CONF-870713--56

# WHAT ARE THE ATTRIBUTES OF A GOOD STANDARD AND ASSOCIATED CRITERIA?*

BNL 40063

Jack Allentuck

BNL--40063

okhaven National Laboratory

DE87 014289

Upton, New York USA

ABSTRACT

The Department of Energy (DOE) Standards and Criteria (S&C) provide the framework upon which Office of Security Evaluations (OSE) inspections of safeguards and security at DOE facilities are conducted. The S&C were created to assure that inspections are comprehensive, standardized to the extent possible and accurately reported in meaningful terms, and that assessments are objective. With these goals in mind, the desirable attributes of a standard and its associated criteria are relevance, inspectability, and limited need for inspector judgement.

## INTRODUCTION

The fame or notoriety of the Office of Security Evaluations' (OSE) Standards and Criteria (S&C) has grown and spread since they were first used in an inspection at the Pittsburgh Naval Reactors Office in the spring of 1986. In this paper we inquire into the desirable attributes of a Standard and its associated Criteria. Our approach is to consider the background of the S&C, examining the objectives behind their creation and then to review certain practical matters related to making determinations in the field on the status of safeguards and security systems. Based on the OSE objectives in creating the S&C and the practical considerations which we mentioned, we proceed to identify desirable attributes for the S&C. We then examine certain standards and their criteria and determine either that the desirable attributes are present or absent.

The OSE in its inspection function serves as the eyes and ears of the Assistant Secretary for Defense Programs (ASDP) the assessment of the effectiveness of safeguards and security policies and programs at DOE operations offices and facilities. The director of OSE reports directly to the ASDP, however, information developed by inspections teams and included in OSE inspection reports gets a significantly wider audience. While directed to the ASDP, as the senior secretarial offices for departmental safeguards and security cognizance the Office of Safeguards and Security (OSS), Department of Energy (DOE) program offices, affected field office managers and, when required, the staff and members of Congressional oversight committees receive copies of the report or briefings.

The purpose of the report is to provide information for policy formulation and corrective action. However, directly or indirectly OSE inspection reports have caused one or more of the following:

- Improvements in safeguards and security systems at DOE facilities
- The initiation of capital improvements (some involving substantial costs)
- The halt, albeit temporary, of production in various facilities of the DOE complex
- The temporary shut-down of a non-weapons research facility
- Changes in the course of some promising careers as required by the need for accountability
- The propagation of good ideas
- Congressional initiatives
- Some distorted press accounts caused by misperceptions on the part of the media
- True stories in the press
- Problems with labor unions
- Other effects, known and unknown.

Thus, it is highly important that OSE inspections be comprehensive; that information developed be correct and accurately validated and reported in meaningful terms, that analyses be objective and have the same meaning from place to place. In addition, due attention must be paid to assuring that the needed information can actually

*This work performed under the auspices of the U.S. Department of Energy, Contract # DE-AC02-76CH00016.

be obtained and validated in the field during the limited period allowed for an inspection.

A worthy goal, which to my mind will only be achieved in an approximate sense, is a reproducible inspection, an inspection report for a given facility which would not change if prepared by a different set of inspectors on the basis of their own inspection. The reason that a reproducible inspection and resulting analysis is only an approximately achievable goal is that, however standardized an inspection, the element of inspector judgement will never be eliminated. Limiting its scope is however desirable.

The matter of reproducible inspections aside, the goal of meaningful ratings which have the same significance whenever they are used, require inspection of all departmental facilities to the same set of standards. To this end, OSE developed the set of Inspection Standards and Criteria since renamed DOE Safeguards and Security Standards and Criteria (S&C). We will not be concerned here with the important fact that the S&C have been de facto transformed into a statement of DOE policy. Our concern is focused on the S&C as a set of directions for inspections and assessments.

The S&C, organized into a set of eight inspection topics, were developed by a number of committees composed of DOE field office employees, OSE staff and contractor personnel. While the objectives of comprehensiveness and standardized procedure were of utmost importance, the outcome of the S&C development process was influenced by the divergent interests of those who inspect (OSE staff) and those who are inspected (DOE field office and contractor employees).

