary could cross the perimeter isolation zone, or remain in that zone, without being observed.

The inspectors should monitor the camera displays in the CAS and/or SAS, and observe operation of supporting subsystems, such as camera switching, sequencing, video recording, pan-tilt-zoom (PTZ) control, and date/time generation, if used. The inspectors should also observe the interfacing of systems, including automatic call-up of CCTV upon intrusion-detection system activation, CAS/SAS operator actions, and control and direction of response forces based on CCTV assessment of adversary actions.

The number of camera zones selected for testing depends on the time available, the importance of CCTV in the overall assessment system, and the number of potential deficiencies identified during the site tour. The following guidelines are intended to assist the inspector in selecting zones for testing:

- Normally, a minimum of two camera zones should be tested in conjunction with the perimeter intrusion-detection system test. If zone camera configurations vary (for example, cameras facing one another versus cameras that follow in sequence) or if automatic camera call-up differs because of changes in the intrusion-detection system sensors used, a representative sample of each configuration type should be tested.
- If a variety of cameras and camera lenses are employed, a representative sample should be tested.
- If PTZ cameras are used for perimeter surveillance, at least one of these should be checked, particularly if it is the type that automatically shifts to a preset field of view upon intrusion-detection system activation. PTZ cameras should not be the primary means of assessment in a PIDAS.
- If special application cameras are used (for example, very low light level or infrared), at least one should be tested.
- Tests should be conducted for selected zones in which deficiencies are anticipated due to terrain, vegetation, obstructions, or lighting conditions.
- If the initial tests do not indicate problems, and the camera scenes displayed at the CAS/SAS appear to be generally clear and uniform, the inspectors need not test numerous cameras. However, if deficiencies are apparent, the inspectors should collect sufficient data to determine whether the weakness is an isolated problem or a systemic deficiency.
- Tests should be conducted to evaluate speed of camera call-up and assess if any vulnerabilities exist as a result.

Evaluation

The purpose of a CCTV assessment system is to support the intrusion detection and response functions by promptly and accurately assessing alarms (to include verification of nuisance and false alarms), determine adversary actions, and direct protective forces response. The principal factor in evaluating the CCTV system is whether it effectively and reliably provides prompt and complete observation of the perimeter isolation zone, and particularly the area adjacent to the inner perimeter fence line in any

zone from which an alarm is received. Other factors to consider in the evaluation are:

- Is the CCTV system the sole or primary means of assessment and observation, or do SPOs observe the perimeter? System requirements (such as automatic camera call-up) vary depending upon the degree of reliance on CCTV.
- Does the camera layout provide complete coverage of the perimeter or are there gaps that could be exploited by an adversary?
- Are there terrain irregularities, visual obstructions, shadows, or lighting deficiencies that create exploitable weaknesses in the camera coverage?
- Does the CAS/SAS display function of the CCTV system adequately support the assessment requirement in terms of speed of camera call-up, resolution, size of monitor display, and video recording, as applicable to system configuration and the availability of other assessment aids?
- Is the CCTV equipment capable of performing properly in all light conditions, day or night?
- Are the monitor displays (if any) in security towers or other guard posts functional and effective for their intended purpose?
- Are environmental concerns adequately addressed for all expected climatic conditions in terms of environmental enclosures, heaters, blowers, wipers, and other such devices?

Interpreting Results

The following guidelines are provided to assist inspectors in interpreting results in the context of overall system performance:

- As with other security elements, a perimeter CCTV system is only as strong as its weakest link. Tests that indicate that an adversary can cross a camera zone without observation, following intrusion-detection system activation, are evidence that the CCTV assessment system is not fully reliable. The significance of this finding must be analyzed in the context of the site-specific protection objectives and the effectiveness of other assessment aids.
- In some cases, facility tests indicate that visual obstructions, lighting deficiencies, or other weaknesses exist in individual camera zones. However, the capability to assess perimeter alarms remains because of partial coverage from an adjacent camera or from direct visual observation. In such cases, the deficiencies are of lesser concern because other assessment aids provide compensation. However, these deficiencies may indicate problems in system design or in the test and maintenance program. Testing and maintenance deficiencies may be attributed to inadequate maintenance procedures, insufficient attention to reported problems, or incomplete procedures for reporting CCTV failure or degradation.
- Facility tests that indicate that cameras are properly calibrated and aligned, in conjunction with tests conducted by inspectors that indicate an intruder can be effectively observed, are evidence that tested portions of the system are operational and maintenance procedures are effective. However, facility tests do not ensure that all modes of defeat have been assessed or that all weather and lighting conditions have been evaluated to maximally stress the system.
- Facility tests that indicate that individual cameras are not operating in accordance with the manufacturer's specifications may simply be an indicator of isolated equipment degradation. However, such deficiencies may be evidence of a system-wide weakness in the maintenance program or a failure of system components due to age. Most camera image tubes have a predictable useful life, after which rapid degradation and failure can be expected. If all of the cameras in the system were installed at the same time, it is likely that camera failures will occur in rapid succession throughout the system. Life

