SAND2011-3415C

Technical Implementation of Nuclear Nonproliferation Cooperation to Complement IAEA Safeguards

George T. Baldwin

Sandia National Laboratories, Albuquerque, NM 87185-1373 USA

Abstract:

Compliance with the terms of a state's international safeguards agreement with the International Atomic Energy Agency (IAEA) has long been a key underpinning of the nuclear non-proliferation regime. The framework for international safeguards relies on an independent organization, the IAEA, acting under bilateral agreements with states to verify declarations of nuclear materials and activities, and reporting its conclusions annually to the world at large. The system has worked well for decades; nevertheless, there has been and continues to be interest in supplementing the compliance-based system with voluntary measures by a state to demonstrate commitment to nuclear non-proliferation goals. Direct state-to-state exchange of non-proliferation-relevant information is one such approach. For example, the cooperation of Brazil and Argentina was an enabling factor in the accession of those two countries to the Treaty on the Non-proliferation of Nuclear Weapons (NPT) and acceptance of IAEA Safeguards. In some cases, a regional sharing of non-proliferation relevant information may be appropriate. Such cooperation has been of interest to various states in the Asia-Pacific in particular. The step from a bilateral exchange to multilateral cooperation presents a major technical challenge, however. To begin, interested parties to regional voluntary cooperation or "transparency" must clearly define the goals and expectations of the cooperation. There must be perceived benefit to such cooperation to justify the effort and costs, but at a minimum, the sharing must cause no harm. It is critical to establish the associated requirements for information sharing, which necessarily must address security concerns. Fundamentally, each party to the cooperation must be able to trust the information obtained from the regional network, and similarly, be confident in the security of information it discloses to the network. If implemented properly, a regional system can withstand the ups and downs in political relations between states. Measures for authentication and encryption of information are only part of any technical framework, which must be augmented with appropriate procedural measures as part of a system solution. Sandia National Laboratories has been a partner with Japan, Korea, the European Commission, and other states under bilateral agreements with the U.S. Department of Energy to develop sound technical approaches that facilitate regional non-proliferation cooperation.

Keywords: safeguards, regional cooperation, transparency, information security

1. Introduction

1.1. Safeguards by an independent, trusted third party: IAEA

Even before the appearance of the Treaty on the Nonproliferation of Nuclear Weapons (NPT), nuclear supplier states recognized the value of an independent third party to verify peaceful use of technology and materials transferred to recipient states. Accordingly, the International Atomic Energy Agency (IAEA) quickly assumed such responsibilities, which were codified under "project agreements" that implemented safeguards as described in IAEA Information Circular (InfCirc) 66. This third-party role of the IAEA in providing safeguards was instrumental in relieving states of what otherwise would have required an enduring bilateral relationship between supplier and recipient states. The ensuing duplication of effort, lack of uniform approach, lack of integration, overlapping jurisdictions, etc. would have led quickly to a costly, unmanageable, and unsustainable mess. With the advent of InfCirc 153 comprehensive safeguards agreements following the NPT, the IAEA safeguards system gained even better efficiencies through consolidation. In sum, the creation of this centralized framework for international nuclear safeguards was indeed instrumental to the success of the nonproliferation regime. Much of the evolution of that regime has focused on what tools are necessary for the IAEA to implement safeguards effectively.

1.2. IAEA releases a safeguards conclusion, but not the data

While the creation of the IAEA safeguards system relieved states of direct responsibility for verifying the peaceful use of nuclear materials and technologies that had been shared with others, it did not dismiss their interest in the “answers.” The IAEA announces a Safeguards Implementation Report (SIR) annually, which is limited to the conclusion drawn by the IAEA in respect of the implementation of safeguards in a particular state having a safeguards agreement with the IAEA. Information supporting the IAEA conclusion is not released, but instead is protected as “Safeguards Confidential.” The confidentiality of safeguards information, an IAEA pledge to an inspected state, is argued as being necessary to ensure the full cooperation of the state with the IAEA. An inspected state could otherwise be reluctant to be completely forthcoming with the IAEA. Compliance information could entail proprietary secrets, reveal physical protection measures, or otherwise put at risk justifiable activities or assets if disclosed indiscriminately. Thus “safeguards confidential” is standard practice; it is a critical enabling factor for IAEA safeguards.

1.3. State transparency can complement Safeguards

For various reasons, states may at times desire more than the safeguards assurance provided by the IAEA. The global system is not meant to address all of the particular questions that might arise in limited geopolitical situations. The cooperation of Brazil and Argentina, which led to the formation of the Brazilian-Argentine Agency for Accounting and Control of Nuclear Materials, ABACC, is a good historical example. Direct cooperation was the enabling factor for both countries to accede to the Treaty on the Non-proliferation of Nuclear Weapons (NPT) and only then accept IAEA Safeguards. Twenty years later, ABACC still receives enduring support from the two states.

