A Systematic Approach for Implementing Managed Access at Sensitive Nuclear Facilities

George T. Baldwin
Sandia National Laboratories

"Managed access" is an often-used term to describe various special arrangements for conducting on-site inspections where sensitive information is present. The information that is sensitive, either because it is classified, proprietary, or private, must be protected from disclosure during inspections. "Managed access" refers to those measures that both protect sensitive information, yet enable an inspection to take place. Typically, a host may devise such measures from a predominantly defensive point of view, or underestimate the time and effort required to prepare adequately.

In this paper we propose a systematic approach to implementing managed access, particularly for nuclear facilities that might be subject to verification of a Fissile Material Cutoff Treaty (FMCT). The systematic approach begins with the need for the host to demonstrate compliance with an agreement, before considering protection measures. Determining in advance what is the *minimum sufficient information* to reveal is mutually beneficial to inspector and host. The inspector's job is facilitated by the host preparation, and the host may be able to avoid unnecessary and costly protection measures. Although there is no guarantee that an inspector will accept what the host deems to be minimum sufficient information, it nevertheless provides a sound basis both for pre-inspection preparation and for appealing disagreements.

INTRODUCTION

What is Managed Access?

We will use the following as a working definition[1] of the term "managed access" for the discussion that follows:

A process by which one party (the "host") enables another (the "inspector") to gather only necessary and sufficient information for assuring that the host is in compliance with an agreement, while at the same time protecting sensitive information from unnecessary disclosure.

By "sensitive" information, we mean any information that may be classified, proprietary, private, etc. It makes no difference whether a facility is military or commercial. It is entirely the assessment of the host to decide what is or is not sensitive.

The way in which managed access can be implemented varies from formal, written procedures to ad hoc measures worked out during an inspection. The Strengthened Safeguards System additional protocol adopted by the International Atomic Energy Agency (IAEA) envisions at least some managed access measures to be spelled out formally in the Facility Attachments. More likely, measures are developed by the host facility during its preparation for a verification inspection, but not formalized in the written Facility Attachment. Other measures may only be developed on the spot during an inspection, in negotiation between inspectors and escorts to resolve difficulties that may only arise at the last minute.

Need for Systematic Approach and Preparation

Although managed access measures can be devised at the last minute to respond to unanticipated needs of an inspection, such use of managed access should only be a last resort. The flexibility such on the spot negotiation provides should never be used as an excuse for the lack of adequate preparation for verification inspections. Ad hoc approaches to preparation are unnecessarily costly and risky. The consequences of unnecessary disclosure of sensitive information might be dire, whether by undermining national security, or giving away commercial trade secrets to business competitors.

Preparation in advance for verification inspections is not required by the agreement itself; instead, it is usually left to the individual agencies, businesses, and organizations to take measures (or not) as they see fit. The Defense Treaty Implementation Readiness Program (DTIRP) is one good example of an effort to assist in advance preparation. Such preparations are usually preoccupied with protection of sensitive information, logistics, reduction of impact on operations, and similar defensive concerns. Demonstrating compliance may not be high on the list of facility concerns.

Planning should even be done before an agreement is concluded. Such work can provide early feedback to policy makers and negotiators, helping to avert problems that might otherwise only appear later. Once an agreement is concluded, its provisions are often impossible to reverse.

Unless an agreement provides escape clauses allowing protection of sensitive information, there is usually no way to protect sensitive information that *is* subject to an agreement, short of abrogating the agreement. To hope that sensitive information subject to an agreement will simply not be detected is risky and irresponsible.

A Different Perspective

There has already been a considerable amount of work concerning managed access measures for a number of treaties and agreements. Most all such work emphasizes the use of managed access for the protection of unrelated sensitive information. In this paper, we recommend considering a different primary emphasis: the use of managed access to demonstrate compliance with an agreement.

