Proceedings of the INMM & ESARDA Joint Annual Meeting
May 22-26, 2023, Vienna, Austria

GOOD PRACTICE GUIDANCE FOR NUCLEAR MATERIAL ACCOUNTING AND CONTROL MEASURES USED TO MITIGATE INSIDER THREAT AT RESEARCH REACTORS

Rachel Hunneke
Oak Ridge National Laboratory

Joel Lewis
Lawrence Livermore National Laboratory

ABSTRACT

The International Atomic Energy Agency (IAEA) Nuclear Security Series No. 25-G Implementing Guide titled "Use of Nuclear Material Accounting and Control for Nuclear Security Purposes at Facilities" and No. 32-T Technical Guidance titled "Establishing a System for Control of Nuclear Material for Nuclear Security Purposes at a Facility during Use, Storage and Movement" describe enhancements or measures that can be added to an existing facility nuclear material accounting and control (NMAC) system to provide additional opportunities for increased nuclear security via timely detection of unauthorized removal of nuclear material. These documents also provide information about how the enhanced NMAC system can be used to provide deterrence against such possible actions. The guides also note that an NMAC system used to support nuclear security has primary objectives for (1) maintaining and reporting accurate, timely, complete, and reliable information on nuclear material; (2) maintaining control over the nuclear material; (3) providing the basis for investigation and resolution of any irregularity indicating a possible loss of nuclear material; and (4) providing information helpful to the recovery of missing material. Although this information is very useful, it needs to be complemented with a set of technical and administrative measures that provides insight about what constitutes an effective NMAC system used to support nuclear security. The US Department of Energy's National Nuclear Security Administration's Office of Global Material Security (DOE/NNSA/GMS), Nuclear Material Accounting and Control Functional Team has reviewed the guidance contained in NSS 25-G and NSS 32-T to develop a set of technical and administrative measures that an operator could consider when designing an NMAC system to support nuclear security for research reactors. This set of technical and administrative measures can also be considered by the competent authority to develop regulations and guidance for item facility operators that provide for an effective national mitigation strategy for detecting and deterring insider threat. This paper describes the processes that were used to identify the mitigation measures and how they can be incorporated into the design of an NMAC system used to support nuclear security for research reactors.

INTRODUCTION

Hundreds of research reactors exist across the world, and although they are smaller than typical nuclear power reactors, it can be challenging to implement nuclear material accounting and control (NMAC) for nuclear security at these types of facilities. A facility NMAC system can be enhanced to contribute to the facility's nuclear security and has an essential role in protecting the facility. A facility can support nuclear security by enhancing its existing NMAC system to prevent, detect, and respond to malicious actions and insider threats. Research reactors are represented by a wide variety

Note: This manuscript has been authored in part by UT-Battelle, LLC, under contract DE-AC05-00OR22725 with the US Department of Energy (DOE). The publisher acknowledges the US government license to provide public access under the DOE Public Access Plan (http://energy.gov/downloads/doe-public-access-plan).

of designs and purposes, so the nuclear security and NMAC systems will be unique to each facility, which can make the task of designing and implementing these systems and measures more challenging.

The importance of nuclear material accounting and control (NMAC) for nuclear security is recognized by the International Atomic Energy Agency (IAEA), which provides useful references about NMAC and nuclear security. IAEA references include the following examples:

- The IAEA Nuclear Security Series (NSS) No. 25-G Implementing Guide titled "Use of Nuclear Material Accounting and Control for Nuclear Security Purposes at Facilities"
- The IAEA Nuclear Security Series (NSS) No. 32-T Technical Guidance titled "Establishing a System for Control of Nuclear Material for Nuclear Security Purposes at a Facility during Use, Storage and Movement"

These guides will be referred to as NSS 25-G and NSS 32-T, respectively. The guidance provided in these documents describes enhancements or measures that can be added to an existing facility NMAC system to provide additional opportunities for increased nuclear security via timely detection of unauthorized removal of nuclear material. It also provides information about how the enhanced NMAC system can be used to deter against such actions. This guide also notes that an NMAC system used to support nuclear security has the following primary objectives: (1) maintaining and reporting accurate, timely, complete, and reliable information on nuclear material; (2) maintaining control over the nuclear material; (3) providing the basis for investigation and resolution of any irregularity indicating a possible loss of nuclear material; and (4) providing information helpful to the recovery of missing material.