cycle planning for the maintenance and replacement of equipment is required to avoid this and should be documented in maintenance procedures.

Special Considerations

Some sites employ specialized camera equipment, such as video motion detection systems or very low-light-level cameras that have special test requirements. In such cases, inspectors should be sure to familiarize themselves with the manufacturer's instructions for operation, test, and maintenance of the equipment.

Special attention should be paid to nighttime lighting conditions, including shadowed areas and the effects of transient lighting changes due to vehicle headlights and opening of doors. To increase the efficiency of the data-gathering effort, CCTV testing should be integrated with related inspection activities, such as barrier inspections, intrusion-detection system testing, and checks of tamper and line supervision alarms.

Responsibilities

Inspectors: Select cameras for testing. Direct testing and monitor video displays and recording. Typically one inspector will be stationed at the CAS and at least one at the perimeter.

Facility: Conduct routine testing. Provide technicians and test devices, as necessary. Provide radios for two-way communications. Provide security compensatory measures, as required. Provide personnel (normally an SPO) to conduct zone testing at the direction of inspectors.

Internal Coordination

Testing should be scheduled to avoid conflicts with exercises or activities involving other topic teams (primarily the protective force topic team). Daytime testing is typically conducted concurrently with the perimeter intrusion-detection system testing.

Security Considerations

All normal security considerations should be observed. Normally, an SPO must monitor (directly or using CCTV) test activity to ensure that no unauthorized personnel enter the PA.

Personnel Assignments

Test Director:

Facility CCTV System Point of Contact:

Facility Protective Force Representative:

Inspection Team Safety Coordinator:

Facility Safety Coordinator:

Logistical Requirements

Personnel:

- Protective force representative
- CCTV technicians
- Tester

Equipment:

- Radio
- Contrasting clothing for nighttime tests

Safety:

- Follow normal operating procedures
- Complete a safety plan
- Notify the CAS/SAS before testing is conducted
- Station one inspector in the CAS
- Coordinate prevention of any armed response in the area of test personnel

Perimeter CCTV Testing

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

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

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

Concerns

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

- PTZ cameras should have limit switches to preclude their facing directly into bright light sources. Also, if they are called up by intrusion-detection system activation, they should be programmed to automatically position themselves to view the area from which the alarm was received.

Types of Tests

- Functional Test

  A functional test of each camera should be performed from the CAS/SAS by calling up each camera scene to verify that cameras are operating and that a clear image is received. If multiple monitors are used for continuous display (for example, nine-inch sequenced monitors) inspectors should verify their function and sequencing (if employed). Check all PTZ functions for proper operation. Also check video-recording systems.

- Field-of-View Test

  In conjunction with the perimeter intrusion-detection system test, inspectors should conduct field-of-view tests if the far point of the camera field of view appears to be excessively long (that is, a clear image of an intruder cannot be seen at the far end of the camera's field of view). To conduct this test, a person should be positioned at the far end of the field of view and should slowly walk across the isolation zone. This test should also verify that the inner perimeter fence line is within the field of view of each camera that observes the isolation zone.

- Obstruction Test

  A test should be conducted when an identified obstruction or shadow may preclude effective observation. This test is conducted by having a person run to and hide behind the obstruction or in the shadowed area.

