Using an NMAC System Enhanced for Nuclear Security to Mitigate the Insider Threat

Martha Williams, Sandia National Laboratory (Contractor)
Noah G. Pope, Sandia National Laboratory (Contractor)
Lia Brodnax, Los Alamos National Laboratory

Abstract

Nuclear security systems are designed to protect against theft or other unauthorized removal of nuclear material from nuclear facilities. Reports from the IAEA Incident and Trafficking Database suggest that most known instances of theft have involved a malicious facility insider. One means of accomplishing the goal of protecting nuclear material from an insider is for States and nuclear facilities to enhance their established Nuclear Material Accounting and Control (NMAC) programs to meet nuclear security objectives. An NMAC program enhanced for nuclear security is essential to detecting loss or theft of nuclear material, aiding in recovery of lost or stolen nuclear material, and providing information about material type and quantity that is necessary for resolving questions of theft. An enhanced NMAC program also helps to deter acts by malicious insiders, because insiders know that malicious acts will be detected by NMAC measures designed specifically to detect attempted theft. The process NMAC uses for nuclear security is to establish a system of conditions through rules, procedures, and technical measures, so that when conditions become off-normal, an irregularity is declared and must be formally investigated. Examples of off-normal conditions include failure to obtain authorization to access a nuclear materials area, violation of a two-person rule, or discovery of a broken tamper-indicating device. In a facility with an NMAC program enhanced for nuclear security purposes, a situation such as one of these off-normal conditions would be investigated until it was proven that the situation was not a malicious act caused by an insider. This paper presents tools being developed by the U.S. Department of Energy's National Nuclear Security Administration's Office of Global Material Security (DOE/NNSA/GMS) for assisting States and facilities in enhancing existing NMAC systems at nuclear facilities to mitigate the insider threat.

1. NMAC and the Insider

Protecting nuclear material from a facility insider intent on misusing it is a major focus of nuclear security. Nuclear Material Accounting and Control (NMAC), a system that already exists at most nuclear facilities, can be used to support nuclear security, including mitigating the insider threat. (NMAC is also sometimes referred to as MC&A.) A facility's existing NMAC system measures, which were originally established to meet international safeguards obligations, may not be sufficient for nuclear security; however, with enhancements to the existing system, NMAC can play a critical role in detecting and deterring malicious activities by a facility insider.

Each State that has a Safeguards Agreement with the IAEA has committed to establishing a State System of Accounting and Control (SSAC). In turn, nuclear facilities in the State are required to have systems that enable them to account for and control the nuclear material in their possession, i.e., NMAC systems. NMAC accounting data provide the information used for preparing reports

concerning a facility's nuclear material holdings, which are submitted to the State competent authority and then submitted by the State to the IAEA.

NMAC was originally developed in the 1950's as a means of responding to the concern that States could develop nuclear weapons programs. In the 1950's it was believed that only States had the resources (financial, scientific, and technological) to manufacture nuclear weapons. By the early 2000's it was clear that a non-State actor might also pose a threat. A well-funded organization or even a group of individuals might illegally acquire a nuclear weapon and detonate it, steal nuclear material to build a nuclear weapon, or use illegally obtained nuclear material to construct an improvised nuclear device or radiological dispersal device (a dirty bomb).

Changed Assumptions Require a Changed Response. In response to the threat posed by a non-State actor, who might even be a facility insider, the response taken by the IAEA has been increased emphasis on the role played by nuclear security in protecting nuclear facilities and nuclear material. This included increased emphasis on the role of NMAC in providing for the security of nuclear material.

The facility NMAC system can also be used to support nuclear security. IAEA Nuclear Security Series (NSS) No. 13, *Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5)*, paragraph 2.1, states that "The objectives of nuclear security are to protect against unauthorized removal of nuclear material, locate and recover missing or stolen nuclear material, protect nuclear material and nuclear facilities against sabotage, and mitigate the radiological consequences of sabotage."

Whether or not an established NMAC system at a nuclear facility is adequate from a nuclear security point-of-view depends on the extent to which it includes the elements and measures that are described in this paper and, in more detail, in the IAEA Implementing Guide, *Use of Nuclear Material Accounting and Control for Nuclear Security Purposes at Facilities*, NSS No. 25-G. The objective of NSS 25-G is to "describe how to use an NMAC system at a nuclear facility to enhance nuclear security by detecting in a timely manner any unauthorized removal of nuclear material and providing deterrence against such possible actions." The importance of implementing nuclear material controls is described extensively in the IAEA's nuclear security publications. Accounting and control are both of major concern to maintaining the security of nuclear material. Quickly resolving questions concerning indications of missing nuclear material requires a robust NMAC system that maintains complete and detailed records.