In no way are we suggesting that protecting of sensitive information is any less important than before. It is still of paramount importance. But that importance does *not* require that protecting sensitive information be the first consideration in the preparation for verification inspections. Indeed, in this paper we seek to illustrate how a different guiding paradigm, that of demonstrating compliance, may actually make the job of protecting sensitive information that much easier and successful.

APPROACH

Consider two fundamentally different approaches to managing inspector access at a facility: *Maximum access,* which seeks to provide the greatest space for an inspector to operate in, and *focussed access,* which limits access to only that which the host deems appropriate to the agreement in question. We begin by describing each approach in principle, and then contrast the two with an example of a hypothetical verification problem under a Fissile Material Cutoff Treaty (FMCT).

DISCLAIMER

Maximum Access

One way to approach the access problem is to protect everything that needs to be protected, and allow the inspector virtually unrestrained access to everything else. This "maximum access" approach thus creates two categories of information, as depicted schematically in Figure 1.

The maximum access approach often assumes that the inspector is able to make a determination about compliance based solely upon information found within the "everything else" category. Problems arise when the inspector sees protected items or areas (e.g., covered by a shroud), and expresses concern that the protection may be hiding something subject to the agreement.

The maximum access approach offers two main advantages. The first is that to some extent, it prepares a facility for inspection under most any agreement. Whether CWC or FMCT, there might be little difference in preparation. A second advantage is that it offers "maximum transparency." The facility has made every effort to grant the inspection the latitude to go where it wants and learn what it wants, whether or not it pertains to the agreement in question.

Figure 1. Illustration of the "maximum access" approach to protecting sensitive information. An inspector is denied access to the "information to protect" space, but may seek information relevant to a particular agreement everywhere else.

Maximum access has drawbacks, however. For one, there is no assurance *a priori* that compliance can be judged from the information that is not protected. Second, inspectors left to their own devices may waste time and resources while trying to accomplish their mission. The implicit message to the inspection team is "Look wherever you want and do what you need to, but you're on your own. Our facility is open to the maximum extent possible." Third, and perhaps most serious, is that this approach inherently draws attention to the very objects or information that it tries to protect. Even if not obviously protected visually, an inspector could be tempted to "push the envelope," just to see what access limits exist. Indeed, an inspection strategy could well be not to worry much about anything where access has been granted. The mere fact that it is open to the inspection makes it less of an issue. It is more likely that the facility is hiding non-compliant activity behind the cloak of protecting sensitive information. Especially in the case of sensitive facilities, there may be so much that needs to be protected, it conveys the impression that compliance is being hidden. This creates a potentially adversarial atmosphere, where the facility may be challenged continually to prove its need to protect.

Focussed Access

A different way to approach the managed access problem is to determine just what the inspector needs to know, and devise how to reveal only that information with minimal disruption to everything else. As shown in Figure 2, we again create two categories of information, but they are quite different from the case of maximum access.

Focussed access is definitely "minimum transparency", which is not necessarily desirable under prevailing thinking. However, we are dealing here with sensitive facilities. We make no secret that there are secrets: There are things going on here that we would rather someone from the outside did not know. In exchange, we have taken upon ourselves the burden of demonstrating why this facility is compliant with the terms of a particular agreement. We are helping the inspector achieve his or her verification goals.