- Speed of Response Test

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

Test Guidelines

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

Checklist
Exterior Perimeter CCTV System
Interview Items

Installation location _____

_____

Operational test frequency _____

_____

Operational test method _____

_____

Calibration test frequency _____

_____

Calibration test method _____

_____

Acceptance criteria for calibration test _____

_____

Make/model _____

_____

Environmental protection equipment _____

_____

Special equipment (recorders, PTZ cameras) _____

_____

Maintenance history/records _____

Mounting method (tower, pole, wall)

Tamper switches (transmitter, receiver, junction boxes)

Tour/Visual Inspection Items

Obstructions present? _____

_____

Shadows present? _____

_____

Terrain level? _____

_____

Zone length OK? _____

_____

PTZ cameras, other cameras? _____

_____

Overlap sufficient? _____

_____

Mounting towers/poles rigid? _____

_____

Lighting adequate? _____

_____

Environmental housings adequate? _____

_____

Data Collection Sheet
Exterior Perimeter CCTV System

Test Method

	Zone Tested	Functional Test	Field of View Test	Obstruction Test	Speed of Response Test
1					
2					
3					
4					
5					
6					
7					
8					
9					
10					
11					
12					
13					
14					
15					
Comments:					

This page is intentionally left blank

Part 4
Interior CCTV Performance Tests

This page is intentionally left blank

Part 4
Interior CCTV Performance Tests

Objective

The objective is to test the effectiveness of interior CCTV systems in providing surveillance and assessment of intruder movement and actions.

(Note: CCTV cameras that are physically located outside but cover the exteriors of portals or emergency exits are included within the scope of this performance test.)

The most directly applicable DOE requirements are:

Applicability	Order Reference
Category I and II SNM	DOE Manual 470.4-2 Ch1 Chapter V, Paragraph 3
Classified Matter	DOE Manual 470.4-2 Ch1 Chapter V, Paragraph 3
DOE Property and Unclassified Facilities	DOE Manual 470.4-2 Ch1 Chapter V, Paragraph 3

System Tested

System - Assessment system

Functional Element - Interior CCTV

Components - CCTV cameras, enclosures, mounts, transmission lines, interface with the intrusion-detection system and the CAS/SAS, switching and displays, and testing and maintenance of the interior CCTV

Scenario

The inspectors should select various CCTV zones for testing, usually in conjunction with interior intrusion-detection system tests, during an initial facility tour. Zone selection is based on a number of factors, including CCTV layout, intrusion-detection system configuration, interior lighting, and operating history of the cameras. The inspectors should review building layouts, architectural drawings, and briefly tour the facility to familiarize themselves with the location of protected spaces in relation to camera coverage. This tour should reveal potential problems created by camera placement, visual obstructions, poor lighting, and improper camera alignment.

The inspectors should observe, whenever possible, the facility's CCTV technicians and SPOs as they conduct routine operational and calibration tests of CCTV cameras and associated equipment. Cameras are selected for testing according to the number, type, configuration, and operating/maintenance history of the units in the system. Test, calibration, and maintenance procedures are observed to determine whether they are consistent with DOE orders and approved SSSP requirements, and whether they are an effective means of verifying proper system operation.

The inspectors should conduct individual camera testing during daylight and darkness and, if practical, verify that cameras function properly throughout the full range of light conditions. Testing generally consists of walk tests within various camera zones to determine whether coverage allows observation of an intruder within the camera's field of view. In addition, testing should be conducted at the most distant end of the field of view to verify that the camera lens provides a discernable image at the maximum viewing distance. Other tests are conducted where camera placement, alignment, obstructions, or lighting conditions indicate that CCTV coverage may not be effective. The purpose of these tests is to determine whether an adversary could enter, exit, or remain within a protected space without being observed.

Inspectors should monitor the camera displays in the CAS and SAS, to observe the operation of supporting subsystems, such as camera switching, sequencing, video recording, PTZ control, and date/time generation. The inspectors should also observe the interfacing of systems, including automatic call-up of CCTV upon intrusion-detection system activation, CAS/SAS operator actions, and control and direction of response forces based on CCTV assessment of adversary actions.