INSPECTABILITY

Given this background on the development of the S&C and its heavy emphasis on comprehensiveness and standardization, their usefulness as a basis for inspection and assessment rests on their "inspectability". An examination of what is meant by this term requires a review of the basic structure of the S&C: a standard and a set of associated criteria. A standard is a required or desired characteristic of the safeguards and security system. Here we interpret the terms "safeguards and security system" to include not only physical components and human actors but also functions designed to maintain the effectiveness of such systems, for example, field office surveys of safeguards and security systems.

Before we proceed further an example of a standard and its criteria is in order. The example is taken from the Materials Control and Accountability (MC&A) section of the S&C and refers to monitoring waste streams leaving a Material Access Area (MAA) to protect against unauthorized removals via waste streams. The direct objective is to detect movements of SNM in waste streams.

Standard

The facility monitors all liquid, solid, and gaseous waste streams unless otherwise approved by the cognizant Operations Office.

Criteria

4.3.2.2.5.1 All waste monitors are maintained under a documented quality assurance (QA) program.

4.3.2.2.5.2 The facility has a response plan for evaluating and resolving all unscheduled alarm conditions.

4.3.2.2.5.3 Radiation monitors are sensitive to gamma/neutron radiation as appropriate to the waste streams and the specified material types.

4.3.2.2.5.4 The QA program includes procedures for calibration of monitors using SNM sources of the type found in the MAA.

4.3.2.2.5.5 The alarm response plan ensures that the responsible safeguards authorities are notified immediately, unless the report has no safeguards significance.

4.3.2.2.5.6 The facility evaluates and resolves all unscheduled alarm activations.

In a section which follows we will examine this standard and its criteria for the presence of desirable attributes.

Ideally, the inspector determines whether or not a standard is met by examining a set of criteria which are provided him by the S&C. The determination by the inspector whether or not criteria are fulfilled is based on a review of documents, by observation of processes and by testing performance. If enough of the criteria are fulfilled the standard is determined to have been met. Thus, at least in theory, the direct subject of the inspection are the criteria.

After this long digression we return to the definition of "inspectability". In brief, "inspectability" with specific reference to the S&C, means that it is possible to determine during the course of the inspection whether or not a set of criteria are fulfilled and that such a determination leads directly to a decision that the standard has been met.

Some remarks on levels of inspectability are in order. To this end we define several categories of standards:

- Standards which refer to the existence of a process or system
- Standards which refer to the performance of a process or system

The second of these categories is further subdivided into subcategories.

- Processes or systems without human actors.

- Processes or systems with human actors.

We can now establish a hierarchy of inspectability. From the most readily inspectable to least inspectable we rank systems as follows.

| Category of Standard | Inspection Activity |
|---|---|
| Standards which refer to the existence of a process or system. | Examine documented assignments of responsibility and procedures. |
| Standards which refer to the performance of a process or system which have no human actors. | Check performance of process or system. |
| Standards which refer to the performance of a process or system which have human actors. | Check performance of process or system. |

While the statement that a process or a system exists implies that it will continue to exist unless it is removed or replaced there is less assurance about the performance of a system in the future. Where the performance of a system containing no human actors is concerned its continued acceptable performance might be assured by the existence of a QA program and a testing program. Where the performance of a system which depends on human actors is concerned any assurance about performance almost disappears. It follows that determining whether a standard relating to the performance of a system which includes human actors is met is more difficult than one which relates to the performance of a system without human actors and much more difficult that one which relates to the existence of a system. Considerations of this kind lead to the desirability of being able to make a statistical statement related to a level of confidence about a criterion being fulfilled as an alternative, where appropriate, to a simple yes-or-no compliance related answer. This matter should have a place on the OSE agenda for the near term.

