

Conf-950787--29

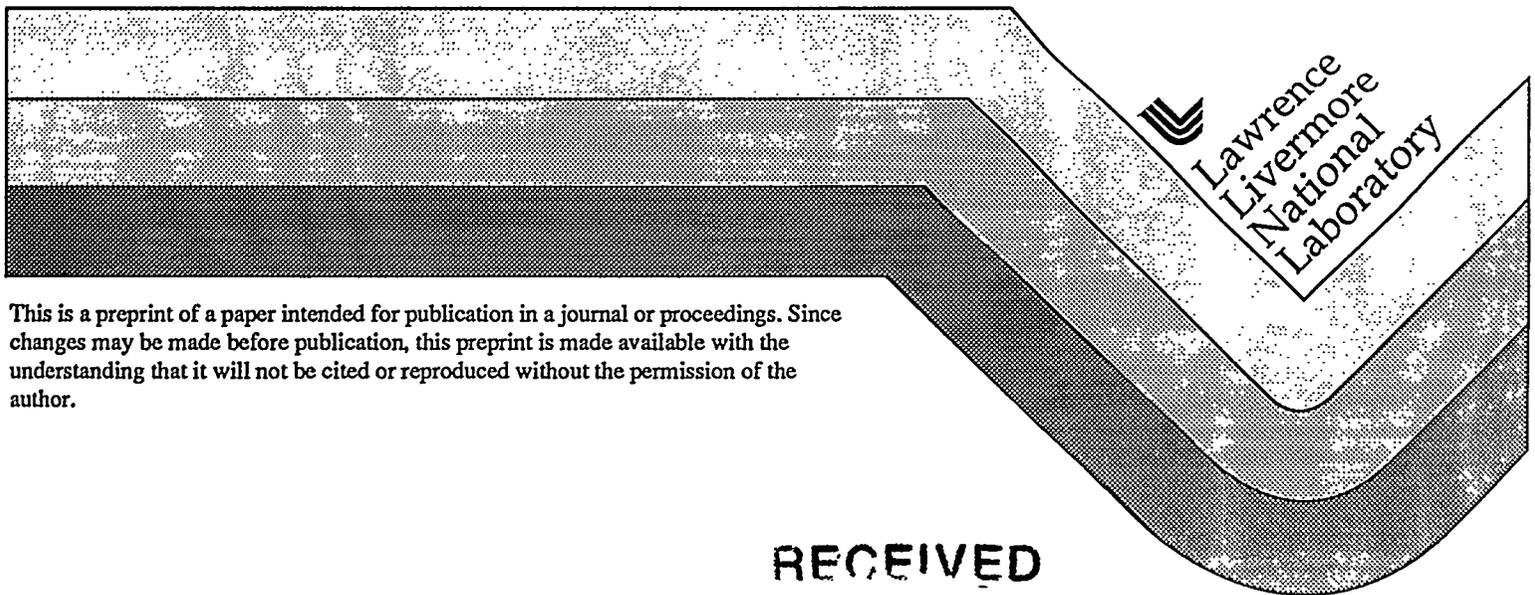
UCRL-JC-121005  
PREPRINT

## Analysis of Insider Threats Against Computerized Nuclear Materials Accountability Applications

Edwin Jones  
Alan Sicherman

This paper was prepared for:  
Institute of Nuclear Materials Management Meeting (INMM)  
Palm Desert, CA  
July 10-12, 1995

July 1995



This is a preprint of a paper intended for publication in a journal or proceedings. Since changes may be made before publication, this preprint is made available with the understanding that it will not be cited or reproduced without the permission of the author.

RECEIVED

AUG 04 1995

OSTI

## **DISCLAIMER**

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, make any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

## **DISCLAIMER**

**Portions of this document may be illegible in electronic image products. Images are produced from the best available original document.**

# Analysis of Insider Threats Against Computerized Nuclear Materials Accountability Applications

E. D. Jones and Alan Sicherman  
Fission Energy and Systems Safety Program  
Lawrence Livermore National Laboratory  
Livermore, CA 94550