The number of camera zones selected for testing depends on the time available, the importance of CCTV in the overall assessment system, and the number of potential deficiencies identified during the site tour. The following guidelines are intended to assist the inspector in selecting zones for testing:

- A minimum of two camera zones should be tested, normally in conjunction with the interior intrusion-detection system test. If camera configurations vary or if automatic camera call-up differs because of changes in the intrusion-detection system sensors used, a representative sample of each type of configuration should be tested.
- If a variety of camera lenses and focal lengths are employed, a representative sample should be tested.
- If interior PTZ cameras are used, inspectors should check at least one, particularly if it is one that automatically shifts to a preset field of view upon intrusion-detection system activation.
- If special-application cameras are used (for example, very-low-light-level, video motion detection, or infrared), at least one should be tested.
- Inspectors should conduct tests on cameras for which deficiencies are anticipated because of configuration, alignment, obstructions, or light conditions.
- If initial tests do not indicate problems, and the camera scenes displayed at the CAS/SAS appear to be generally clear and uniform, the inspectors need not test numerous cameras. However, if deficiencies are apparent, the inspectors should collect sufficient data to determine whether the weakness is isolated or systemic.
- Procedures should be in place to assure that no obstructions can be placed in the "assessment area" (if none, test to see if boxes or objects can be placed).

Evaluation

The purpose of a CCTV assessment system is to support the intrusion-detection and response functions by promptly and accurately assessing alarms (to include verifying nuisance and false alarms), determine adversary actions, and direct protective force response.

Assessing System Effectiveness

The principal objective in evaluating the CCTV system is to determine whether it effectively and reliably provides prompt and adequate observation of the protected space and the principal entry points. The following points should be considered in the evaluation:

- Is the CCTV system the sole or primary means of assessment and observation, or do SPOs provide visual observation of the area? System requirements (such as automatic camera call-up) vary, depending on the degree of reliance on CCTV.
- Does the camera layout provide complete coverage or are there gaps that could be exploited by an adversary?
- Are there visual obstructions and procedures or lighting deficiencies that create exploitable weaknesses in the camera coverage?
- Does the CAS/SAS display function of the CCTV system adequately support the assessment requirement? Aspects to consider include the speed with which cameras are called up, resolution and size of monitor displays, and video recording.
- Is the CCTV equipment capable of performing properly in all light conditions, day or night?
- Are the monitor displays (if any) at guard posts functional and effective for their intended purpose?
- Are all essential cameras in the system functional (or compensatory measures in place)?

Interpreting Results

The following guidelines are provided to assist inspectors in interpreting results in the context of overall system performance:

- Testing that indicates that an adversary can cross a camera zone unobserved following intrusion-detection system activation is evidence the CCTV assessment system is not fully reliable. The significance of this deficiency must be analyzed in the context of the site-specific protection objectives and the effectiveness of other assessment aids.
- In some cases, facility testing indicates that there are visual obstructions, lighting deficiencies, or other weaknesses in individual camera zones. However, the capability to assess intrusion-detection system alarms remains because of partial coverage from an adjacent camera or direct visual observation. Although these weaknesses are less serious because of these compensatory measures, they may indicate problems in system design or the test and maintenance program. Test and maintenance deficiencies may be attributed to inadequate maintenance procedures, insufficient attention to reported problems, or incomplete procedures for reporting CCTV failure or degradation.
- Facility testing that indicates cameras are properly calibrated and aligned in conjunction with inspection team testing that indicates an intruder can be effectively observed, is evidence that tested portions of the system are operational and that maintenance procedures are effective. However, such tests do not ensure that all modes of defeat have been assessed or that all conditions have been evaluated.
- Facility testing that indicates individual cameras are not operating in accordance with the manufacturer's specifications may simply be an isolated instance of equipment degradation. However, such deficiencies may also be evidence of a system-wide problem regarding the maintenance program or component aging. Most camera image tubes have a predictable useful life, after which rapid degradation followed by failure can be expected. If all the cameras in the system were installed at the same time, it is likely that camera failures will occur in rapid succession throughout the system. To avoid this multiple failure

problem, life cycle planning for the maintenance and replacement of equipment is required, the written details of which should be included in the facility maintenance procedures.

Special Considerations

Some sites employ specialized camera equipment, such as video motion detection systems or very-low-light-level cameras, which have special test requirements. For such equipment, inspectors should familiarize themselves with the manufacturer's instructions.

Special attention should be paid to nighttime and after-hours lighting conditions, including shadowed areas and the effects of transient lighting changes due to vehicle headlights, opening of doors, or other light sources.

Has the system been reviewed for classification? How is the video protected from unauthorized access?

