SAND2011-4021C

ADDRESSING THE INSIDER THREAT - A CALL TO INMM COMMUNITY ACTION

Ruth Duggan
Sandia National Laboratories[i]
PO Box 5800, MS-1361, Albuquerque, NM 87185-1361

ABSTRACT

While nuclear security systems have always faced outside threats, the insider threat still poses significant challenges to security. In March 2010, the Standing Committee on International Security of Radioactive and Nuclear Materials in the Nonproliferation and Arms Control Division conducted its fifth annual workshop on Reducing the Risk from Radioactive and Nuclear Materials. This workshop focused on the best practices and challenges addressing the insider element with respect to illicit radioactive materials trafficking, performance testing, and the secure transport of radioactive and nuclear materials. Presentations were made by invited panelists to discuss these best practices and to pose the challenges to be met. Working groups then identified technology gaps, policy gaps, and prioritized options for addressing these identified gaps. Participants included academia, policy makers, radioactive material users, physical security and safeguards specialists, and vendors of radioactive sources and transportation services. This paper summarized the results of the workshop with recommendations and calls to action for the Institute for Nuclear Materials Management (INMM) membership community.

INTRODUCTION

The world faces grave threats from nuclear terrorism ranging from terrorists threatening radiological release from nuclear materials to improvised nuclear devices to use of a stolen nuclear weapon. The consequences of these threats underscore the need for the strongest protection measures. Yet, the strongest measures can be circumvented by a determined insider. Sixty-one participants at the 5th Annual Workshop on Reducing the Risk from Radioactive and Nuclear Materials sought to address the insider threat from the perspectives of illicit trafficking, transportation security and performance testing.

WHO IS THE INSIDER THREAT?

Just who is this insider threat that causes such grave concern? When the question was asked of the participants, the answer "All of us!" was quickly derived. What does this mean? While it is easy to identify those persons who handle materials as the most serious threat for theft and those who handle safety systems for sabotage, it became clear that the possibility of introducing and exploiting vulnerabilities could happen throughout system lifecycles. This means that potential insiders include policy makers, designers, regulators, inspectors, operators, maintenance personnel, and other support personnel. Indeed, on a day-to-day basis, most facility operations and material movements involve people. Anyone with access to the system throughout its life cycle might be considered an insider threat. Insiders can take advantage of their access rights,

have knowledge of the facility, its practices and operations, can identify other staff to assist them, and have plenty of time.

Recognizing the potential for anybody with access, whether physical or virtual, to be a threat to nuclear facilities, the participants were then asked to consider the following questions from the perspective of illicit trafficking, transportation security, and performance testing:

1. What are you willing to give up to prove that you are not a threat?
2. What do you need to keep you from becoming a malicious insider?
3. What do our organizations need to do to

    - identify vulnerable employees?
    - prevent coercion that might exploit employee vulnerabilities?
    - support employees if they are targeted?

CHALLENGES IN NUCLEAR SECURITY REGARDING THE INSIDER THREAT

Because insiders already posses the access, skills, and knowledge to carry out authorized activities, it can be very difficult to detected illicit activities such as protracted theft or to separate an accident or error from a malicious act. The only difference in some cases of insider actions may be malicious intent. While arguably the greatest challenge to nuclear security, the very persons considered the greatest potential threats, are also the greatest contributors to security, particularly within a strong nuclear security culture. Yet, in addressing the insider threat, we must be mindful of unintended consequences that may introduce vulnerabilities into the system or make systems less safe in the interest of security.

ILLICIT TRAFFICKING

Historically, many illicit trafficking cases involving targeted theft of radioactive and nuclear material have been perpetrated by insiders acting either singly or with others and most often for financial gain or revenge. Several programs now exist to assist countries with addressing the insider threat after material has been stolen and entered the illicit trafficking market.

Because the insider is systemic, a systems approach to addressing the insider is required. The Nuclear Smuggling Outreach Initiative within the US Department of State is using a holistic approach with each partner country to improve capabilities in regulatory infrastructure, detection, and response and to strengthen regional cooperative efforts through political commitment to addressing illicit trafficking.

The Global Nuclear Detection Architecture Program in the Domestic Nuclear Detection Office within the US Department of Homeland Security proposed that domestic programs to detect illicit materials are best performed in a global context. A stronger legal and regulatory

framework and better trained law enforcement lead to a more effective detection program. Such a program is based on international cooperation in intelligence gathering on the threats to nuclear materials, better detection, interdiction, and attribution; and forensics. This program is working to provide model guidelines for domestic architecture programs that support this global approach.