## ABSTRACT

DOE Order 5633.3B requires that nuclear material accountability (MA) systems provide for i) tracking material inventories, ii) documenting material transactions, iii) issuing periodic reports, and iv) assisting in the detection of: unauthorized system access, data falsification, and material gains or losses. Insider threats against the MA system represent the potential to degrade the integrity with which these requirements are addressed (e.g., altering data to misrepresent the quantity or location of nuclear material). In this paper, we describe a methodology for evaluating potential insider threats against both current and future (e.g., client-server network) MA software applications. The methodology comprises a detailed yet practical taxonomy for characterizing various types of MA system/software applications and their implementation options. This taxonomy facilitates the systematic collection and organization of key information that helps spotlight such things as stages of information flow, transaction procedures, or auditing procedures potentially susceptible to insider falsification. Methodology benefits include helping MA managers and policy makers: i) examine proposed software designs or modifications with respect to how they might reduce or increase exposure to insider threats; and ii) better understand safeguards cost (e.g., operational hindrances) and benefit (resistance to falsification) tradeoffs of different system/software alternatives.

## BACKGROUND

DOE Order 5633.3B (Chapter II, 2.) requires that nuclear material accountability (MA) systems provide for:

- tracking material inventories
- documenting material transactions
- issuing periodic reports
- assisting in the detection of:  
unauthorized system access, data falsification, and material gains or losses

The order also requires that the accounting system provide a complete audit trail on all nuclear materials from receipt to disposition.

Generally, computerized accountability applications can help facilities address DOE 5633.3B policy requirements. Such applications can facilitate: management of large databases, accuracy of transactions recording, automated data cross-checks, rapid generation of inventory listings, and convenient advanced statistical data analysis. Technological progress now allows facilities to consider a variety of different implementation options for their MA applications. Advances such as graphical user interfaces and client-server networks are now being examined in addition to the more traditional stand-alone mainframe applications for their potential advantages in productivity and cost. The ability to modify software and *customize* functions and features such as user interface formats, access controls, and specialized statistical algorithms provide even more possibilities for facilities to consider.

Major benefits of computerized MA applications result from empowering users to perform their jobs more effectively. However, potential insider adversaries with particular kinds of knowledge, skills and abilities (or KSA) might exploit MA system features associated with computerized applications. Relevant KSA areas

\*Work performed under the auspices of the U.S. Department of Energy by the Lawrence Livermore National Laboratory under Contract W-7504-Eng-48.

include application software, database manipulation, electronics components, systems programming, and network communications<sup>1</sup>. Potential misrepresentation or misuse of MA data about the quantity or location of nuclear material by insiders can contribute to:

- degradation of data integrity including having erroneous, missing or garbled data;
- diversion or hoax cover-ups making it more difficult for a facility to ascertain if any material is actually missing from its authorized location or not;
- diminution of confidence in safeguards and security arising from the perception that the MA system is vulnerable<sup>2</sup>.

Applications, of course, can include safeguards for counteracting insider threats. Indeed, another potential advantage of computerized applications lies in the various security features that they can incorporate. However, the way different aspects of MA software applications are customized for specific facilities can significantly impact the security effectiveness of the applications against the insider threat.

How can managers and policy makers logically and pragmatically analyze different customization and design options for MA applications with respect to the insider threat? In this paper, we describe a methodology for addressing this question. In the following sections we give an overview of the approach followed by simple examples of approach features. Then we describe current and planned work to complete and refine the methodology, and a summary of methodology benefits.

## OVERVIEW OF ANALYSIS APPROACH

An MA system can be viewed as having *subsystems* or collections of functions/tasks that address DOE Order 5633.3B requirements. Major MA subsystems include the following:

- Inventories (MA application interface with physical inventories)
- Material Transactions (e.g., modify, split, combine, move functions; transactions involving: *pseudo materials* (e.g., write-offs), containers

(empties), Tamper Indicating Devices or TIDs like tags/seals)

- Report Generation (inventories, transactions, material balance area (MBA) closings (daily, monthly), reconciliations, other materials management and cost accounting requests)
- MA Software (development of source code, master database updating routines, variance propagation algorithms)
- Network/system traffic (e.g., network password/data transmission/encryption features)

Under each of these subsystems, we can develop lists of specific tasks or functions that are performed (e.g., such as *modify, split* etc., under Material Transactions).

Associated with any task, an MA system may have controls (or safeguards) to varying degrees including:

- Access/authorization controls
- Automated controls (for screening information submitted to the system)
- Human oversight controls prior to officially updating a nuclear material database
- Auditing/tracing controls (after database update)

Figure 1 schematically shows the relationship of these safeguards controls to the insider threat concerns.

