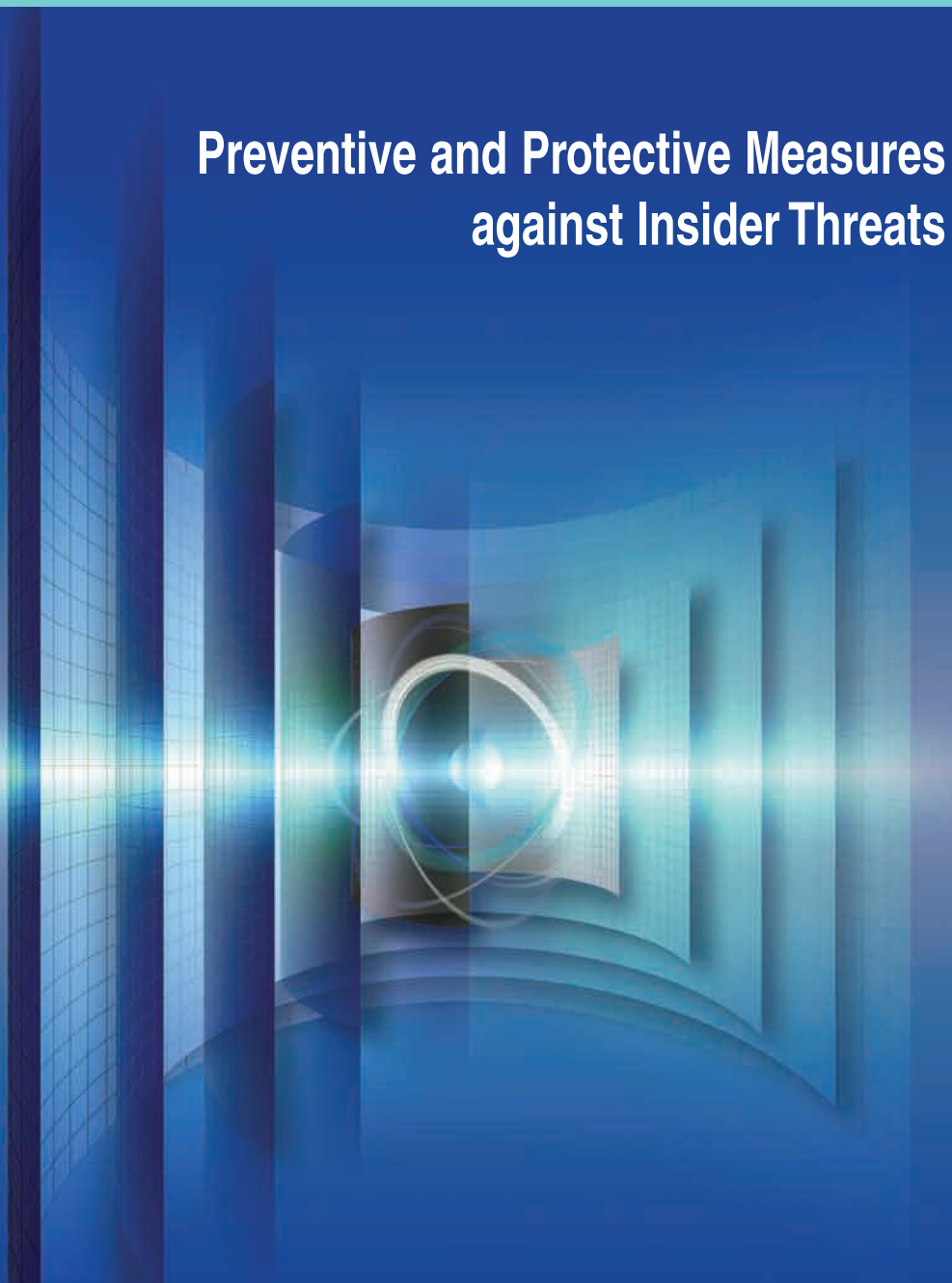
IAEA Nuclear Security Series No. 8

Implementing Guide

Preventive and Protective Measures against Insider Threats



IAEA
International Atomic Energy Agency

PREVENTIVE AND PROTECTIVE MEASURES AGAINST INSIDER THREATS

The following States are Members of the International Atomic Energy Agency:

