

Section 7

TESTING AND MAINTENANCE

Contents

References	7-1
General Information	7-1
Common Deficiencies/Potential Concerns.....	7-2
Planning Activities.....	7-2
Performance Tests.....	7-3
Data-Collection Activities.....	7-3

References

DOE Order 5632.1C

General Information

All PSSs require the support of a comprehensive testing and maintenance program. These programs represent one of the most important aspects of the systems topic, and serve to ensure that each systems 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. In the event that the systems fail, compensatory measures must be implemented. Further, the people who test, maintain, or service alarms are required to have clearances consistent with the highest classification levels being protected, unless such testing and maintenance is performed as bench services away from the protected location, or is performed 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 testing that provides a 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. This includes protective force personnel who are tested for performance.

Details on testing personnel and procedures are found in Appendix E. 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 is required to 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 will 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
- 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.

The results of both the effectiveness tests and the operability tests shall 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. When this situation exists, inspectors should examine the program documentation to determine whether it is complete and whether it provides enough detail to ensure program effectiveness.

Frequently, protective personnel are improperly or inadequately trained for testing the systems for which they are responsible. Many times, members of the protective force will 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 also applies to the many test objects used for testing other search equipment on which SPOs routinely rely.

Sometimes compensatory measures that are required when critical components are out of service are not adequate to ensure equivalent protection.

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

Records reflecting the results of both the effectiveness tests and the operability tests are not 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 of the 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. The inspectors should ask questions such as who originated the request, how and when did the request get to the maintenance department, how was it scheduled, and who verified that the work was accomplished?

B. Inspectors should determine the role of vendors or outside companies in 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, there are quality assurance features 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 limited areas (or other security areas), inspectors should review the DOE-approved security plans to determine whether site-specific requirements for tests and maintenance of alarm systems are being 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 the procedures are clear and

complete, whether they have been reviewed and approved, and whether all organizations have procedures specific to their duties (for example protective forces 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. This may be accomplished separately or in conjunction with performance tests.

G. Inspectors should review reports developed as part of the quality assurance (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 the QA reviews. Occasionally, the resolution process fails to adequately correct problems and will result in a superficial treatment rather than an in-depth remedy.

H. Testing or maintenance that is not performed or is performed late is an indication of inadequate staff or lack of management attention. Extended periods in which equipment awaits repair is another. Testing and maintenance should also be reviewed to determine whether the security managers have the ability to 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 the security technicians do not report directly to security managers, the 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 also review the training and qualifications of security technicians. The inspectors can review resumes and records of formal training and determine how in-house training is handled.

Equipment Performance

J. The best indicator of the quality of the testing and maintenance program is equipment performance. 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 test, scheduled maintenance, and calibration records to verify whether these activities are conducted as scheduled and that records are maintained as required. Typically, inspectors would 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; whereas, 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 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. The inspectors 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 work was initiated
- Dates work was completed and names of personnel accomplishing task
- Verification that work was completed and closeout tests were conducted.

With this process the 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 is intentionally left blank.