RELEVANCE

Having examined the concept of inspectability we now turn to the idea of relevance. By relevance we mean 1) that a standard makes a statement about the status of the safeguards and security system and 2) that a criterion is relevant to the standard with which it is associated. Relevance, of all the issues which go to determining the quality of a standard, is likely to be the most controversial. Relevance has important implications for the efficient utilization of inspection resources: inefficient utilization when standards are not relevant, efficient when they are. Relevance also has implications for the credibility of the inspection and assessment process. When standards are irrelevant to safeguards and security the process may be questioned both by those who are inspected and those who inspect.

When a criterion is irrelevant to a standard, controversy and confusion can result. A likely outcome in such a case is the improper determination by the inspector that a standard is not met.

INSPECTOR JUDGEMENT

Having discussed "inspectability" and relevance we now shift to the requirement that evaluations mean the same across inspections at different facilities as well as from inspection to inspection. Part of this requirement is met by the existence and use of the S&C and the standardization provided by it. The remainder depends on limiting the effects of the variability of inspector judgement. Inspector judgement affects assessments in several ways:

- Inspector selection of the standards to be inspected

- Inspector response to criteria which require him to judge if a system meets "minimum" requirements or is "effective" without providing definitions of the terms

- Inspector determination of how many criteria must be fulfilled before an assertion can be made that a standard is met.

The last of these openings for inspector discretion can be expanded to include questions such as

- How are important criteria weighed against less important criteria?

mined?

Desirable Attributes of Standards and Criteria

Having reviewed the objectives of the OSE in generating the S&C and examined ideas such as "inspectability", "relevance", and "inspector judgement", we can now identify the attributes which are desired in a standard and its associated criteria.

Desirable attributes are:

- The standard should be relevant to the status of the safeguards and security system.

- The associated criteria should be inspectable. It should be possible to make the determination that the criteria are fulfilled during the course of the inspection.

- The need for inspector judgement in determining whether the criteria are fulfilled should be reduced to "as low as reasonably achievable".

  This can be accomplished as follows:

  a) Eliminate unimportant criteria

  b) Eliminate standards which require the inspector to determine things like "effective", "maximum required", etc.

Illustrative Examples

Now we will examine the example of a standard and its associated criteria which we provided earlier in the light of the desirable attributes which are identified above.

a) Standard - the facility monitors all liquid, solid and gaseous waste streams...

b) Criteria - 4.3.2.2.4.1-.6

   Comment: All the criteria except .6 are inspectable. They refer to the existence of systems (except .3). Thus, they are of the kind most easily inspected. Criterion 4.3.2.2.5.3 refers to the performance of a system and is capable of testing, thus given the availability of appropriate sources is inspectable.

   Criterion 4.3.2.2.4.6 is not inspectable and there is no way in which the inspector can determine that "all" unscheduled alarm activation are evaluated or resolved unless he is sure that "all" that have occurred have been logged.

   The criteria, with the exception of the one which is uninspectable, make no demands on the inspector's judgement in

criteria are fulfilled or not.

Which criteria are important? Which less important? The first four are more important than the remaining two. While others might disagree (inspector judgement variability again) to my mind the standard is met if the first four criteria are fulfilled.

Irrelevant Standard

In the section on computer security consider the following:

**Standard**

The buildings and rooms used to house major computing resources are designed to minimize damage or loss to computing resources by fire, flood, natural phenomena, hostile penetration, sabotage, theft, vandalism, and tampering. This should be done commensurate with the value of the resources.

**Standard**

Property standards (control, inventory, and management) are implemented to ensure availability of equipment, and preservation of computing resource assets from loss, misuse, and misappropriation.

The first of these standards is really concerned with preserving information in the computer and may thus have some peripheral relevance to computer security. The second one seems to have no relevance to it at all.

Fortunately, there are not many irrelevant standards in the S&C and within limits inspectors are free to choose which standards to inspect.

Excessive Inspector Judgement

Consider the following from the section on Protection Program Operations.