AFGHANISTAN
ALBANIA
ALGERIA
ANGOLA
ARGENTINA
ARMENIA
AUSTRALIA
AUSTRIA
AZERBAIJAN
BANGLADESH
BELARUS
BELGIUM
BELIZE
BENIN
BOLIVIA
BOSNIA AND HERZEGOVINA
BOTSWANA
BRAZIL
BULGARIA
BURKINA FASO
CAMEROON
CANADA
CENTRAL AFRICAN REPUBLIC
CHAD
CHILE
CHINA
COLOMBIA
COSTA RICA
CÔTE D'IVOIRE
CROATIA
CUBA
CYPRUS
CZECH REPUBLIC
DEMOCRATIC REPUBLIC OF THE CONGO
DENMARK
DOMINICAN REPUBLIC
ECUADOR
EGYPT
EL SALVADOR
ERITREA
ESTONIA
ETHIOPIA
FINLAND
FRANCE
GABON
GEORGIA
GERMANY
GHANA
GREECE
GUATEMALA
HAITI
HOLY SEE
HONDURAS
HUNGARY
ICELAND
INDIA
INDONESIA
IRAN, ISLAMIC REPUBLIC OF
IRAQ
IRELAND
ISRAEL
ITALY
JAMAICA
JAPAN
JORDAN
KAZAKHSTAN
KENYA
KOREA, REPUBLIC OF
KUWAIT
KYRGYZSTAN
LATVIA
LEBANON
LIBERIA
LIBYAN ARAB JAMAHIRIYA
LIECHTENSTEIN
LITHUANIA
LUXEMBOURG
MADAGASCAR
MALAWI
MALAYSIA
MALI
MALTA
MARSHALL ISLANDS
MAURITANIA
MAURITIUS
MEXICO
MONACO
MONGOLIA
MONTENEGRO
MOROCCO
MOZAMBIQUE
MYANMAR
NAMIBIA
NEPAL
NETHERLANDS
NEW ZEALAND
NICARAGUA
NIGER
NIGERIA
NORWAY
PAKISTAN
PALAU
PANAMA
PARAGUAY
PERU
PHILIPPINES
POLAND
PORTUGAL
QATAR
REPUBLIC OF MOLDOVA
ROMANIA
RUSSIAN FEDERATION
SAUDI ARABIA
SENEGAL
SERBIA
SEYCHELLES
SIERRA LEONE
SINGAPORE
SLOVAKIA
SLOVENIA
SOUTH AFRICA
SPAIN
SRI LANKA
SUDAN
SWEDEN
SWITZERLAND
SYRIAN ARAB REPUBLIC
TAJIKISTAN
THAILAND
THE FORMER YUGOSLAV REPUBLIC OF MACEDONIA
TUNISIA
TURKEY
UGANDA
UKRAINE
UNITED ARAB EMIRATES
UNITED KINGDOM OF GREAT BRITAIN AND NORTHERN IRELAND
UNITED REPUBLIC OF TANZANIA
UNITED STATES OF AMERICA
URUGUAY
UZBEKISTAN
VENEZUELA
VIETNAM
YEMEN
ZAMBIA
ZIMBABWE

The Agency's Statute was approved on 23 October 1956 by the Conference on the Statute of the IAEA held at United Nations Headquarters, New York; it entered into force on 29 July 1957. The Headquarters of the Agency are situated in Vienna. Its principal objective is "to accelerate and enlarge the contribution of atomic energy to peace, health and prosperity throughout the world".

IAEA NUCLEAR SECURITY SERIES No. 8

PREVENTIVE AND PROTECTIVE MEASURES AGAINST INSIDER THREATS

IMPLEMENTING GUIDE

INTERNATIONAL ATOMIC ENERGY AGENCY
VIENNA, 2008

COPYRIGHT NOTICE

Printed by the IAEA in Austria
September 2008
STI/PUB/1359

IAEA Library Cataloguing in Publication Data

Preventive and protective measures against insider threats : implementing guide. Vienna : International Atomic Energy Agency, 2008.
p. ; 24 cm. — (IAEA nuclear security series, ISSN 1816–9317 ; no. 8)
STI/PUB/1359
ISBN 978–92–0–109908–2
Includes bibliographical references.

1. Radioactive substances — Detection. 2. Radioactive substances — Safety measures. 3. Radioactive substances — Transportation. 4. Nuclear Terrorism — Prevention. 5. Nuclear Terrorism — Security measures. I. International Atomic Energy Agency. II. Series.