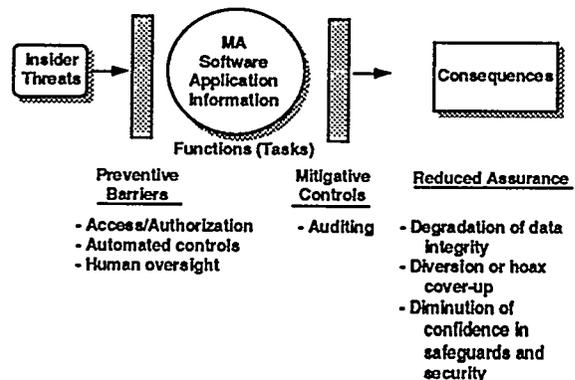


Figure 1. Schematic of MA safeguards control categories and their relationship to insider threat concerns.

We have developed *criteria* for analyzing the potential insider threat for each task of each subsystem in terms of the safeguards categories enumerated above. In the analysis approach, each criterion under the various control categories has an associated set of explicitly described possible *standard* gradations (or levels) tailored to each major MA subsystem. The gradations within each set are arranged from least preferable (weaker control) to most preferable (stronger control) from an insider threat perspective.

We have also developed a scheme for gathering information about MA applications in the form of subsystem and task *templates* for reflecting how each subsystem task is implemented. Based on the information provided on how a task is implemented, a correspondence or mapping is established between the task and one of the *standard* criteria gradations for each of the access, automated, human oversight and auditing criteria.

An analysis of MA systems with respect to potential insider threats can then be performed as follows:

1) For each subsystem task, designers and regulators can examine explicitly the level to which such a task implementation maps with respect to each of the control categories, and where such a gradation falls on the range of least to most preferable.

2) A preference *function* can be formally assessed indicating quantitatively the relative *value* for each gradation from the least to most preferable. The values for each of the separate control category criteria are then aggregated to produce an overall single value for the specific task. The algorithm or preference function for this aggregation is based on a formal preference assessment reflecting the way control categories relate to each other and their relative importance to the task. The functional form and method of assessment are based on formally stated assumptions for modeling expert or decision-maker judgments rationally and consistently.

In the simplest implementation of our approach, this aggregation among *standard* control categories would need to be assessed only once for each major subsystem from an appropriate expert or decision maker. The aggregation scheme quantifies how a variety of control options may achieve a similar overall value vis-à-vis the insider threat for a task,

and facilities can explore which combination of options is most cost-effective in their situations. The scheme also allows selective control categories to be ignored for any analysis. (For example, access may be ignored if the analyst wishes to focus on properties of the MA software application independent of authorized access.)

3) The preference values for tasks are then aggregated to produce an overall single value for the major subsystem. The aggregation scheme here is similar in concept to that in the previous step. How the subsystem tasks relate and their relative importance to the major subsystem must be assessed separately for each subsystem.

4) The preference values for subsystems are then aggregated to produce an overall single value or figure of merit for the entire MA system.

Basic elements of the approach will be illustrated in more detail in the sections below. Table 1 summarizes the elements of the approach that will be focused upon for the remainder of the paper.

**Table 1. Basic elements of MA applications analysis approach.**

<b>Evaluation criteria (six)</b>	
- access/authorization	(auditing)
- automated controls	- scrutability
- human oversight	- resolution
	- responsiveness
<ul style="list-style-type: none"> <li>• each criterion consists of a set of explicitly described levels tailored to each MA subsystem</li> <li>• levels within each set are arranged from least preferable (weaker control) to most preferable (stronger control) from an insider threat perspective</li> </ul>	

<b>Subsystem task templates (five)</b>	
<ul style="list-style-type: none"> <li>• each major subsystem has a set of tasks to be analyzed</li> <li>• analysis of MA applications begins by choosing the level of each criterion that best describes the way each subsystem task is implemented</li> </ul>	

# ILLUSTRATIONS OF BASIC METHODOLOGY ELEMENTS

## Criteria for Evaluating Subsystem Tasks

As shown in Table 1, we have formulated six criteria for evaluating MA application subsystem tasks vis-à-vis the insider threat. The first column of three criteria correspond to each of the three preventive barrier controls depicted in Fig. 1. The second column of three criteria characterize the mitigative auditing controls depicted in Fig. 1.