**Standard**

Building clearing methods provide for the isolation and thorough search of a building, the neutralization and proper handling of all adversaries in the building, and the accomplishment of the objective with minimum danger to the security force.

**Criteria**

Command and control is effective
Planning is effective
Assessment is effective
Containment is effective
Individual tactics are sound
Team tactics are sound
Suspect handling is effective
Application of force is effective

Finally, for man's best friend we have also from the Protection Program Operations section the following criterion:

"The dog can perform to the extent necessary to accomplish the intended mission."

Since there are as yet no DOE orders relating to canine performance, no one, neither man nor beast, will be rated on this subject.

Enhancing Inspectability: An Innovative Approach

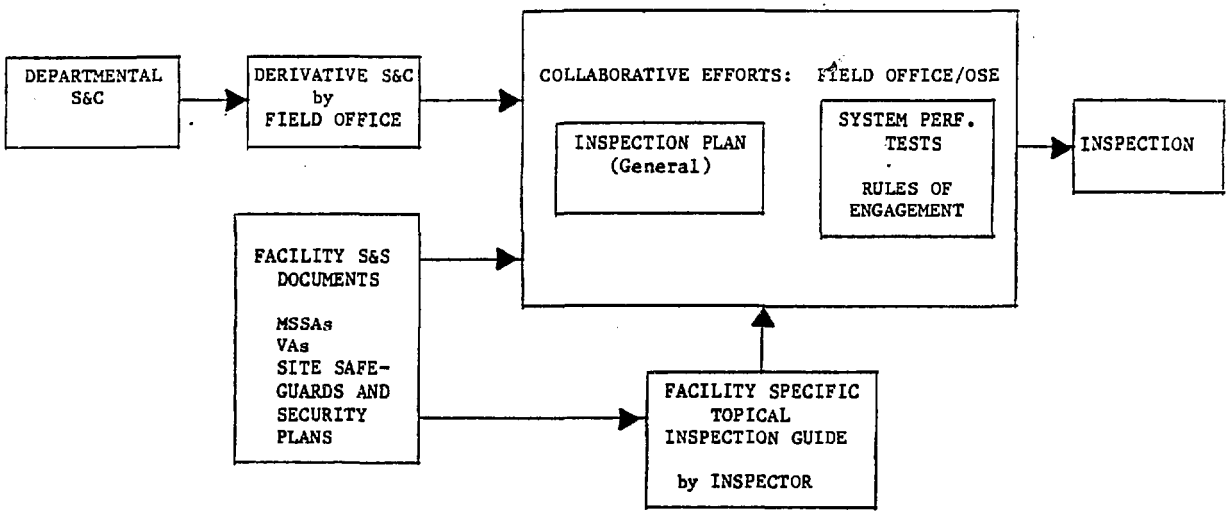
An innovative approach to enhancing inspectability has been attempted at several locations with promising results. It is based on increased involvement by the field office/facility which is to be inspected. The innovative feature is the preparation by the field office/facility of a set of derivative S&C. The derivative S&C originate in the departmental S&C for safeguard and security inspections but are "tailored" by field office and facility staff to be appropriate to the specific facility and its process and activities. Justification for the use of the derivative S&C is provided by the field office for review by the OSE. By itself, this innovative approach eliminates the component of variability of inspector judgement which arises from selection by inspectors of specific S&C to inspect.

Inspectability is further enhanced by facility participation with the OSE in the preparation of the general inspection plan and review of the inspector prepared topical inspection guide. The latter defines the data and information to be collected during the inspection, the "measurability" of the information, essentially the same as inspectability, and the proposed validation techniques. In addition, the decision rule for determining whether or not the derivative S&C are met is defined in the topical inspection guide.

The process described above is displayed in Figure 1.

**Conclusion**

As presently written most of the Standards in the S&C are relevant and make significant statements about the status of the safeguards and security system; the criteria are relevant to the standards and are inspectable; and, the variability of inspector judgement is kept within reasonable limits.




ENHANCING INSPECTABILITY

FIGURE 1

## DISCLAIMER