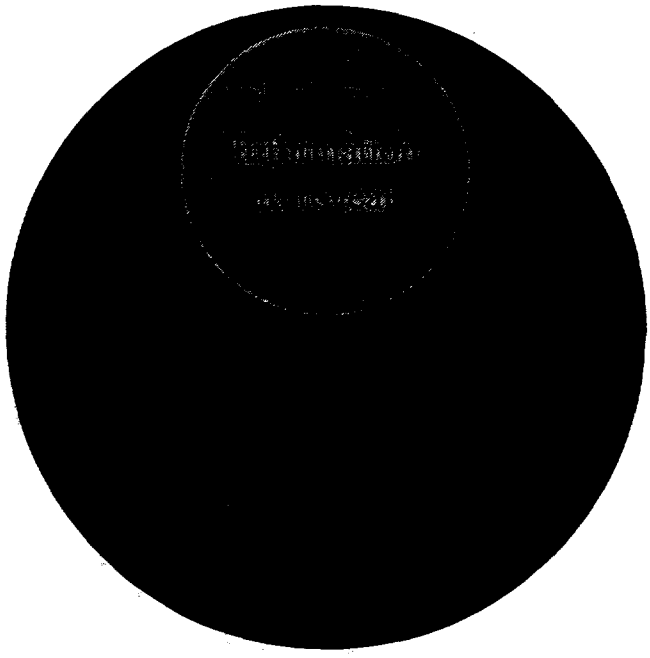

Figure 2. Illustration of the "focussed access" approach to protecting sensitive information. An inspector is restricted to operate only within the "information to reveal" space, which is deemed by the facility to provide the minimum sufficient information for judging compliance.

APPLICATION TO FMCT

A Fissile Material Cutoff Treaty (FMCT) is a potential future agreement that would most likely involve managed access at sensitive nuclear facilities. The treaty is currently under consideration by the Conference on Disarmament, but the negotiations are a long way from completion. Provisions are not universally agreed to, and there is not even a rolling text for a treaty or verification protocol. Nevertheless, work in advance is necessary to explore the implications for verification. For this purpose, we postulate what a treaty might require and more importantly, what might be subject to verification. Insodoing, we are by no means endorsing any particular point of view or policy position.

FMCT would likely not permit the separation of plutonium (Pu) or high enriched uranium (HEU) from irradiated material, without subjecting the recovered Pu or HEU to accounting measures that ensured that it was never used for proscribed purposes (e.g., for nuclear weapons). We assume that any facility that was *capable* of producing Pu or HEU from irradiated material, even if it did not do so, would probably need to be declared and verified. The example cited below is a hypothetical yet plausible scenario to illustrate the different approaches to managed access.

Example: Reprocessing Operation for Medical Isotopes

Molybdenum-99 (^{99}Mo) is a precursor to Technetium-99, a common tracer radioisotope required in many nuclear medicine diagnostic procedures. The ^{99}Mo fission product is recovered from irradiated HEU targets by chemical separation.

Our hypothetical facility consists of three linked hot cells adjoining a research reactor, as depicted in Figure 3. HEU targets are exposed in the research reactor, then are moved by remote handling through a transfer lock into the hot cells. In the first cell, the targets are sheared and the irradiated material dissolved in acid. The solution goes through several processing steps in Cell 2 to isolate ^{99}Mo. A low-volume, highly radioactive waste stream containing unfissioned ^{235}U and fission products is removed by remote transfer to a shielded storage vault for long-term storage. The separated product passes to Cell 3 for quality control checks and assay before transfer to a shielded transfer cask for removal and transportation.