*Access/authorization* refers to preventing anyone not authorized from accessing a particular subsystem task. Gradations for this criterion reflect control provided by security features such as the password scheme that is implemented. For an authorized user, *automated controls* refers to application software features that can screen user input for things like format and numerical logic and consistency prior to updating a database. *Human oversight* is another control mechanism for screening user input. Table 2 illustrates abbreviated descriptions of the levels for the human oversight criterion tailored to the Material Transactions subsystem. (The actual level descriptions are more expansive and also contain more examples.)

**Table 2. Human oversight criterion levels tailored to Material Transactions subsystem.**

- 1 - no additional verification by another person
- 2 - requires understandable non-performance of another to thwart verification; e.g., verification perfunctory or limited spot check
- 3 - requires *tacit* collusion or dereliction of another to thwart verification; e.g., verifier has sufficient opportunity to recognize inappropriate task input but input will be accepted if verifier remains passive
- 4 - requires active collusion by another to foil verification; e.g., transaction input goes into a pending file where it is checked by verifier who must then enable database update
- 5 - requires active collusion of several others; e.g., transaction input to pending file by two persons (requiring two passwords) where it is then checked - by a third verifier before database update

As previously mentioned, the criteria descriptions are explicit and tailored to each subsystem to help analysts and decision makers choose the criterion level that best describes their task implementation. For a different subsystem, the criteria descriptions contain levels and examples more appropriate to *tasks for that subsystem*. For the MA Software subsystem, level 2 for human oversight contains the example: "e.g., reviewer of code modifications typically only examines changes claimed by programmer without independently generating own list of differences to check."

For the auditing criteria, *scrutability* reflects the effort and expertise required to find task information sought in auditing records. *Resolution* reflects the kind of task detail present in auditing records (e.g., "what, where, when, who") and the nature of ambiguities that might exist about a task even after an audit record is examined. *Responsiveness* reflects the circumstances that actually *trigger* an analysis of audit records. Table 3 illustrates abbreviated descriptions of the levels for the responsiveness criterion tailored to the Material Transactions subsystem.

**Table 3. Audit responsiveness criterion levels tailored to Material Transactions subsystem.**

- 1 - only material anomaly triggers analysis of data available for audit
- 2 - anomaly and random checks trigger analysis
- 3 - anomaly and systematic audit analysis of special sensitive transactions (e.g., those accessing special data fields or involving *negative mass*)
- 4 - anomaly and random checks and systematic audit analysis of special sensitive transactions
- 5 - all task transactions trigger audit analysis and auditor is also supplemented by automated search and flagging of audit records for any suspicious task patterns or discrepancies

## Subsystem Task Information Collection Templates

With a subsystem task template, an analyst selects the criteria gradations (levels) that best match the implementation of an MA application design. The concept is illustrated in Fig. 2.

Subsystem -		(audit)					
		access	automated controls	human oversight	scrutability	resolution	responsiveness
Tasks							
Design A:	Modify	3	2	1	5	5	5
	Split	3	2	1	5	5	5
	Move between MBAs	3	3	4	5	5	5
Design B:	Modify	4	3	1	4	5	2
	Split	4	3	1	4	5	2
	Move between MBAs	4	3	1	4	5	2
Design C:	Modify	2	2	5	4	5	1
	Split	2	2	4	4	5	1
	Move between MBAs	2	2	4	4	5	1

Figure 2. Illustrative simplified scoring of subsystem tasks.

Each subsystem template (e.g., five templates to span the subsystems enumerated earlier) has its own set of tasks to be analyzed. For example, the Inventories subsystem tasks can include: generation of inventory checklist, transmittal of checklist, item check, bulk material measurement, measurement device calibration, recording of inventory data, transmittal of inventory data, matching of data to books, and discrepancy resolution. Material transactions tasks can include: modify, split, combine, move within an MBA, move between MBAs, move in/out of facilities, material in process, sweeps and write-off type transactions, container operations and TID operations.

The tasks for each subsystem have enough in common so the same tailored criteria descriptions reasonably apply to all of them. However, not all tasks in a subsystem need have the same safeguards controls as shown in Fig. 2 for illustrative design options. Generally, the list of tasks for each subsystem template should be comprehensive enough to cover: the different types of functions performed that could have different safeguards in their implementation, and the distinct stages of information or task flow involved in the subsystem.