More recently, both Japan and the Republic of Korea have been exploring cooperation on the voluntary exchange of information related to their nuclear activities. In a workshop on regional transparency in Tokyo in February 2008, Wan Ki Yoon (Korea Institute of Nonproliferation and Control) described how the direct cooperation of states strengthened the nonproliferation regime.[1] He used the metaphor of a cone: The safeguards agreements of the IAEA, at the apex, comprised the sides of the cone, with individual sovereign states arrayed in a circular ring at its base. “Transparency” appears in the base of the cone, as an overlapping network of connecting lines between individual states. The complementary nature of compliance with IAEA safeguards and voluntary state transparency contributes to a more robust nonproliferation assurance.

Safeguards confidentiality is an obligation of the IAEA, not an obligation of the providing state. If a state should decide that sharing information with other recipients—even safeguards information—is in its national interest, there is nothing to prevent it from doing so. Such transparency carries both benefits and risks. Precisely *how* information might be shared for regional transparency applications can affect the balance of risks and benefits significantly. The purpose of this paper is to frame the problem for information sharing from a technical perspective.

2. Context for Nuclear Nonproliferation Cooperation

Unlike compliance with IAEA safeguards, voluntary information sharing between states is not governed by clear cut guidance on *what* information should be involved, nor *how* it should be shared. Many factors must be considered: the goals in sharing information, the types of information involved, what sort of reciprocity may be expected, associated threats and risks, the need to be able to trust the information, a scalable technical architecture for sharing, metrics to evaluate the viability and utility of a technical sharing solution, procedural resolution of anomalies, and a host of additional factors.

2.1. Different approaches to transparency

Before considering any technical implementation, it is important to consider the various ways a state might choose to provide nuclear nonproliferation information voluntarily. The following description is meant only to illustrate the differing contexts for consequent technical solutions, rather than to discuss the relative merits of transparency approaches.

An option that is always open is unilateral information sharing. This could be completely open release, such as posting on a universally-accessible web site. On the other hand, unilateral sharing could instead be confined to some limited audience. Ideally, a "limited audience" should mean a single recipient, so that if the information were to appear elsewhere, it's clear who forwarded it. If more than a single recipient, there is little practical difference from open release without some effective mechanism that constrains further information sharing and dissemination.

Instead of using a unilateral approach, a state wishing to improve transparency could do so by working out an agreement with a recipient party. Although there is no reason why such an agreement couldn't involve one-way information sharing, it more likely involves reciprocal, two-way information sharing. The simplest situation is under a bilateral arrangement, with a single, consolidated channel for the associated information exchange.

Extending beyond a bilateral agreement, information sharing can be enlarged to multilateral involvement. One possibility might include a third party as an intermediary to facilitate an otherwise more difficult bilateral relationship. Or it could involve additional states all as relatively equal participants to a common arrangement. As soon as the context moves from bilateral to multilateral—the addition of just a third party—the implications for the technical dimension of information sharing become fundamentally more complicated. Indeed, technical solutions that sufficed for bilateral information sharing may no longer be acceptable, unless the original bilateral technical approach anticipated the scaling to multilateral from the beginning.

2.2. Considerations in "supplying" transparency

Here we assume that providing information is something that a state *wants* to do. It is not something that is required, or that has predefined requirements: it is entirely up to the state to decide how it would be done.

Most important, there must be a need that answers the question "why" it should be transparent. The need should be defined in clearly stated goals and objectives. It might be to address an explicit external request, respond to a real or perceived need, or just to provide assurance. In the nuclear nonproliferation realm, it is typically to demonstrate responsible stewardship of nuclear materials and technology: peaceful use, peaceful intent, competence of staff, etc. Lines can blur, particularly with transparency efforts related to operational safety, physical security, and related concerns.

A second critical consideration is to define precisely the audience: *Who* is the intended recipient of provided information? Presumably the state has identified a "need to know." At this stage, the state also may wish to consider who does not need to know, and why not.

Next, one can consider more specifically *what* information to provide. That information should address the "why" question, the goals and objectives, preferably from the point of view of the recipient of the information. What information is desired and useful, vs. what is possible? What information would be of interest and valuable? What information would strengthen confidence among parties, vs. what might be counterproductive, vs. what might be irrelevant? What types of information can be considered? Possibilities are endless: documents, declarations, measured data, images. It is also instructive to paint the possibilities on a spectrum of value. Typically the information will be anecdotal or suggestive, rather than complete and comprehensive.