To increase the efficiency of the data-gathering effort, CCTV testing should be integrated with related inspection activities, such as barrier inspections, intrusion-detection system tests, and checks of tamper and line supervision alarms.

Responsibilities

Inspectors: Select cameras for testing. Direct testing and monitor video displays and recording. Typically, one inspector will be stationed at the CAS and at least one with the test team.

Facility: Conduct routine testing. Provide technicians and test devices, as necessary. Provide radios for two-way communications. Provide for security compensatory measures, as required. Provide personnel (normally an SPO) to conduct zone tests at the direction of the inspectors.

Internal Coordination

Testing should be scheduled to avoid conflicts with the activities and performance tests conducted by other topic teams (primarily the protective force topic team). Testing typically should be conducted concurrently with interior intrusion-detection system tests.

Security Considerations

All normal security considerations should be observed. Normally, an SPO must monitor (directly or via CCTV) test activity to ensure that no unauthorized personnel enter protected spaces.

Personnel Assignments

Test Director:

Facility CCTV System Point of Contact:

Facility Protective Force Representative:

Safety Coordinator:

Facility Safety Coordinator:

Logistical Requirements

Personnel:

- Protective force representative
- CCTV technicians
- Tester

Equipment:

- Radio

Safety:

- Follow normal operating procedures
- Complete a safety plan
- Notify the CAS/SAS before conducting any test
- Station one inspector in the CAS
- Arrange to prevent any undesired armed protective force response

Interior CCTV Testing

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

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

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

Concerns

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

Types of Tests

- Functional Test

  A functional test of each camera should be performed from the CAS/SAS by calling up each camera scene to verify that all cameras are operating and that a clear image is received. If multiple monitors are used for continuous display, their function and sequencing (if employed) should be verified. Any PTZ functions should also be checked for proper operation, as should video-recording systems.

- Field-of-View Test

  In conjunction with the interior intrusion-detection system test, field-of-view testing should be conducted if the far point of the camera's field of view appears to be excessively long (that is, a discernible image of an intruder cannot be obtained at the far end of the camera field of view). To conduct this test, a person should be positioned at the far end of the field of view and should walk slowly

across that field of view. In general, this test should also verify that critical access portals are within the camera's field of view.

- Obstruction Test

  A test should be conducted whenever an obstruction and/or lighting conditions could preclude effective observation. This test is conducted by having a person hide behind the obstruction or in a darkened area.

- Speed of Response Test

  To test for speed of camera response when automatic call-up of a camera upon intrusion-detection system activation is employed, a person should activate an interior sensor and then attempt to rapidly exit the area covered by the camera. This test is used to verify that automatic camera call-up and/or video recording is rapid enough to allow observation before the intruder can leave the camera's field of view.

Test Guidelines

- All the foregoing tests should be conducted under day, night, and overcast conditions to ensure that the cameras can function in all light conditions, as applicable.
- At a minimum, test at least two camera zones, if possible.
- Conduct obstruction tests whenever functional testing indicates that the assessment capability in a camera zone is significantly degraded by an obstruction.
- If a significant number of camera zones (more than ten percent) exhibit degraded picture quality, maintenance records should be reviewed to determine whether useful camera life limits have been exceeded because camera image tubes have not been replaced.

Checklist
Interior CCTV System
Interview Items

Installation location _____

_____

Operational test frequency _____

_____

Operational test method _____

_____

Calibration test frequency _____

_____

Calibration test method _____

_____

Acceptance criteria for calibration test _____

_____

Make/model _____

_____

Camera mounting hardware _____

_____

Special equipment (recorders, low-light-level or PTZ cameras) _____

_____

Maintenance history/records _____

_____

Tamper switches (transmitter, receiver, junction boxes) _____

_____

Tour/Visual Inspection Items

Obstructions present? _____

_____

Zone length OK? _____

_____

PTZ cameras, other cameras? _____

_____

Overlap sufficient? _____

_____

Mounting adequate? _____

_____

Lighting adequate? _____

_____

Data Collection Sheet
Video – Interior CCTV

Test Method

	Zone Tested	Functional Test	Field of View Test	Obstruction Test	Speed of Response Test
1					
2					
3					
4					
5					
6					
7					
8					
9					
10					
11					
12					
13					
14					
15					
Comments:					