#### Illustrative Insights from Initial Analysis Step

Although simplified, Fig. 2 illustrates how the methodology described here helps to systematically formalize safeguards strengths and weaknesses of different MA design options for different tasks, and also how different application implementations can involve tradeoffs among safeguards controls. For Design A, automated and human oversight controls are relatively de-emphasized, while auditing controls are stressed. Design B has stronger automated controls but has less responsive auditing capability. Finally, Design C stresses human oversight controls while de-emphasizing auditing responsiveness.

Even using just the initial analysis step described in this paper, the methodology in trials to date has provided a diagnostic tool that helps analysts and decision makers recognize in explicit fashion different safeguards control implications of MA design options. Often planners can improve on individual task safeguards controls by adding features that are relatively easy to implement. However, adding certain extra safeguards features could exact significant penalties in operations. Thus *tradeoffs* often need to be considered as illustrated in Figure 2.

## Aggregating Across Tasks and Subsystems

In order to compare alternatives as to their effectiveness against the insider threat, the following issues must be addressed:

- how to quantify the safeguards value of criterion levels
- how criterion levels impact safeguards effectiveness for tasks
- how task effectiveness impacts subsystem effectiveness
- how subsystem effectiveness impacts overall effectiveness

Probabilities are used to quantify effectiveness in vulnerability assessment or VA tools<sup>3</sup>. An alternative with tradeoffs resulting in a higher estimated probability of adversary defeat is preferred when costs and operational impacts are acceptable. For accountability applications, however, other approaches whose details exceed the scope of this paper (e.g., multiattribute utility/value preference function theory<sup>4</sup>) may prove more practical. The MA approach outlined here allows for relative value judgments for criterion gradations without forcing these judgments to be interpreted as probabilities. With any approach, the key point is how to logically compare the efficacy of improving on one criterion versus another, or improving on one task versus another in appropriately calibrating tradeoffs.

With an insider VA tool such as ASSESS<sup>3</sup>, a very specific material target is identified, and the probability of adversary defeat is understood in the context of literally moving material from a target location to a place off site along a physical path. For evaluating MA software applications, however, we may not know what precise information compromise will actually result in any harm to the facility. What is needed instead is a practical characterization of how computerized MA application features affect the *level of effort* required by insiders to misrepresent or misuse data. This contrasts with a probability approach which would require defining many specific kinds of data compromise as well as estimating their probabilities of occurrence given insider attempts.

## CURRENT PLANS AND SUMMARY

The methodology presented here is intended to be flexible to meet the needs of MA system planners and decision makers. The basic approach allows for easy modification or extension of details (such as

the spectrum and gradations of criteria) to address decision making needs. Also, analysts can focus on one subsystem alone or use a subset of MA controls in a modular analysis fashion. Current plans are to: continue testing and documenting the approach, demonstrate aggregated system evaluation, and provide training and transfer of the approach to the field.

In summary, we believe the methodology can help managers and policy makers:

- collect information about MA applications relevant to the insider threat
- spotlight the relative strengths and weaknesses of application safeguards for a variety of accountability tasks using explicit criteria; the higher the criteria levels, the greater KSA required by an insider to misrepresent/misuse information
- evaluate tradeoffs between different system-software designs vis-à-vis effectiveness against the insider threat.

## REFERENCES

1. D. S. Fortney and J. J. Lim, "A Technical Approach for Determining the Importance of Information in Computerized Alarm Systems," *Proceedings of the 17th National Computer Security Conference*, Baltimore, MD (October 1994).
2. A. Sicherman, "Measuring the Safeguards Value of Material Accountability," *Proceedings of the 29th Annual Meeting of the Institute of Nuclear Materials Management*, Volume XVII (June 1988).
3. R. A. Al-Ayat, C. J. Patenaude, T. A. Renis, and R. Saleh, "A Comprehensive Method for Evaluating Safeguards Against the Insider Threat," *Proceedings of the 30th Annual Meeting of the Institute of Nuclear Materials Management*, Volume XVIII (July 1989).
4. R. L. Keeney and H. Raiffa, *Decisions with Multiple Objectives*, New York: John Wiley & Sons, 1976.