IAEAL 08–00540

FOREWORD

In response to IAEA General Conference resolution GC(46)/RES/13 of 20 September 2002, the IAEA adopted an integrated approach to protection against nuclear terrorism. This approach coordinates IAEA activities concerned with the physical protection of nuclear material and nuclear facilities, nuclear material accountancy, detection of and response to trafficking in nuclear and other radioactive material, the security of radioactive sources, security in the transport of nuclear and other radioactive material, emergency response and emergency preparedness in Member States and at the IAEA, and promotion of adherence to and implementation by States of relevant international instruments. The IAEA also helps to identify threats and vulnerabilities related to the security of nuclear and other radioactive material. However, it is the responsibility of the States to provide for the physical protection of nuclear and other radioactive material and the associated facilities, to ensure the security of such material in transport, and to combat illicit trafficking and the inadvertent movement of radioactive material.

Physical protection systems are intended to prevent unacceptable consequences arising from malicious acts. The more serious the potential consequences, the more important it is to have a high degree of confidence that physical protection systems will be effective as planned.

Nuclear material and nuclear facilities have the potential to lead to a variety of unacceptable radiological and proliferation consequences if subjected to a malicious act. The need for high confidence in the effectiveness of physical protection has long been recognized by those concerned with nuclear material and nuclear facilities. The highest level of confidence in physical protection demands a close correlation between protective measures and the threat. This approach is firmly grounded in the fundamental principle that physical protection of nuclear assets under the jurisdiction of a State should be based on the State's evaluation of the threat to those assets.

A clear understanding of the threat can lead to a detailed description of potential adversaries, including 'outsiders' and 'insiders'.

Insider threats in particular present a unique problem for a physical protection system. Insiders could take advantage of their access rights, complemented by their authority and knowledge of a facility, to bypass dedicated physical protection elements or other provisions such as measures for safety, material control and accountancy, and operating measures and procedures. Further, as personnel with access in positions of trust, insiders are capable of carrying out 'defeat' methods not available to outsiders when confronted with protection elements and access controls. Insiders have more

opportunities to select the most vulnerable target and the best time to execute the malicious act.

A number of IAEA publications deal with physical protection against the unauthorized removal of nuclear material and against sabotage of nuclear material and nuclear facilities. These publications provide general recommendations on the design and evaluation of protection measures, and are mainly oriented to the prevention of external threats.

With the objective of developing a comprehensive set of guidance, the decision was taken to develop a guide written specifically with regard to insiders. As a consequence, this publication provides general guidance for the prevention of and the protection against internal threats. It provides guidance on implementing the recommendations of INFCIRC/225/Rev.4 (Corrected) and should be used in conjunction with IAEA-TECDOC-967 (Rev.1) and IAEA-TECDOC-1276 and with other publications in the IAEA Nuclear Security Series.

CONTENTS

1. INTRODUCTION

1.1. BACKGROUND

A number of IAEA publications deal with physical protection against the unauthorized removal of nuclear material and against sabotage of nuclear material and nuclear facilities.

The Convention on the Physical Protection of Nuclear Material (CPPNM) [1] provides general requirements for the physical protection of nuclear material and specific requirements for the protection of material while in international transport. The Amendment to the CPPNM [2] was adopted by the Diplomatic Conference of State Parties to the CPPNM by consensus on 8 July 2005, and is subject to ratification, acceptance or approval. The scope of the Amendment covers requirements for the physical protection of nuclear material in domestic use, storage and transport and also protection of nuclear material and facilities against sabotage. In addition, the Physical Protection Objectives and Fundamental Principles [3] have been reflected in the Amendment.

The Physical Protection Objectives and Fundamental Principles, GOV/2001/41 [3], contains four overall objectives and 12 principles essential to the development of a comprehensive physical protection regime.

The Physical Protection of Nuclear Material and Nuclear Facilities, INFCIRC/225/Rev.4 (Corrected) [4], provides recommendations and further guidance to the State's competent authority on how to implement domestic requirements in a manner consistent with these recommendations. It is supplemented by IAEA-TECDOC-967 (Rev.1), Guidance and Considerations for the Implementation of INFCIRC/225/Rev.4 (Corrected) [5].

The Handbook on the Physical Protection of Nuclear Material and Facilities, IAEA-TECDOC-1276 [6], provides practical advice for the facility operator on the design of a physical protection system, on the array of measures and equipment for a particular facility, and on response functions and guidance for the facility to evaluate the effectiveness of the physical protection system in place; however, this handbook addresses internal threats in a limited scope only.

1.2. INSIDER ISSUES

The term 'adversary' is used to describe any individual performing or attempting to perform a malicious act. An adversary may be an insider or an

outsider. The term 'insider' is used to describe an adversary with authorized access to a nuclear facility, a transport operation or sensitive information. The term 'outsider' is used to describe an adversary other than an insider.