2. Nuclear Security Relies on NMAC

The focus of an NMAC system for nuclear security is to establish measures to mitigate the risk posed by an insider intent on stealing or misusing nuclear material. Protecting nuclear material by erecting walls, fences, vaults, and other barriers is the obvious way to keep it inside a nuclear facility. But walls and fences cannot protect nuclear material from a determined malicious active insider who has authorized access to conduct work inside those barriers. Even a nuclear facility with the best physical protection system in the world – best guns, toughest fences, and smartest guards – is vulnerable to malicious acts performed by an insider.

A facility's existing NMAC program can be enhanced (as described in Section 3 below) to deter and detect actions taken by an insider intent on stealing nuclear material or assisting an outsider. An NMAC program enhanced for nuclear security is essential to detecting loss or theft of nuclear

material. It is also necessary for providing information about material type and quantity that is necessary for resolving questions of theft and for aiding in recovery of lost or stolen nuclear material. If there is a question concerning whether nuclear material has been lost or stolen from a facility, the question can only be answered definitively if there are records that document the type and quantity of nuclear material at the facility. NMAC measures can also deter theft by an insider. Knowledge that the NMAC system is likely to detect the theft and "catch them in the act" should deter many potential malicious insiders.

NMAC and the Insider. In the context of nuclear security, an insider is a person with access to or information about a nuclear facility or nuclear material. An insider may be a manager, an operator, janitorial staff, or in any other position in the facility. An insider may be an escorted visitor. An insider may also be someone working with or providing information to an outsider. What distinguishes an insider from an outsider is access. Access may be physical access or even remote access, such as computer access.

NMAC and the Outsider. Physical protection systems and armed response forces at nuclear facilities are designed to prevent an outsider from gaining access to nuclear material. However, if a nuclear facility is attacked by outsiders, physical protection cannot provide information necessary for determining if nuclear material was stolen or lost. Information maintained in the NMAC system is necessary for resolving questions of theft or loss, whether theft by an insider or outsider.

NMAC's Contribution to Nuclear Security. Without the information provided by NMAC, resolving indications of possible theft or misuse would be impossible. If nuclear material is stolen, NMAC provides information about what has been stolen – material type, form, and quantity – which is critical to ensuring that recovery of the material is complete. NSS 13 recommends in paragraph 3.26, "The operator should ensure control of, and be able to account for, all nuclear material at a nuclear facility at all times." The NMAC system makes this possible. The NMAC system should include measures to account for all nuclear material through receipt, storage, handling, use, and final disposition; and the NMAC system should include administrative and technical measures to control nuclear material during all activities.

The information a facility nuclear security system needs about the facility's nuclear material is most readily available in the NMAC system. NSS 25-G states in paragraph 1.7, "The primary objective of an NMAC system is to maintain and report accurate, timely, complete and reliable information on all activities and operations (including movements) involving nuclear material. This information should include the locations, quantities and characteristics of nuclear material at the nuclear facility. The goal is to maintain control over the nuclear material to ensure continuity of knowledge, and thereby to enhance the ability to deter and detect unauthorized removal of nuclear material."

Nuclear security is concerned with the non-State actor. Nuclear security is concerned with theft or misuse of quantities of nuclear material much smaller than what is needed for a nuclear weapon. For nuclear security, detection is timely if it prevents successful completion of theft or misuse of nuclear material.

3. Enhancing NMAC for Nuclear Security

Enhancing an existing NMAC system so that it will be effective for nuclear security begins with assessing the different NMAC elements that are already in place. NSS 25-G lists (in Chapter 4) the elements of an NMAC system that are necessary for nuclear security and describes enhancements

that make a facility NMAC program more effective for nuclear security. Figure 1 presents an outline of the elements and measures, both technical and administrative, described in NSS 25-G:

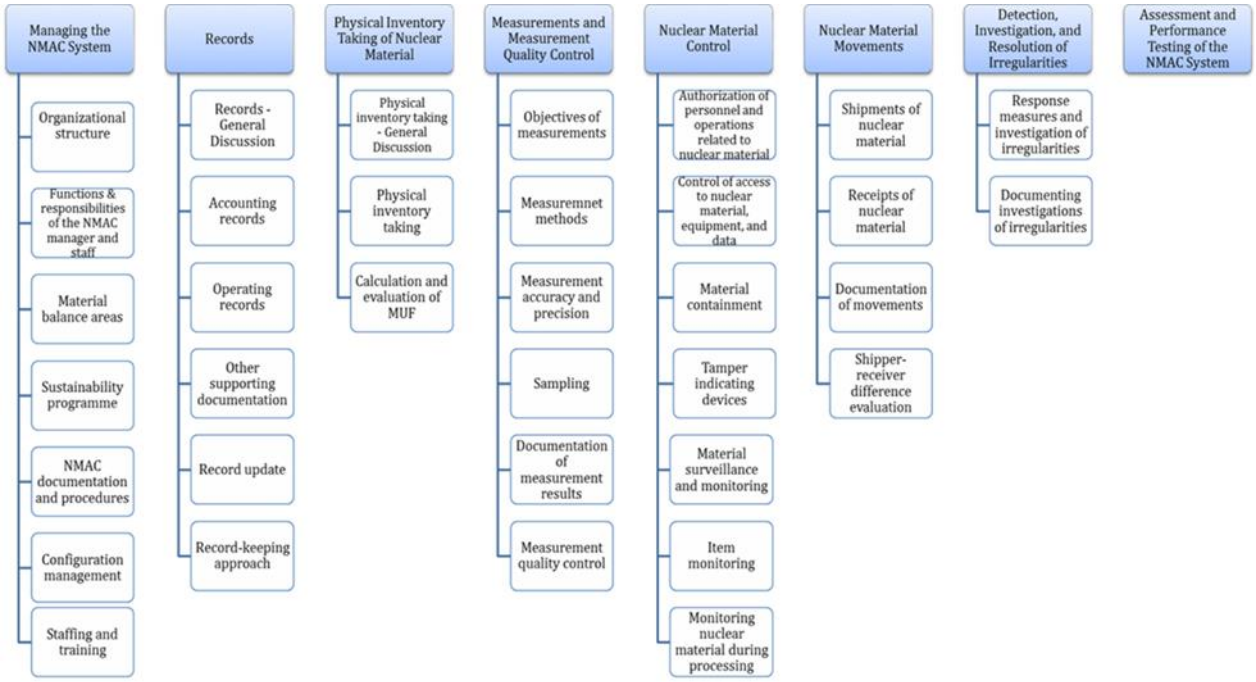

Figure 1: Technical and Administrative Elements Supporting Nuclear Security

A State or facility can (and should) evaluate its existing NMAC system to determine if it is adequate for nuclear security. Some of the measures used to enhance an NMAC program and make it effective for nuclear security are described in the following paragraphs. The list is not comprehensive. More detail is available in NSS 25-G.

Managing the NMAC System. The person who is appointed to manage the facility NMAC system (the NMAC Manager) should be trained to recognize the insider threat and the importance of NMAC in insider threat mitigation. The NMAC manager should be independent from the managers of other facility departments, especially the operations organization, to avoid potential conflicts of interest. The facility NMAC program should be described in detail in a written NMAC Plan, which should be subject to approval by the State authority. The existing material balance area (MBA) structure may need to be subdivided so that the physical areas where a potential loss or theft occurs is more limited, making investigation easier. Staffing of the NMAC organization should be adequate to assure that nuclear security concerns are met. NMAC staff and management should be trained and qualified. Facility management should promote a strong working relationship between the NMAC organization and the other facility organizations involved in activities related to nuclear material. All facility personnel should have a clear understanding of the importance of NMAC to the security of nuclear material.

Records. Records, whether hand-written or computerized, are the foundation of the NMAC system. Accurate, complete, and timely records are essential for resolving any incident involving nuclear material. The facility should prepare a record of every nuclear material item received and the item record should be updated for every activity it is involved in. The signatures of the person conducting the activity or making the change and a witness should be part of the record. A complete history of all nuclear material items should be readily available, including quantity, type, form, and exact location. Records should be up-to-date, and changes should be recorded as soon as possible after they occur. The records system should be capable of quickly creating a list of the current inventory. Measures should be taken to prevent falsification of records. Records should be backed-up and protected. The records system should be secure. Only authorized individuals should have access to NMAC records.