When would the information be provided? The transparency could be a one-time event, or an ongoing promise. It could be offered at regular, predictable times, or only on occasion as desired by either of the parties. Information may be "pushed," i.e., sent out as decided by the supplier, or "pulled", i.e., retrieved if and when desired by the recipient. The provision could be prompt, or with some time delay.

What is the expected result of the information sharing? Is there any expectation of feedback, such as comment, questions, or even just acknowledgment? What is important to know after release? Was the information appreciated? Understood as intended? Valued? Looked at? Or does it suffice to consider "no news is good news"? Arguably, some benefit must be expected, or it would be nonsensical to expend the effort in the first place. A difficult technical question is how to measure or assess the results from transparency. If one cannot measure the benefit, however, then it is impossible to assess the cost/benefit for the transparency.

Unexpected results of information sharing must also be considered—at least to assess potential threats and the vulnerabilities that might be introduced through providing information. Collateral damage arising from the potential misuse of information, whether by the intended audiences, or leaks to unintended audiences, presents a risk.

How to supply the transparency is where the technical solution becomes especially important. Generally the desire for low-cost, low-impact solution involves some automation of the information sharing process. The process needs to employ a trusted mechanism that addresses security concerns. Could information be recalled if necessary? How would the system employ a review pipeline? Some level of oversight or audit will be necessary.

2.3. Considerations in “receiving” transparency

The recipient of transparently-offered information has a corresponding set of considerations. Typically, the situation is one of desiring to receive certain information and then finding a way to motivate another party to disclose it. But here we will instead assume that we are past that step: the information will be or has been provided. Knowing that another party is providing the information, the recipient at the very least needs to decide: What do we do with it?

The “why look at it?” consideration is relatively easy. The information is available; it might be useful, so take a look. Why not?

What to do with the information presents two possibilities: ignore it or act on it. In the latter case, *how* to deal with received information is the major consideration. Especially if this is an ongoing (vs one time) provision of information, is there a business process to manage it? Who is the responsible point of contact? What is the pipeline to others who “need to know”, either the raw information as-is, or some derived result, such as an analysis or summary?

Several questions must be answered in the course of analysis and evaluation:

1) How well do I trust this information? Can I be sure that I know where it came from, that it hasn’t been tampered with (integrity), that its attributes are valid (e.g., time stamps)?

2) How valuable is this information? Do I care about it?

3) Assessment: what does this information tell me? Is there anything else, besides the intended message? Does it raise any questions? Is it consistent with other sources of information? Is there anything missing?

4) Next steps: Is there any follow-up that needs to be done internally? What consequent action is appropriate? Is a reciprocal response expected, or just an acknowledgment?

2.4. Considerations for multilateral arrangements

Multilateral arrangements introduce significant complexities for transparency. Immediately there is now a greater likelihood of facing a diverse audience, which could limit the scope of information a state is willing to share.

One way to deal with the differing interests is through “compartmentalization”: having separate groups within the multilateral group. But what are now the business rules governing the way information and communication takes place within the arrangement? They can quickly become complex.

Authentication now becomes more important, which is the technical implementation for positively identifying the source of received information. Otherwise it is possible in principle for one party to impersonate another. Authentication also helps to preserve the integrity of information, identifying what is truly a genuine version. Especially as more recipient parties are involved, it is more likely to have multiple copies of information in circulation.

"Trust" is a key concept for voluntary sharing arrangements. Generally, trust needs to be the *outcome* of the transparency; the underlying system should not assume a trusted arrangement in the first place.

Any transparency arrangement needs to be able to add new members, or deal with members departing, seamlessly. Such extensibility requirements have many technical implications. The architecture or topology is important—how are parties connected with another. Is there a centralized location where information is exchanged (hub and spoke); is it instead a maze of two-way connections between each pair of participants; or are there other strategies?

2.5. Considerations for all parties to transparency

All parties to a transparency arrangement would have many common, overarching issues. The topics suggested here are not comprehensive, but provide just a starting point.

A critical concern is security. What are the threats? What are the risks from the information sharing? Information surety is a paramount concern for transparency arrangements, not just for safeguards.[2]

Another concern is resilience, especially in how to deal with abnormal or unanticipated situations, such as accidents or system failures. There must be alternate communication channels for resolving various questions and problems. The arrangement must also be able to survive periods where the environment—outside the sharing arrangement—is not necessarily "cooperative."

How long is shared information available or retained? It is conceivable that information may also be used for safeguards. In that case, might there be there any conflicts?