The guidance provided by the IAEA on this topic is very important and useful, but it would be beneficial to supplement it with more detailed guidance about what constitutes an effective NMAC system. This is a complex topic which calls for additional guidance on the implementation and enhancement of NMAC measures for nuclear security in specific facility types. This paper describes the development of a set of technical and administrative measures that an operator could consider when designing an NMAC system used to support nuclear security for research reactors. In addition, this set of technical and administrative measures can be considered by the competent authority to develop regulations and guidance for item facility operators that provide for an effective national mitigation strategy for detecting and deterring insider threat.

DEVELOPING THE GUIDANCE

The "Research Reactor Facility Measures against the Insider Threat" and the "Good Practices for the Implementation of Suggested Measures for Nuclear Security" guidance documents (**Figure 1**) were created by the US Department of Energy's National Nuclear Security Administration's Office of Global Material Security (DOE/NNSA/GMS), Nuclear Material Accounting and Control Functional Team based on a review of IAEA guidance and contributors' experience and knowledge. More specifically, the IAEA references NSS 25-G and NSS 32-T were a core source of information for this project. The contributors to this guidance have expert knowledge about and experience with nuclear material accounting and control, nuclear security, and insider threat mitigation. It was

especially important to involve contributors with experience working at or operating a research reactor, so several of the contributors have this experience, each from a different facility.

Figure 1. Covers for the "Research Reactor Facility Measures against the Insider Threat" (*left*) and the "Good Practices for Implementation of Measures for Nuclear Security" (*right*) guidance documents.

Using NSS 25-G and NSS 32-T as a starting point, the contributors created two documents to provide additional guidance on nuclear security measures at research reactors. The first document, "Research Reactor Facility Measures against the Insider Threat," provides information about where, when, and why to implement NMAC measures at a research reactor to mitigate the insider threat. The second document, "Good Practices for the Implementation of Suggested Measures for Nuclear Security," is similar to an appendix and provides more details about what these NMAC measures are and how they can be implemented.

RESEARCH REACTOR FACILITY MEASURES AGAINST THE INSIDER THREAT

The "Research Reactor Facility Measures against the Insider Threat" guidance document attempts to provide information about measures that can be used in a research reactor to protect the facility against an insider threat. The guidance describes different measures that can be used in areas common to most research reactors and applicable to various activities conducted at many research reactors. Every research reactor is unique, and these facilities include a wide variety of designs, purposes, operating environments, and infrastructure. The guidance is not intended to be exhaustive or inclusive of all areas, activities, or measures, but it serves as a reference or starting point to assist facilities with improving or developing nuclear security systems. It is a useful tool to start a conversation about potential insider threat scenarios and commensurate measures that could provide deterrence, detection, delay, and response to malicious actions.

The main section of the document is tabular and arranges information by location and activity within the facility. Information is also provided about the threat that each measure is protecting against and the goal of each measure. An example of a section of this guidance document is included in **Figure 2**, which provides a preview of the information included in the shipping/receiving process area section.

Process Area	Operational Activity	Malicious Action	Goal	Mitigating Measure(s)
Shipping/Receiving	Receipt of Fresh Fuel	Theft	Detection of theft indicators such as broken TIDs, violated containment, missing material, modified paperwork	Shipment Inspection
			Detection of substituted or missing nuclear material	Confirmatory Measurements
			Detection of malicious actions leading to or resulting in theft of nuclear material such as incorrect data entry or diversion of nuclear material	Two-Person-Rule
			Detection of malicious actions leading to or resulting in theft of nuclear material such as incorrect data entry or diversion of nuclear material	Separation of Duties
			Current information on all nuclear material available to facility management to confirm/deny missing nuclear material	Record Update
		Theft or Sabotage	Detection of malicious actions leading to or resulting in theft or sabotage of nuclear material by other persons knowledgeable of correct procedure	Standard Operating Procedure
		Sabotage	Deter/Detect attempts to damage fuel to damage reactor during operation or interfere with operations	Two-Person-Rule
				Partner Country Measure
	Receipt of target	Sabotage	Detection of sabotage indicators such as broken TIDs, violated containment, substituted material, modified paperwork	Shipment Inspection
			Deter/Detect attempts to substitute or damage target to cause reactor damage during irradiation	Two-Person-Rule
		Sabotage or misuse of reactor	Detection of substituted target material that could possibly damage reactor during irradiation or create unauthorized highly radioactive material	Confirmatory Measurements
				Partner Country Measure
	Return of Empty Fuel Containers	Theft	Deter/Detect use of container to hide theft of nuclear material	Shipment Inspection
			Deter/Detect use of container to hide theft of nuclear material	Two-Person Rule
			Deter/Detect use of container to hide theft of nuclear material	Facility Tamper Indication Device installed after inspection
				Partner Country Measure

Figure 2. A preview of the table from the "Research Reactor Facility Measures against the Insider Threat," showing the provided information from the shipping/receiving process area.