Physical Inventory Taking of Nuclear Material. The facility operator should conduct periodic physical inventory taking (PIT) of all nuclear material in every MBA. The frequency should depend on quantity and nuclear material category and should be decided upon by the State authority. If conducted correctly, the PIT confirms the presence of nuclear material listed in the nuclear material records (the book inventory) and provides evidence that the facility NMAC system has been effective. For PIT every nuclear material item is physically identified, producing a list of the physical inventory. The items listed in the records should match one-to-one with items listed during the PIT and any difference should be investigated. The results of the PIT should be compared with the book inventory, including evaluation of the material balance. Plans should be in place for conducting an unscheduled PIT, if necessary. An unscheduled PIT might be necessary if an alarm occurs, e.g., a critically alarm that required an evacuation, a claim by someone outside the facility that nuclear material has been stolen from the facility, or an indication that nuclear material is missing or not in its assigned location.

Measurements and Measurement Quality Control. Knowledge of nuclear material quantities helps to deter and detect unauthorized removal. Accurate and precise measurements are important to nuclear security because they reduce measurement uncertainties, which could conceal unauthorized removal. Measurements are especially important for facilities that process nuclear material. Effective nuclear security depends on accurate, timely and complete information regarding the facility's nuclear material inventory.

Nuclear Material Control. The primary purpose of nuclear material control measures is to maintain continuity of knowledge of the nuclear material. Control measures are established to deter and detect any actions that could lead to unauthorized removal or misuse of nuclear material. They are the most effective tool against an insider who intends to steal or misuse nuclear material. NSS 25-G describes many types of control measures, some of which are mentioned here. IAEA technical guidance document NSS No. 32-T, *Establishing a System for Control of Nuclear Material for Nuclear Security Purposes at a Facility during Use, Storage and Movement* has more detailed guidance on the use of controls for protecting nuclear material, especially from an insider.

Measures that control who has access to nuclear materials are essential to nuclear security. They help detect unauthorized handling or movements. An effective nuclear material control program can make it possible to identify problems in time to provide for detection and response. Control measures deter theft because the insider knows that controls are in place to detect malicious acts.

Containment can be used to delay access to nuclear material. Tamper-indicating devices (TIDs) can be used as a means of detecting unauthorized access to contained nuclear material. Examples of

containment include vaults, cans, buckets, tanks, storage pools, shipping casks, fuel assembly structural components, etc. When nuclear material is not being used, it should be stored in a vault or other room that can be locked and sealed with a TID. A broken TID would "sound an alarm".

All activities involving nuclear material should be authorized in writing. Separation of duties serves as an additional measure to deter and detect insider threats. Use of a "two-person rule" is another way of deterring an insider.

Records should be prepared and maintained of all NMAC control activities. For example, records should be kept of access to a vault or room where nuclear material is stored. Control records should be subject to a two-person rule. Records of control are extremely important in conducting an investigation if there is an indication that nuclear material has been stolen, because they provide information concerning who has had access to the nuclear material.

Item and process monitoring programs should be established, depending on the type of facility, to monitor nuclear material between PITs. Item monitoring is a program where the location and integrity of a statistical random sample of items are verified between PITS, thus increasing the likelihood of detecting unauthorized removal of nuclear material between PITs.

Control elements are often administered jointly by NMAC and physical protection. This makes communication, cooperation and coordination between the two organizations very important. Responsibilities may be defined by the State competent authority. Some of the areas where physical protection and NMAC may share responsibility are control of access to areas where nuclear material is present, use of material containment and surveillance, key control, and use of radiation portal monitors and metal detectors.

Nuclear Material Movements. Nuclear material is more vulnerable to theft by an insider during movement than at any other time and movements should be subject to extensive accounting and control measures. All movements, even movements within the facility, should require written authorization. Complete records should document all movements of nuclear material including re-locations within an MBA, movements between MBAs, and shipments to another facility. Facilities should establish measures to provide assurance that unauthorized removal during movements will be detected. Procedures should be developed to verify prior to shipment off-site that shipping containers labelled as empty are actually empty and that items removed from a nuclear material area that are identified as non-nuclear are truly non-nuclear. All shipping activities should be subject to oversight by NMAC and physical protection personnel who are knowledgeable about NMAC requirements and are capable of recognizing unauthorized activities.