A physical protection system is designed and evaluated against threats posed both by outsiders and insiders. Insider threats present a unique problem. Insiders could take advantage of their access (i.e. right or opportunity to gain admittance), complemented by their authority (i.e. power or right to enforce obedience) and knowledge of the facility (i.e. awareness or familiarity gained by training or experience), to bypass dedicated physical protection elements or other provisions such as safety, nuclear material control and accountancy (MC&A), and operating measures and procedures.

Further, as individuals having authorized access and with positions of trust, insiders could be capable of defeating methods not available to outsiders. Insiders have more opportunity (i.e. more favourable conditions) to select the most vulnerable target and the best time to perform or attempt to perform the malicious act. They can extend the malicious act over a long period of time to maximize the likelihood of success. This could include, for example, tampering with safety equipment to prepare for an attempt or act of sabotage or falsifying accounting records to repeatedly steal small amounts of nuclear material.

This guide provides guidance on how to implement the recommendations set out in INFCIRC/225/Rev.4 (Corrected) [4] — hereinafter referred to as INFCIRC/225 — and is written specifically with regard to insiders. It should be used in conjunction with IAEA-TECDOC-967 (Rev.1) [5] and IAEA-TECDOC-1276 [6].

1.3. OBJECTIVE AND SCOPE

The objective of this guide is to provide general guidance to the competent authority and operators[1] on prevention of and protection against insider threats. Threats to nuclear facilities can involve outsiders, insiders or both together in collusion.

The term 'threat' is used to describe a likely cause of harm to people, damage to property or harm to the environment by an individual or individuals

[1] The term 'operator' is used to describe an entity (person or organization) authorized to operate a nuclear or radiological facility or authorized to use, store or transport nuclear material and/or radioactive material. Such an entity would normally hold a licence or other document of authorization from a competent authority or be contractors of a holder of such an authorization.

with the motivation, intention and capability to commit a malicious act. Insiders pose a severe threat to a facility because such adversaries can exploit their advantages of having authorized access, authority and knowledge to betray trust and bypass security measures.

An insider may be in any position at a facility, from the highest level employee to the lowest. Detailed analysis of insider threats is, by nature, facility specific because of the wide range of facility types to be protected (e.g. research reactors, nuclear power plants and other nuclear fuel cycle facilities). Owing to the facility specific nature of the insider threat, guidance is not included in a general document such as INFCIRC/225.

The scope of this guide — in line with INFCIRC/225 — covers unauthorized removal of nuclear material and sabotage of nuclear material and facilities. This guide applies to any type of nuclear facility, notably nuclear power plants, research reactors and other nuclear fuel cycle facilities (e.g. enrichment plants, reprocessing plants, fuel fabrication plants and storage facilities), whether in operation, shut down or being decommissioned.

This guide should be considered during the design, construction, commissioning and operation phases of new facilities. The guide also covers unauthorized removal of nuclear material and sabotage during the transport of nuclear material. Guidance and measures presented in this guide can also be applied to the physical protection of other materials, including radioactive sources or radioactive waste.

The terminology used in this guide follows the definitions set out in the CPPNM and the 2005 Amendment thereto [1, 2] and/or the IAEA Safeguards Glossary [7].

2. IDENTIFICATION OF POTENTIAL INSIDER THREATS

This section presents guidance for identifying potential insider threats at the facility level. The guidance uses the information on insiders provided in the design basis threat or other State level documents, such as a national threat assessment, as a starting point, and further defines insiders by a rigorous examination of characteristics of the facility site or the transport operation.

The design basis threat is a regulatory tool for planning, designing and evaluating a physical protection system. A State should consider attributes and characteristics of potential insiders and reflect them as appropriate in the

design basis threat. Depending on the State, the design basis threat addressing insiders may or may not be detailed.

When the design basis threat has not been developed for certain areas of nuclear activities with potentially limited radiological and proliferation consequences, the measures to protect against insiders should be based on those proposed in Section 5. Proper implementation of such measures would provide an appropriate basis for complying with INFCIRC/225 recommendations.

In addition to the information in the design basis threat, other information for each facility or transport operation should be assessed or analysed to describe every individual employee or type of potential insider on the bases of levels of access, authority over others and their knowledge of the facility operations, transport arrangements and other general capabilities that support opportunities for performing or attempting to perform malicious acts.

Insiders may have different motivations and may be passive or active, non-violent or violent (Fig. 1). The term 'motivation' is used to describe the motive forces that compel an adversary to perform or attempt to perform a malicious act. Motivation may include ideological, personal, financial and psychological factors and other forces such as coercion. Insiders could act independently or in collusion with others. They could become malicious on a single impulse, or act in a premeditated and well prepared manner, depending upon their motivation.