It was suggested that generally, nuclear materials are well protected at nuclear facilities and that significant improvements have been made in detecting radioactive materials at country borders; however, once unauthorized removal of material has occurred, there is little done in detecting nuclear materials within a country's borders. For this situation, it was proposed that countries with nuclear or radioactive materials have a mobile, rapid-response expert team to provide frequent and random sampling for radioactive materials and to assist in all phases of response once material is discovered. Understanding the pathways materials might take using existing high traffic, commercial routes or smuggling routes can help guide where to deploy rapid detection and response teams. These teams should be able to determine the type of material and its potential consequences and begin the forensics process to identify the source of the material, where it has been, and who had it prior to its discovery.

A global effort is required to aggressively investigate all allegations of nuclear or radioactive materials smuggling, to coordinate with all agencies involved with nuclear and radioactive material and law enforcement, and to promptly update international partners for national level threat assessments. The key to a successful interdiction program is a global detection and response structure to deal with illicitly trafficked materials in a safe and secure manner before significant consequences result.

TRANSPORTATION SECURITY

Global nuclear expansion also means an increase in nuclear material transportation. Nuclear materials are generally considered more vulnerable in transport than when contained in a nuclear facility. Protective measures, largely delay and response, to protect nuclear materials during transport are designed for an outsider. However, with a few modifications, such systems can work equally well against insiders. For example, if all access to the materials is limited to only entities at origination or destination, then the delay features in transportation systems work equally well for the outsider and insider on the transport team. A minimum of two man-rule evoked for transportation operations works to thwart a single insider threat.

A particular challenge comes when considering how much information to share with the transportation team regarding the cargo they are carrying. With less information and a controlled set of drivers, the knowledge base of the insider is limited, thereby reducing the interest in this particular cargo. However, by knowing what the cargo is, the transportation team better understands its significance and their role in protecting such material from either threat.

One proposal was to designate a universal monitoring system with a robust tamper-indicating device to effectively track UF_6 cylinders. This system must address the multiple identifiers currently on cylinders since identification labels are not consistent across manufacturers or countries and legibility can be affected by harsh environmental conditions. The adoption of a global standard to a unique identification number will render tracking these cylinders across international borders more effective. Because there are a limited number of cylinder manufacturers, an international database for UF_6 cylinders could be maintained independently of the cylinder handlers.

Just as transportation systems are designed to thwart an outsider attack, they should also be designed to counter malicious acts perpetrated by the insider. Mechanisms for detecting malicious insider acts, responding to such events, and mitigating the consequences of insider-involved sabotage of transportation shipments must be included in the transportation security system design. The mechanisms most advocated by workshop participants were limiting the information the transportation team has about the shipment, reducing the ability of an insider to act alone to achieve goals, and making transportation containers robust against sabotage events designed to effect a release of radioactivity.

PERFORMANCE TESTING FOR THE INSIDER

While it is relatively straightforward to measure the performance of technology, it is much more difficult to measure the effectiveness of the human elements of security. A design basis threat is often used as the metric for performance of a physical protection system. Protection measures such as limiting access and privileges to the minimum needed to perform a specific job, human reliability programs, exercising need-to-know policies, and two- or three-man processes serve to limit the ability of a single insider to accomplish a malicious act. For these protection systems, performance is only based on what is detected without an understanding of what has not yet been detected. Computer-based simulations offer a capability to examine system performance including response to such events.

The most credible insider scenarios include the following potential insider threats:

- Employees handing nuclear material
- Nuclear material accountancy and control system specialists
- Physical protection specialist
- Mid-level managers

Just as with the malicious outsider, the malicious insider scenario begins with data collection and situational analysis. The insider tends to be more opportunistic to achieve covert possession of nuclear material. Such Covert possession involves defeating the physical protection system and information systems associated with nuclear materials accountancy and control. Thus, every process involving material handling or physical security should be examined for how the system

could mask or detect malicious insider activity, whether being perpetrated by a single insider or a collective insider.