Detection, Investigation and Resolution of Irregularities. NSS 25-G defines an irregularity as "An unusual observable condition which might result from unauthorized removal of nuclear material, or which restricts the ability of the facility operator to draw the conclusion that unauthorized removal has not occurred." The process NMAC uses for nuclear security is to establish a system of conditions through rules, procedures, and technical measures, so that when conditions become off-normal, an irregularity is declared which must be formally investigated. Examples of off-normal conditions include discovery that a nuclear material item is not in its recorded location, a broken TID on the door to a storage area, an unexplained difference between the book inventory and the physical inventory, failure to obtain authorization to access a nuclear materials area, violation of a two-person rule, an unauthorized change to NMAC records, trends such as consistent losses calculated in the material

balance, etc. The list of possible irregularities is extensive – a violation of any NMAC measure can result in an irregularity. In a facility with an NMAC program enhanced for nuclear security purposes, a situation such as one of these off-normal conditions would be investigated until it was proven that the situation was not a malicious act caused by an insider.

Observation of an irregularity serves as a "trigger" that starts an investigation. NMAC for nuclear security depends on identification and investigation of irregularities as a means of mitigating the insider threat. Any irregularity, even one that seems harmless, might be an indication that an insider is attempting to steal nuclear material or "testing the system" to see if the irregularity caused by the attempt will be caught. All irregularities should be investigated.

Assessment and Performance Testing of the NMAC System. The NMAC system measures and elements should be subject to periodic assessments and performance tests. The frequency of the assessments should be established by the State competent authority. Assessments should also be conducted when changes are made to the system.

4. State Responsibility for NMAC

Responsibility for nuclear security rests with the State. The 2006 *Amendment to the Convention on the Physical Protection of Nuclear Material* states that "The responsibility for the establishment, implementation and maintenance of a physical protection regime within a State Party rests entirely with that State". This includes responsibility for the protection of nuclear material. Consistent with this international nuclear security instrument, NSS No. 20, *Objective and Essential Elements of a State's Nuclear Security Regime: Nuclear Security Fundamentals*, states that each State is responsible for its own nuclear security regime: "Responsibility rests with the State for meeting the [nuclear security] objective … by establishing, implementing, maintaining and sustaining a nuclear security regime applicable to nuclear material, other radioactive material, associated facilities, and associated activities under a State's jurisdiction." If nuclear material is lost or stolen, the State (and the facility) are responsible for investigating and, if possible, returning the nuclear material to a situation where it will be under control.

Part of the State responsibility is developing a legal and regulatory framework for NMAC that is effective for nuclear security. New regulations may be necessary to meet the State's goals and objectives for nuclear security. NMAC regulations established by the State should be consistent with a graded approach and defense-in-depth. That is, more stringent measures should be taken to account for and control more attractive nuclear material (material with greater consequences resulting from a malicious act) than those applied to less attractive material.

The facility NMAC system should be subject to oversight by the State's competent authority, including periodic inspections and evaluations of the NMAC system elements and measures in place at the facility to ensure that the nuclear security objectives are met.

5. NMAC and Other Facility Organizations

Because NMAC responsibilities and activities often overlap with that of other facility organizations, communication, cooperation, and coordination are essential.

Coordination with Physical Protection. Because NMAC and physical protection elements and measures sometimes overlap, they must be coordinated. Clear lines of communication and responsibility should be established and maintained between NMAC and physical protection

personnel. If nuclear material is stolen, both NMAC staff and physical protection staff will be involved in the response. Other examples of areas where both NMAC staff and physical protection staff play a role or have an interest are control of access to nuclear material and areas where nuclear material is used or stored, use of surveillance equipment (e.g., cameras), response to a nuclear security incident, use of a two-person rule, key control (e.g., keys to equipment used to move heavy items), etc. Facility procedures should clearly define specific responsibilities when there are overlaps, including how information is shared.

Coordination with Safeguards. One NMAC system should be sufficient for a facility, but that single system can be used for both IAEA safeguards and nuclear security. NMAC staff should be aware of the two different purposes and their equal importance. For nuclear security, the NMAC system should provide complete and up-to-date information about all items of nuclear material. Necessary information includes exact locations, quantities, and types and forms of the nuclear material items. The purpose of the information is to discourage and detect any attempt by a malevolent insider to steal or misuse nuclear material. For nuclear security, accounting records should be able to resolve indications of missing material quickly. Suppose a facility receives a phone call alleging that nuclear material has been stolen. If NMAC records have been maintained as required for nuclear security, the facility should be able to assess the allegation and respond in near-real-time. Timeliness is of utmost importance to nuclear security.