First, the table was categorized by process areas commonly used in a research reactor. The table was then organized by operational activities within these process areas. For example, some operational activities that take place in a shipping/receiving process area would be receipt of fresh fuel or receipt of target. If a specific activity is not called out, the operational activity will list "general area." **Table 1** contains the process areas and operational activities included in the guidance document.

The next column in the table provides information about what malicious action the associated measure is mitigating as well as the goal of the mitigating measure. The malicious action column includes items, such as

- damage or breakage of fresh fuel assembly, irradiated fuel assembly, or storage cask;
- sabotage or misuse or target or reactor;
- theft; and
- use of waste stream to shield theft of nuclear material.

Table 1. Process Areas and Associated Operational Activities

Process area	Operational activity
Shipping/receiving	Receipt of fresh fuel Receipt of target Return of empty fuel containers
Vault type room	Storage of fresh fuel, radioactive sources, experimental materials, targets and legacy materials Movement of material to other facility areas
Reactor	Fuel exchange
Irradiated fuel storage (wet)	General area Material movement Cask loading
Irradiated fuel storage (dry)	General area Cask movement
Irradiated waste storage	General area
Non-radioactivate waste storage	General area
Target preparation	Target preparation
Target area or scattering facilities adjacent to the reactor	General area Loading or unloading of target

The goal column is next, which provides more detail about how the mitigating measure may detect, deter, or delay malicious action in a facility. This column is specific to the mitigating measure and the associated processing area and operational activity. For example, a confirmatory measurement could be used during a receipt of fresh fuel to the shipping/receiving process area for the goal of detecting substituted or missing nuclear material. Another example is using the physical inventory taking measure for the goal of detecting or deterring theft of materials.

The mitigating measure(s) used in the final column of the table are listed in **Table 2**. In addition to these measures, there is also a row in the guidance document that states “partner country measure” in red. This row is included at the end of each operational activity section of the table. This space is included in the table for document reviewers from partner countries to contribute additional measures to the document. More information about the document reviews is included in a later section.

Table 2. Mitigating Measures by Implementation Type

Mitigating measure(s)	Type
Accounting measurements	Technical
Authorization of activities	Administrative
Confirmatory measurements	Technical
Item monitoring	Technical
Periodic administrative checks	Administrative
Physical inventory taking	Administrative
Records update	Administrative
Schedule of activities	Administrative
Separation of duties	Administrative
Shipment inspection	Administrative
Standard operating procedures	Administrative
Tamper-indicating device (seal)—facility program	Technical
Two-person rule	Administrative
Waste stream monitoring	Technical

GOOD PRACTICES FOR THE IMPLEMENTATION OF SUGGESTED MEASURES FOR NUCLEAR SECURITY

The "Good Practices for the Implementation of Suggested Measures for Nuclear Security" document is a reference for how to implement the measures found in the previous document. The descriptions included are intended as a starting point for developing or adapting the implementation of measures to a specific facility and its infrastructure. Each facility is unique and varies in physical structure, age, use, culture, and location. Therefore, the nuclear security measures and implementation practices will need to be adapted to specific facilities.

The main section of the document is tabular. For each nuclear security measure, the table provides information about which facility organizations are involved in implementing the measure, relevant reference documents, and whether the measure is an administrative or technical measure. An example of a section of this guidance document is shown in **Figure 3**. This figure shows a preview of the information included in the accounting measurements row of the table.

Measure	Purpose and Description	Implementation Good Practice	Suggested Coordinating Organizations
Accounting Measurements (Technical Measure) *Reference:* *NSS 25-G* *10 CFR Part 74*	Accounting measurements are an integral part of any nuclear material control and accounting system as they form the basis for initial entry into the accounting database. Beyond this they are necessary to identify differences or errors in the documentation which accompanies receipts of material from other holders. Each facility should have a structured and qualified system to measure material and document results. Documentation of such measurements forms critical archives for future material movement or processing.	Accounting measurements in the first instance are based on a measurement system which is qualified as accurate and maintained within quality controls established which can defend the continuing accuracy of the results. Trained personal are necessary for continuing qualification of the measurement system. Thus, ongoing training and qualification is inherently required. Quality certification of the system is a concept which is covered in many areas of facility operations and is a topic of its own. The accounting measurements themselves are necessary for all material on initial receipt or on creation/transformation in order to support accurate entries into the nuclear material accounting database. The baseline inventory is thus established and can be provided to external auditors or inspectors and is defendable and accurate. Once an accurate baseline inventory is established then verification activities against that inventory can be carried out. Further, changes in the inventory that may occur over time due to shipments/receipts and facility processing activities can be accurately documented and thus maintain an accurate inventory. Such a measurements as outlined here should be grounded in procedures that are reviewed and approved by appropriate levels of management and operations staff. **Partner Implementation Good Practice**	• Nuclear Material Accounting and Control • Safety (particularly Radiation Protection or Health Physics) • Operations • Physical Security (if appropriate)

Figure 3. A preview of the table from the "Good Practices for the Implementation of Suggested Measures for Nuclear Security," showing the provided information for the accounting measurements.