General security performance testing requirements are based on a system performance standard against a particular threat and what the system must accomplish. Just as the system is modeled and tested against various outsider scenarios, the system should be analyzed against an insider by examining how the insider must get the material out. Every material operation must be analyzed to determine pathways out of the facility. The approach to insider mitigation must be multi-faceted and include opportunities to detect unauthorized activities at multiple layers. In particular, material control provides the means to prevent or detect loss of material when it occurs or soon afterward. Thus material control features should be multi-layered to eliminate the consequences of a single-point failure, coordinated with accounting, physical protection safety, and operations. Many material control and accounting elements may be considered performance tests of the system through random physical inventories, evaluation of system/receiver differences, and item monitoring. Anomalies must be identified, investigated and resolved. The risk of the insider threat can be mitigated by recognizing material control and accounting as more than just accounting.

Many of the security measures dealing with the insider are associated with nuclear security culture. One aspect of security is the organizational environment which can either foster security conscientious employees or foster disgruntled employees. Organizational excellence was proposed as a nuclear security culture metric for consideration. Organizational excellence looked at the factors listed in Table 1.

Table 1. Organizational Excellency Factors

- Benefits packages that attract and retain employees
- Diversity acceptance
- Employee development
- Employee engagement
- Job satisfaction
- Salary/overall compensation package
- Physical environment
- Quality culture
- Support of teaming
- Supervisory relationships
- Strategic posture

INMM CALL TO ACTION

As a result of working group discussions, the participants determined that the following investments should be made:

- Attention to the well-being of the people working in the nuclear industry – People operating in a strong security culture who are satisfied with their jobs are less likely to become insider threats. In particular, the need was recognized for:
    - strong programs to support employees in potentially vulnerable situations and to report suspicious behavior and

    - good compensation packages for workers in this industry.
- Process analysis for transportation and material movement activities to minimize the potential for undetected insider malevolent acts – Processes that limit human interaction or single human operations are less vulnerable to malevolent insider manipulation.
- Continued efforts toward a global system for the protection, detection, and interdiction of nuclear and radioactive materials – Because the actions of the insider may be the most difficult to detect in a timely fashion:
    - global detection architecture, including tracking of material containers, to assist in the detection of these materials at borders
    - rapid response teams to assist in the detection of radioactive materials between facilities and borders and to appropriately respond to discovery of these materials depending on the circumstance.

CONCLUSIONS

In nonproliferation, "Trust but verify" is a well understood tenet that also applies to addressing the insider threat. The best defense against the insider is developing a strong nuclear security culture in which the impacts of any threat are both well understood and taken personally by staff and everyone is invested in providing a safe and secure environment for nuclear materials. Technology should be carefully designed and implemented so that it cannot be changed or bypassed by employees. Measures should include safety and safeguards systems such as proliferation resistant processes and systems that alarm when system operational behaviors exceed strict thresholds. The goal of these security measures is to present the insider with sufficient uncertainty of success that he will chose not to make the attempt in the first place. If the insider is not dissuaded, then security of these materials must rely on detection, interdiction, and attribution. While efforts to reduce available fissile material should continue, a global partnership on the tracking, detection, and interdiction of nuclear and radioactive materials should be encouraged to provide an international solution.

Lastly, as part of a strong nuclear culture, most employees are doing the right thing. As with any venture, there will be some who will seek to subvert the system. We should strive to make the goals of a malicious insider difficult to achieve and unattractive to contemplate. Additionally, as part of a nuclear security culture, we are all part of the detection system that identifies when things are not as they should be. It is incumbent upon us to build a culture of trust that enables self-reporting of employee vulnerabilities as well as reporting suspicious behavior that can be addressed with discretion.

THE NEXT WORKSHOP

Plans are already underway for the 6th Annual Workshop for Reducing the Risks from Nuclear and Radioactive Materials. The topic of the Insider Threat will again be addressed, but from a detection, delay, response, and mitigation perspective. In addition to physical protection professionals, the standing committee especially seeks the participation of facility operators for

smaller facilities and health physicists. The workshop in planned for February 6-8, 2012 in Washington DC.

ACKNOWLEDGEMENTS

The author gratefully acknowledges the contributions of the workshop panel chairs: Galya Balatsky, Steve Bellamy, and David Lambert for the successful workshop and the participation of our international colleagues to ensure that the discussions maintained an international perspective. Gratitude is given for the excellent job performed by William Charlton, Jessica Feener, and the student chapter at Texas A&M in hosting this workshop.

---

[i] Sandia National Laboratories is a multi-program laboratory operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL8500.