6. NMAC and the Insider

NMAC helps prevent theft by an insider. Figure 2 illustrates how an NMAC system enhanced for nuclear security can detect and deter insider activities.

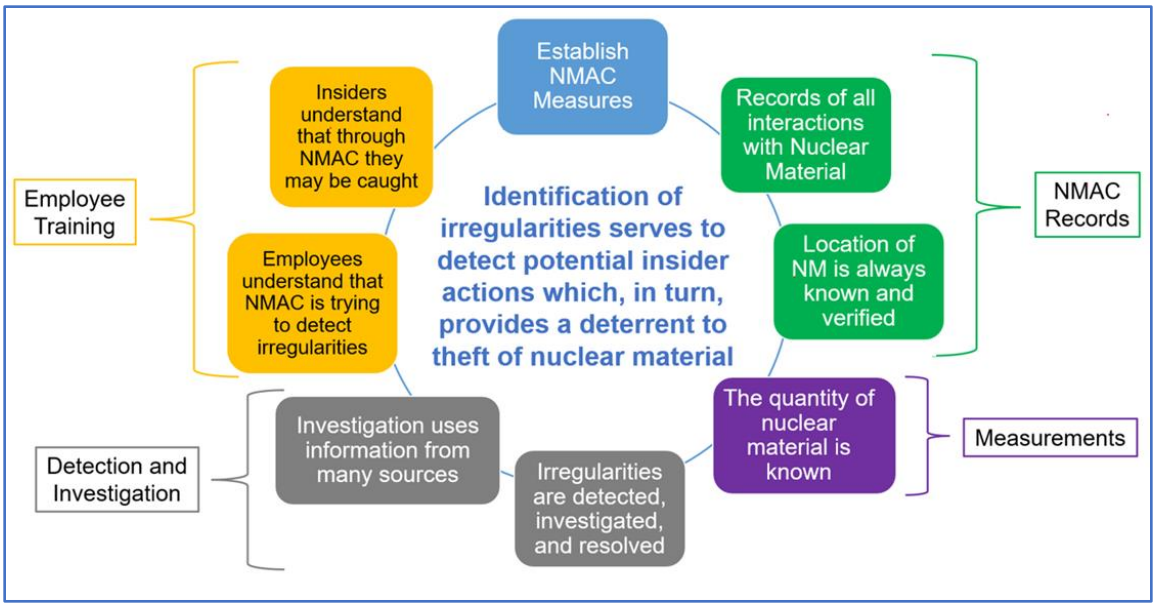

Figure 2: NMAC Helps Prevent Theft by an Insider

The State is responsible for establishing NMAC regulations that ensure the security of nuclear material. Facilities are responsible for establishing NMAC measures that implement the regulations.

Records should be maintained of all nuclear material and all activities involving nuclear material. To detect and deter theft or other malicious activities involving nuclear material by an insider, it is important that the exact location and quantity of all nuclear material is known and that records are maintained describing all activities involving nuclear material. Failure to comply with NMAC measures and controls creates an irregularity which may indicate that an insider activity is in progress. All irregularities should be investigated and resolved. If facility personnel are trained and aware that NMAC will detect malicious actions, the potential insider will be deterred.

7. Summary: NMAC's Importance to Nuclear Security.

A facility NMAC system used for nuclear security maintains and reports accurate, complete, up-to-date, and reliable information about its nuclear material and all activities involving its nuclear material. A facility NMAC system used for nuclear security ensures continuity of knowledge of nuclear material by maintaining control over it. NMAC measures can reveal irregularities, which "trigger" prompt investigations and enable detection of malicious insider activity. NMAC can act as a deterrent to insider theft because of increased likelihood of detection. In resolving a nuclear security incident, NMAC can provide valuable information on types, quantities, and specific locations of nuclear material items. Effective use of NMAC elements and measures enhances nuclear security.

8. Tools Developed for Assessing an NMAC System

The U.S. Department of Energy's National Nuclear Security Administration's Office of Global Material Security (DOE/NNSA/GMS) has developed tools for assisting States and facilities in enhancing existing NMAC systems at nuclear facilities to mitigate the insider threat. Cooperative programs include joint workshops, system design, training and upgrades related to nuclear security and NMAC.