The first column includes the measures, which are the same measures included in the "Research Reactor Facility Measures against the Insider Threat." It also states whether the listed measure is an administrative or technical measure. This information is shown in **Table 2**. An *administrative measure* is implemented with the use of policies, procedures, and guidelines, and a *technical measure* involves the use of technology and equipment. This first column also provides references that can provide further information about the listed measure. The reference documents listed have been published by the IAEA, the US Nuclear Regulatory Commission, and DOE. The documents currently referenced in the document include:

- IAEA Nuclear Security Series
  - No. 08-G (Rev. 1) Implementing Guide, "Preventive and Protective Measures against Insider Threat"
  - No. 25-G Implementing Guide, "Use of Nuclear Material Accounting and Control for Nuclear Security Purposes at Facilities"
  - No. 32-T Technical Guidance, "Establishing a System for Control of Nuclear Material for Nuclear Security Purposes at a Facility during Use, Storage and Movement"
- US Nuclear Regulatory Commission Regulations Title 10, Code of Federal Regulations (CFR)
  - 10 CFR 73.55 "Requirements for Physical Protection of Licensed Activities in Nuclear Power Reactors against Radiological Sabotage"
  - 10 CFR Part 70 "Domestic Licensing of Special Nuclear Material"
  - 10 CFR Part 74, "Material Control and Accounting of Special Nuclear Material"
- US DOE Standards
  - DOE-STD-1194-2011, "Nuclear Materials Control and Accountability"

The next column, purpose and description, provides a short description of the measure and its usefulness. The implementation good practice column provides more detailed information on good practices for implementing each of the measures. In some cases, there are multiple ways to implement measures or differences in implementing measures in different category facilities. This information is included where applicable. In addition, examples of how measures may be implemented are provided in this section as well. Similar to the last document, each section includes a statement that says "partner implementation good practice." This provides space for document reviewers to contribute additional information on good practices for implementing the measures.

The final column, suggested coordinating organizations, lists organizations or teams within the facility that may be involved in the implementation of each measure. These suggested coordinating organizations are listed in **Table 3**.

Table 3. Coordinating Organizations that may be Involved in Implementing Nuclear Security Measures

Suggested Coordinating Organizations
Maintenance
Nuclear Material Accounting and Control
Operations
Physical Security
Purchasing
Response Forces
Safety
Training

PURPOSE AND USE OF GUIDANCE

The "Research Reactor Facility Measures against the Insider Threat" and the "Good Practices for the Implementation of Suggested Measures for Nuclear Security" guidance documents are meant to be used as references, suggestions, and conversation starters about potential insider threat scenarios and appropriate measures that could provide deterrence, detection, delay, and response to malicious actions. They may be useful for operators to consider when designing their facility's NMAC system used to support nuclear security. They may also be useful for the competent authority to consider when developing regulations and guidance for item facility operators that provides for an effective national mitigation strategy for detecting and deterring insider threat.

The guidance documents described can be useful tools when developing, adapting, and implementing NMAC measures for nuclear security, but the information included is not intended to be an exhaustive list or to be inclusive of all possible areas, activities, measures, or implementation practices. The information is not a substitute for each facility's examination of what accidental or malicious actions could result in the theft, misuse, or sabotage of the research reactor or its nuclear material, and each facility is highly encouraged to use the expertise of existing personnel. Personnel who perform operations in areas ranging from normal operation, to maintenance, to clean up have useful input. Also, personnel responsible for security in areas that assess all operational scenarios for opportunities of theft, sabotage, or misuse of the reactor by an insider adversary should be consulted.

CONTINUING WORK

The “Research Reactor Facility Measures against the Insider Threat” and the “Good Practices for the Implementation of Suggested Measures for Nuclear Security” guidance documents are intended to be shared, reviewed, and updated with experts internationally. There are spaces provided in each the documents for additional contributors to add their input to the documents. Every facility is unique and may use different measures or implementation practices, and including different practices in these guidance documents is important. Contributions from collaborators will help expand the effective implementation of measures to mitigate the insider threat. Furthermore, by allowing these documents to be continually revised, the guidance will remain current. These guidance documents have already been shared with collaborators in several countries and will be updated with any feedback received.