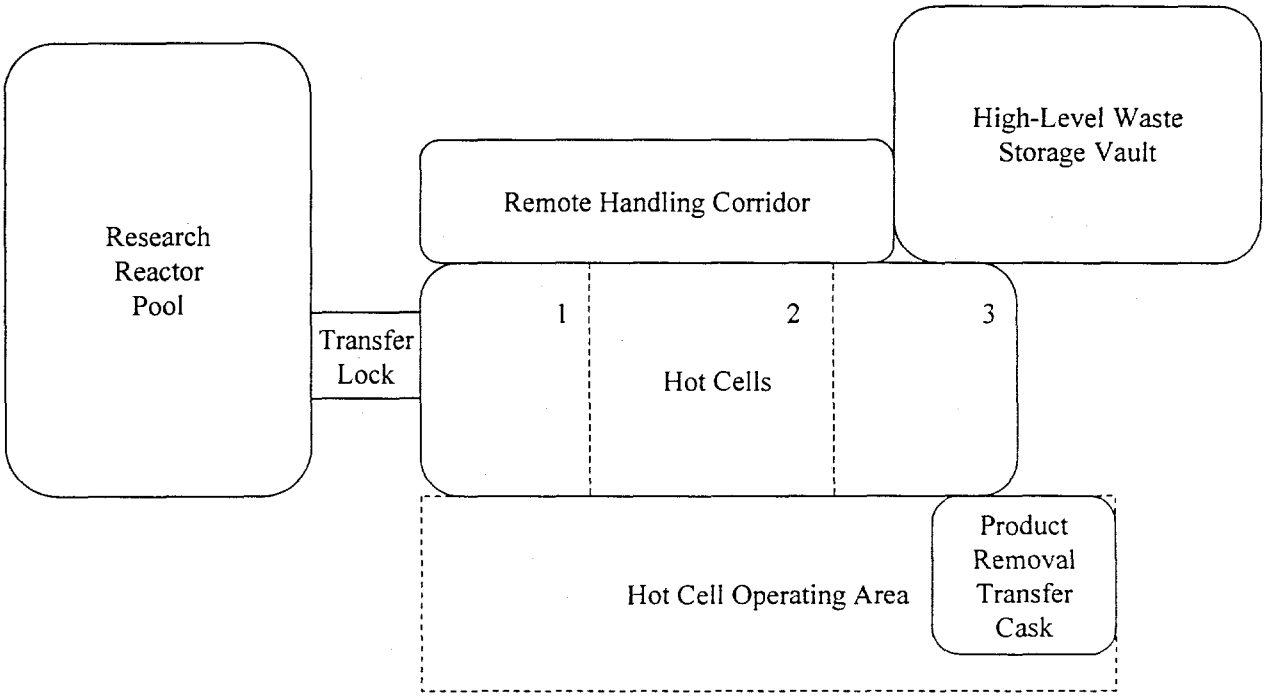

Figure 3. Schematic layout of a hypothetical hot cell reprocessing operation to recover from irradiated HEU targets.

In our hypothetical scenario, we postulate that the facility maintains its competitive advantage as a supplier of the medical radioisotope, because it protects trade secrets dealing with the design of the HEU targets, and certain processing steps in the wet chemistry for separation. Yield information is also considered secret.

Verification Approaches

A hot cell complex that services a research reactor is certainly in principle a reprocessing-capable facility, and would need to be declared and verified under FMCT. We will further assume that the HEU used in the targets was not subject to accounting, because it existed in a nuclear-weapon-state party to the NPT[2] before entry into force of the FMCT.

Maximum Access

In a maximum access approach, the facility might see fit to shroud the shearing machine and any targets or sheared hulls within cell 1. Otherwise, inspectors would be allowed to inspect the hot

cells through the viewing windows. Log books and material samples would not be made available, for sensitivity reasons. Operations would need to be suspended upon notification of inspection, to shroud equipment. They would need to remain shut down during the inspection, so as not to interfere with inspector viewing, and not to reveal process steps.

Despite maximum access, compliance would still be an open question. There would still be no straightforward way for the inspector to be assured the activity was not a solvent extraction to recover Pu from natural U targets, for example. Inspections would disrupt production of the relatively short-lived product and impact delivery contracts.

Focussed Access

In focussed access, the facility might choose to do something quite different. It might propose to demonstrate that no separated HEU or Pu leaves the hot cell facility, and that such information is sufficient. For example, it could establish a perimeter bounding the operation, and subject anything exiting the perimeter to verification. After a single baseline inspection to verify facility design, an unattended surveillance system provides continuous monitoring of the operations. Hot-cell operations would be watched continuously with cameras outside of the hot cells, viewing the room (i.e., the "hot cell operating area" in Figure 3) from the side. A camera could see the access ports, but could not see into the hot cells. Video would be captured whenever triggered by the opening of an access port. (Anything seen being *removed* from the hot cells through these ports would be cause for concern, but that is not an issue for the facility because they are only used as entry ports, and not for removing tools or materials.)