Metrics--tools that can indicate objectively the value of transparency—are important to establishing its importance and justify sustaining the investment. Without them, it would be difficult to assess the cost/benefit of transparency.

Particularly bilateral arrangements should consider regional expandability: How might additional parties join the cooperation? At the very least, an arrangement needs to consider the "outside" environment, paying attention to how the sharing arrangement may be perceived by other states. Does the transparency arrangement itself need to be transparent to outsiders?

In certain situations, there may be a role for an intermediary. Can two parties cooperate directly, or do they require a trusted third party to facilitate an arrangement?

3. Technical implementation

All of the foregoing discussion suggests that the entire undertaking of transparency implementation entails a great deal of work. For an enduring solution, there are significant benefits to automating as much of the process as possible to reap cost efficiencies. If designed well, technical solutions to automate a transparency arrangement can do much more than simply collect, transmit and store data. Two aspects in particular are critical (1) the technical solution accurately implements the requirements of a viable sharing arrangement, and (2) that the solution reliably implements appropriate security for the intended sharing arrangement, which is key to promoting trust between the parties.

Comprehensive requirements for information sharing are essential to enable the design and development of a system solution. Any technical approach will need to identify and develop the technical building blocks for the information sharing, both the technologies (such as remote monitoring) and the procedural elements. The scope may involve research and development, training, prototype experiments, testing and other activities.

Implementation is concerned with what methods can be used to generate, authenticate, transmit, store, archive, access, protect and evaluate information. How are availability and reliability assured? How will the system be maintained? How to accommodate new technology developments or obsolescence? Personnel turnover? What approvals will be necessary? What testing will be required? The answers to all of these and other questions will comprise the functional requirements for an information-sharing network.

4. Discussion

4.1. Implications for safeguards

State to state and regional cooperation on nuclear nonproliferation might at first seem unnecessary, particularly to those who believe that the compliance-based safeguards system is fully sufficient. But the argument may be irrelevant, as various states are contemplating transparency measures anyway.[3] It is critical *how* they implement such information sharing, so that the likelihood of a benefit exceeds the possibility for negative impact. Although transparency could complement IAEA measures by addressing the kinds of questions the safeguards system is not designed to answer, there is (in principle) a risk that the two systems could give inconsistent messages.

4.2. Implications for regional systems

European safeguards under the Euratom treaty was a parallel development along with the IAEA system, yet has managed to evolve and continue under a partnership agreement with the IAEA. The Brazilian-Argentine Agency for Accounting and Control of Nuclear Materials (ABACC) was a special case that was instrumental in facilitating Argentina and Brazil's accession to the Treaty on the Nonproliferation of Nuclear Weapons (NPT); it too has managed to evolve and continue. There remains a possibility that other regional systems could appear, although it is not clear just what they would look like. Nevertheless, voluntary cooperation employing transparency is a distinct possibility. Nascent efforts at state-to-state cooperation in the area of nuclear nonproliferation could eventually mature into future regional systems. It is therefore timely that the technical details for implementation are given proper attention early in the development.

5. Summary

Voluntary information sharing ("transparency") between states is complicated, involving considerations from the point of view of the supplier state, the recipient state, and greater complexity when in an multilateral context. Many technical details are involved, and security measures are necessary to mitigate risks. Nevertheless, such nuclear nonproliferation cooperation can complement IAEA safeguards and strengthen the nonproliferation regime. A comprehensive, systematic approach is necessary to ensure successful implementation.

Acknowledgments

The author thanks past and present colleagues at Sandia National Laboratories, as well as many international partners in the U.S. Department of Energy's international nuclear safeguards collaborations with partners in the Asia-Pacific, South America and Europe, particularly with the Japan Atomic Energy Agency and the Korea Institute of Nonproliferation and Control, who have contributed valuable discussions related to the technical implementation of transparency. The International Nuclear Safeguards and Engagement Program of the U.S. National Nuclear Security Administration has been a generous sponsor of ongoing work by Sandia National Laboratories in this area. Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.

References

1. Wan Ki Yoon, "Technology Based Built-in Transparency Approach," presentation given at the Japan Atomic Energy Agency Transparency Workshop, Tokyo, Japan, 20 Feb 2008.

2. George Baldwin and Keith Tolk, "Information Security for Safeguards and Nonproliferation," paper presented at the 31st ESARDA Annual Meeting, Symposium on Safeguards and Nuclear Material Management, 28 May 2009, Vilnius, Lithuania.

3. Kazuko Hamada, “Transparency and nonproliferation in the Asia-Pacific region: Enhancing transparency, strengthening the nonproliferation regime,” Progress in Nuclear Energy 50 (2008) 660-665.