This page is intentionally left blank

Part 5
Alarm Processing and Display

This page is intentionally left blank

Part 5
Alarm Processing and Display

Objective

The objective is to test the effectiveness of alarm processing, annunciation and display at alarm stations. The applicable DOE references are:

Applicability	Order Reference
Category I and II SNM	DOE Manual 470.4-2 Ch1 Chapter V, Paragraph 1 & 2
Classified Matter	DOE Manual 470.4-2 Ch1 Chapter V, Paragraph 1
DOE Property and Unclassified Facilities	DOE Manual 470.4-2 Ch1 Chapter V, Paragraph 1

System Tested

System - Alarm station functions

Functional Element - Alarm processing and display equipment

Components - Alarm monitors and displays, alarm printers, recording devices, annunciator panels, related equipment controls, switchers, and equipment testing and maintenance

Scenario

Alarm processing and display equipment encompasses the entire annunciation, monitoring, and display equipment and devices employed at the CAS/SAS. This equipment is used to monitor and record the activity associated with all other active subsystems in the security system including: CCTV, intrusion-detection systems, tamper and line supervision alarms, emergency power supplies, communications equipment, access controls, and search equipment.

Since alarm processing and display functions are directly related to the operation of other subsystems, a specific test of such functions is not conducted. Rather, the inspectors note the effectiveness of displays and annunciations at the CAS/SAS in the course of conducting other tests on intrusion detection, access controls, and other systems. The alarm processing and display functions to be tested depend upon the types of security subsystems in use and the types of annunciation/display equipment used at the CAS and SAS. The inspectors should review building layouts and security system drawings and tour the facility to familiarize themselves with systems configuration and operations so as to effectively evaluate systems annunciation and display capabilities.

While conducting individual subsystems tests, the inspectors note the effectiveness of annunciation and display of alarms, camera scenes, or status indication for the following subsystems or components:

- interior and exterior intrusion-detection system alarms
- line supervision and tamper-indication alarms

- CCTV display monitors and recording devices
- biometric and/or card access controls
- search equipment (SNM detectors, metal detectors), if appropriate
- power supplies
- activated barriers (smoke, foam)
- remotely operated vehicle barriers and gates.

Any components used to maintain a historical record of alarms, displays, or status indication are also to be reviewed. These include alarm logs maintained by computer memory or on storage media (computer tapes or disks), computer printouts, chart recorders, or video recordings, as appropriate.

Inspectors must also verify that the SAS is properly equipped and operated to serve as a completely functional backup to the CAS. The SAS need not be fully redundant with the CAS (that is, alarm processing and display equipment need not be identical), but it must be capable of performing all required alarm response functions. At some facilities, an alarm condition is annunciated in the SAS only if the CAS operator fails to acknowledge it within a prescribed period. Inspectors may elect to verify the operation of such an alarm annunciation capability.

The following guidelines are intended to assist the inspector in selecting items of equipment for testing:

- Evaluate at least one example of each type of annunciation device, display, status indicator, control device, or recording/logging device, if possible.
- Verify that the system functions under emergency power supply conditions and shows no degradation of alarm processing and display.
- Evaluate CCTV system displays and video-recording capability under conditions of both daylight and darkness.

Evaluation

The purpose of alarm processing and display functions is to ensure the capability of the CAS/SAS to control, monitor, and respond to all components of the facility security systems. These functions directly support the requirements to promptly and accurately assess alarms, provide personnel access controls, determine adversary actions, and direct protective force response.

Assessing System Effectiveness

The principal objective in evaluating the alarm processing and display system is to determine whether it effectively and reliably provides prompt and adequate control and monitoring of critical security systems. Other points to consider in the evaluation are:

- Do all alarms provide clear audible and visual annunciation/display?
- Are there provisions to call the CAS/SAS operator's attention to an alarm-associated camera display?
- Does the monitoring equipment provide for straightforward and easy acknowledgment of all alarms?
- Is the status of all power supplies (normal AC, batteries, and generators) clearly indicated at all times?
- Are video displays and recordings clear and available at the CAS and SAS?