In addition to the two guidance documents already developed and shared, further guides are being developed to cover additional facility types. The goal is to develop guidance documents for all nuclear facility types. The “Good Practices for the Implementation of Suggested Measures for Nuclear Security” guidance document will be a reference for all of the facility documents, and it may need to be expanded as guidance for more facility types is developed.

A guidance document titled “Nuclear Power Plant Facility Measures against the Insider Threat” has already been developed. This document was developed in parallel with the guidance for research reactors and shares the same concept and structure. These two facility types typically contain item material types, so the measures contained many similarities. The development of a guidance document for fuel fabrication facilities is currently in progress. Unlike research reactors and nuclear power plants, this facility type contains bulk material. NMAC measures for bulk material are very different and can be more complicated than the measures used for item material types. This requires the “Good Practices for the Implementation of Suggested Measures for Nuclear Security” guidance document to be expanded to include information about implementing these measures for bulk materials.

Finally, it would be beneficial to expand this guidance to include other components of nuclear security, such as physical protection, cybersecurity, response, or performance evaluation. Currently, the guidance documents focus mainly on NMAC measures. This task has not yet started, but initial feedback from collaborators indicates that it would be useful to include measures outside of NMAC in these documents.

CONCLUSIONS

A set of guidance was created by the DOE/NNSA/GMS Nuclear Material Accounting and Control Functional Team to provide additional information about NMAC measures for nuclear security and insider threat mitigation, as well as implementation practices of these measures at research reactors. Two guidance documents have been created, titled “Research Reactor Facility Measures against the Insider Threat” and “Good Practices for the Implementation of Suggested Measures for Nuclear Security.” The guidance is intended to be used as a starting point for operators or the competent authority to consider when developing a facility NMAC system, regulations, or guidance. Research

reactors have a wide variety of designs and purposes, so the nuclear security and NMAC systems will be unique to each facility. These documents have been shared with collaborators from partner countries to contribute their feedback to the guidance. The development of additional guidance for other nuclear facility types, including nuclear power plants and fuel fabrication facilities, is ongoing.

ACKNOWLEDGEMENTS

This material is based upon work supported by the US Department of Energy, Office of International Nuclear Security (NA-211). Thank you to Robert Bean (Oak Ridge National Laboratory), Robert Marek (Pacific Northwest National Laboratory), and Jorge Navarro (Oak Ridge National Laboratory) for their contributions developing the guidance documentation described in this paper. Finally, we would like to thank Brent McGinnis (Pacific Northwest National Laboratory) for providing a review of the guidance documentation.

REFERENCES

[1] 10 CFR Part 70. "Domestic Licensing of Special Nuclear Material." Code of Federal Regulations, Title 10, Nuclear Regulatory Commission, Part 70, Washington, DC.
[2] 10 CFR 73.55. "Requirements for Physical Protection of Licensed Activities in Nuclear Power Reactors against Radiological Sabotage." Code of Federal Regulations, Title 10, Nuclear Regulatory Commission, Part 73.55, Washington, DC.
[3] 10 CFR Part 74. "Material Control and Accounting of Special Nuclear Material." Code of Federal Regulations, Title 10, Nuclear Regulatory Commission, Part 74, Washington, DC.
[4] DOE-STD-1194-2011. 2011. Nuclear Materials Control and Accountability, Washington, DC: US Department of Energy.
[5] International Atomic Energy Agency. 2019. Establishing a System for Control of Nuclear Material for Nuclear Security Purposes at a Facility During Use, Storage and Movement, IAEA Nuclear Security Series No. 32-T, IAEA, Vienna.
[6] International Atomic Energy Agency. 2020. Preventive and Protective Measures Against Insider Threats, IAEA Nuclear Security Series No. 8-G (Rev. 1), IAEA, Vienna.
[7] International Atomic Energy Agency. 2015. Use of Nuclear Material Accounting and Control for Nuclear Security Purposes at Facilities, IAEA Nuclear Security Series No. 25-G, IAEA, Vienna.
[8] "Research Reactor Facility Measures Against the Insider Threat." 2022. US DOE/NNSA/GMS Office of International Nuclear Security. LLNL-MI-839144.
[9] "Good Practices for the Implementation of Suggested Measures for Nuclear Security." 2022. US DOE/NNSA/GMS Office of International Nuclear Security. LLNL-MI-841208.