Inspectors could review the recorded video images, and observe ongoing operations through the cameras during inspections. Shrouding would be unnecessary, because inspectors are denied access to the room, and the camera field of view is limited. The product removal port could be further instrumented with a gamma spectrometer to document that the product contained only ^{99}Mo, and not Pu or HEU.

The shielded remote-handling corridor behind the hot cells and the connecting high-level waste storage vault would be within the control perimeter. Normally there is no access through the heavy shield doors, and these could be sealed. Annual removal of old waste containers for disposal could be coordinated with a scheduled inspection.

Many additional details would be involved in the complete verification regime, but we omit them here for brevity. For example, inspectors would probably need to know that separated fissile material was not being removed clandestinely in small containers inside the waste drums, and that materials could not exit via the transfer lock and reactor pool. The important point is that the facility decided how they would demonstrate compliance.

DISCUSSION

Note that some information, *although related to the agreement,* might still be protected as sensitive information and not provided to the inspector. For example, an inspector might argue that the particular organic solvent used in the extraction process was relevant to the inspection team need to determine compliance, because they could determine whether or not it was able to remove plutonium or HEU. In our example, however, the facility insists that that information is proprietary. They argue that the other information they are providing is sufficient to determine compliance.[3]

It is nevertheless possible that the inspector may not accept the facility-offered demonstration of compliance. Three steps can be taken to avoid such a conflict: (1) red teams and mock exercises should be used during preparation to help anticipate problems; (2) the means used to demonstrate compliance should be discussed in advance with the inspectorate, to encourage buy-in in advance; and (3) the facility can as a last resort consider allowing additional measures. Otherwise, the facility can simply refuse to comply with the inspector request. By having prepared for verification with a compliance-based approach, the facility has already established an argument that can now be used to appeal an impasse, which is not the case if it takes a purely protective approach.

In this example, just how the treaty chose to define *production* could profoundly affect the acceptability of verification approach preferred by our hypothetical facility. It is just one example of why a serious consideration of alternative verification approaches, from the point of view of demonstrating compliance, is so important in advance of completed treaty negotiation.

CONCLUSIONS

A compliance-focussed approach to managed access is essential in preparing a facility for verification inspections. An approach that seeks primarily to protect specific information while otherwise allowing maximum access may be counterproductive for sensitive facilities, especially because it calls attention to the very things it seeks to protect. Focussed access acknowledges from the outset that a sensitive facility has justifiable reasons not to be completely open about its operations, and should need only to provide the minimum information that will suffice to determine compliance. By emphasizing the compliance aspect, focussed access is mutually beneficial to inspector and host for the effective conduct of managed access inspections.

ACKNOWLEDGMENT

We appreciate both external funding from DOE/NN-42 and internal funding from Sandia National Laboratories for supporting this work. Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy under Contract DE-AC04-94AL85000.

---

[1] The Chemical Weapons Convention (CWC) formalized the concept of managed access, as described in the following two paragraphs from Part X, Section C of the CWC Verification Annex:

"46. The inspection team shall take into consideration suggested modifications of the inspection plan and proposals which may be made by the inspected State Party, at whatever stage of the inspection including the pre-inspection briefing, to ensure that sensitive equipment, information or areas, not related to chemical weapons, are protected...

"48. In conformity with the relevant provisions in the Confidentiality Annex the inspected State Party shall have the right to take measures to protect sensitive installations and prevent disclosure of confidential information and data not related to chemical weapons."

[2] NPT = Treaty on the Nonproliferation of Nuclear Weapons

[3] The CWC also deals with this concern. The "Confidentiality Annex" states:

"1. The obligation to protect confidential information shall pertain to the verification of both civil and military activities and facilities... the Organization [for the Prohibition of Chemical Weapons] shall:

(a) Require only the *minimum* amount of information and data necessary for the timely and efficient carrying out of its responsibilities under this Convention..." *[author's emphasis added in italics]*