- Are line-supervision and tamper-indication alarms clearly displayed and distinguished from other alarm conditions?
- Are alarm processing and display equipment adequately protected against tampering or physical attack?
- Are scheduled testing and maintenance performed on all alarm processing and display equipment?
- Are invalid or unauthorized keycard (or biometric) access attempts promptly and clearly annunciated?
- Does the system provide a historical log of all keycard or biometric access transactions?
- Are controls for security lighting and emergency power available at the CAS and SAS?
- Are there provisions to ensure that the SAS operator is aware of changes in the status of intrusion-detection systems (for example, from secure to access)?
- Are records of false and nuisance alarms maintained by the system?

Interpreting Results

The following guidelines are provided to assist inspectors in interpreting results in the context of overall system performance:

- The types of alarm processing and display systems in use at DOE contractor facilities vary considerably. This is due to differences in the ages of the systems, the degree of computerization employed, and the size and sophistication of the total site security system. Therefore, considerable judgment must be used in evaluating system effectiveness. The key factors considered are whether displays are prompt, clearly annunciated, and understandable. Human factor concerns are important in determining whether an operator can effectively interact with the system to assess and respond to annunciations and displays.
- Another critical factor in evaluating system adequacy is the ability of the SAS to function as an effective backup to the CAS. In determining this adequacy, the inspector should assess whether the SAS can function in a stand-alone mode to completely and effectively monitor, control, and respond to all critical security system functional elements.

Special Considerations

For those sites that use computer-based alarm processing and display systems, it may be necessary to interview the systems analyst or programmer responsible for system software. Some system anomalies may be due to hardware defects or may be the result of programming errors. Another problem relative to computer-based alarm systems is the control of software and its protection against the insider threat. This problem is such that it requires management support and oversight at the highest level possible.

For CCTV system displays and recorders, testing under conditions of both daylight and darkness is required to evaluate system effectiveness.

In the interest of efficiency in data gathering, system testing should be conducted in conjunction with testing scheduled for CCTV, intrusion-detection systems, access controls, emergency power supplies, and other subsystems of the site security system.

Responsibilities

Inspectors: Select systems for testing. Direct testing and monitor annunciation, displays, and recordings. (Typically, one inspector will be stationed at the CAS and at least one with the test team.)

Facility: Conduct routine tests. Provide technicians and test devices as necessary. Provide radios for two-way communication. Provide security compensatory measures, as required.

Internal Coordination

- Conduct testing concurrently with and as an aspect of other system tests.
- Observe all normal security considerations.

Personnel Assignments

Test Director:

Facility System Point of Contact:

Facility Protective Force Representative:

Safety Coordinator:

Facility Safety Coordinator:

Logistical Requirements

Personnel:

- Protective force representative
- Technicians
- Tester
- Systems analyst or programmer

Equipment:

- Radio

Safety:

- Follow normal operation procedures
- Complete a safety plan
- Notify the CAS/SAS before conducting testing
- Station one inspector in the CAS or SAS
- Test personnel should arrange to prevent any undesired armed protective force response

Alarm Processing and Display Equipment

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

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

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

Concerns

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

Types of Tests

- Function Test

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

- Historical Record Test

  Evaluate any historical records maintained by the system (for example, alarm logs, access control transaction histories, and video recordings) for completeness and accuracy. False and nuisance alarm rates may also be assessed by reviewing these records.

- SAS Test

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

Test Guidelines

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

Checklist
Alarm Processing and Display Equipment
Interview Items

Installation location(s) _____

_____

Operational test frequency _____

_____

Operational test method _____

_____

System acceptance criteria _____

_____

Makes/models (CCTV display/recorders, alarm annunciation, card access control) _____

_____

Maintenance history/records _____

_____

CAS/SAS physical protection measures _____

_____

Tour/Visual Inspection Items

Physical protection adequate? _____

_____

Environmental controls/fire protection adequate? _____

_____

Operator's console and controls layout accessible and functional? _____

_____

All displays clear and readable? _____

_____

SAS equipment sufficient? _____

_____

Records storage adequate? _____

_____

Sound level sufficient? _____

_____

Data Collection Sheet
Alarm Processing and Display Equipment

Test Method

	Location Tested (CAS/SAS, Other)	Device/Equipment Tested	Function Tested	Type of Test (Functional Test, Historical Record Test, SAS Test)
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				
13				
14				
15				
Comments:				

This page is intentionally left blank