

Section 11

ANALYZING DATA AND INTERPRETING RESULTS

Contents

Introduction	11-1
Analysis of Results.....	11-1
Ratings	11-2
Interpreting Results	11-2
Exterior Intrusion Detection and Assessment	11-3
Interior Intrusion Detection and Assessment	11-3
Entry and Search Control/Badges, Passes, and Credentials	11-3
Barriers	11-4
Communications.....	11-4
Testing and Maintenance.....	11-4
Support Systems	11-4
Contractor and DOE Field Element Performance	11-4
Consideration of Integrated Security Management Concepts	11-5

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, in another it may be one of several layers. Auxiliary power systems may support several elements within a PSS and between separate system configurations. Recognition of these dual roles precludes duplicative testing efforts and places the particular element in proper perspective.

All of the 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; and 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 in 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 CCTVs 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 cause the subtopic or topic to be rated anything other than satisfactory).

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

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 operations 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 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 OA-10, and ultimately, the Director of OA.

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 site 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 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 OA-10 inspectors indicate that the sensors are not reliable, it may be an isolated instance of sensor drift, or evidence of deficiencies in the testing and calibration procedures used by the facility. A large number of sensor deficiencies may indicate problems with the testing and maintenance program. In this event, OA-10 inspectors may consider testing a representative sample of sensors in order to determine the extent of the problem. Also, there may be problems with the QA program.

When both the facility and the inspector tests 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 without authorization or detection through one or more portals, 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.

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 communications equipment or duress alarms will have a significant impact on the capabilities of the protective force. One of the most important factors in an effective PSS is ensuring that the protective force responds to intrusion or duress in a timely and effective manner. To be able to do this, they must be able to communicate with the alarm stations, guard posts, response forces, and local law-enforcement agencies. Inadequate communications equipment may be the result of

budget constraints, lack of planning, or the 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, and 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 the result of an isolated instance of component failure or an indication of systemic deficiencies in the design of the system.

Contractor and DOE Field Element Performance

The OA-10 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 operations office surveys and OA-10 inspections
- Responsiveness, indicated by procedures and timeliness in addressing and closing out previous findings
- Quality assurance, 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 systems performance.

In evaluating DOE field element performance, the OA-10 team should consider whether:

- Surveys addressing PSSs are current
- Survey ratings are consistent with survey report narrative and work papers
- Previous OA-10 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 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 Integrated Security Management Concepts

As discussed in Section 1, integrated security management is not currently a DOE policy and OA will not use the guiding principles or core functions as a basis for ratings or findings. However, the integrated security management 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, the inspectors may determine that the reason is that there has not been a 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, OA inspectors should review the results (both positive aspects and weaknesses/findings) of the review of the PSS topic in the context of the integrated security management 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 had 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.

This page is intentionally left blank.