An individual could be forced to become an insider by coercion or by coercing his family members.

Passive insiders are non-violent and limit their participation to providing information that could help adversaries to perform or attempt to perform a malicious act.

Active insiders are willing to provide information, perform actions and may be violent or non-violent. Active insiders are willing to open doors or locks, provide hands-on help and aid in neutralizing response force personnel. Non-violent active insiders are not willing to be identified or risk the chance of engaging response forces and may limit their activities to tampering with accounting and control, and safety and security systems. Violent active insiders may use force regardless of whether it enhances their chances of success; they may act rationally or irrationally.

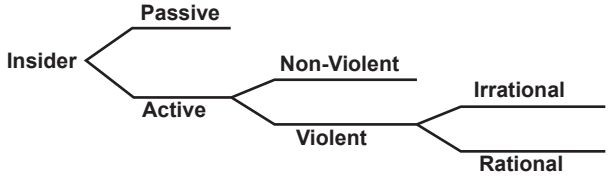


FIG. 1. Categories of insiders.

At a minimum, consideration should be given to the following:

(a) Insiders may hold any position in an organization (e.g. experimenter, physical protection system designer, security guard, material handler, clerk, custodian, safeguards officer, operational and maintenance worker or senior manager). Others not directly employed by the operator but who also have access (such as vendors, emergency personnel, including firefighters and first responders, contractors, subcontractors and inspectors from regulatory organizations) should also be considered.
(b) Insiders may have:
    (i) Access to some or all areas of a facility, systems, equipment or tools;
    (ii) Authority over operations or personnel;
    (iii) Knowledge of facility layout, transport arrangements and/or processes, physical protection, safety systems and other sensitive information;
    (iv) Technical skills and experience;
    (v) Authority to acquire and ability to use tools, equipment, weapons or explosives.

Therefore, insiders may have the opportunity to commit a malicious act during normal operating conditions of a facility, maintenance, transport of nuclear material or emergencies, and may select the most favourable time to do so.

In addition to potential insiders identified through the inherent ability to obtain authorized access, people with no access to a facility or transport operation but with sufficient knowledge and/or authority to conduct a malicious act (e.g. a headquarters manager who issues a counterfeit delivery order to an outside location) should be given specific consideration. These scenarios can, alternatively, be covered by a vulnerability assessment performed in respect of outsiders.

3. SITUATIONS TO BE CONSIDERED IN THE ANALYSIS OF INSIDER THREATS

Certain situations at nuclear facilities may be favourable or conducive to insider threats.

Situations inside the facility or regarding transport, including those related to the workforce, employment issues such as performance appraisals, industrial relation policies and an absence of security culture, security awareness and trustworthiness programmes, may be favourable or conducive to insider attempts to perform malicious acts.

Temporary situations, such as maintenance operations, may lead to a significant increase in the number of access authorizations delivered to, for example, contracting companies.

Situations outside the facility or in the vicinity of transport routes, including the general attitude of the community, whether the surrounding area is urban or rural, and the presence of organized hostile groups, may also be favourable to insider threats. Any discontented faction among the population and social and political animosities should be considered. Special attention should be paid to possible connections between these groups and individuals with experience in facility operations or with access to the nuclear facility.

The operator should be aware of these situations when considering insider threats.

4. TARGET IDENTIFICATION

The objective of this section is to provide general guidance on identifying potential targets for unauthorized removal of nuclear material and sabotage, with a focus on targets attractive to insiders. Other IAEA publications, such as Ref. [4], provide more detailed guidance on target identification.

4.1. OVERVIEW

Target identification is an evaluation of what to protect a priori, including nuclear material, associated areas, buildings and equipment, components, systems and functions, without consideration of the difficulty of providing protection.

Consideration should be given to:

(a) Safety analysis and the associated vital area identification analysis, with Ref. [4], para. 7.1.5, as the starting point to identify potential sabotage targets;

(b) Categorization of nuclear material as it applies to the physical protection of nuclear material (INFCIRC/225) to identify potential targets for unauthorized removal [4];
(c) Design basis threat or other State level documents, such as a national threat assessment, providing information or criteria for the definition of potential targets.

Insider targets are somewhat different from those of outsiders. For example, insiders could commit protracted theft of small amounts of nuclear material from several locations, in each of which the quantity of material is not attractive to an outsider. Moreover, in some cases an insider's sequence of malicious acts leading to sabotage may not be time constrained, which contrasts with the outsider's dependence on time.

An analysis should be conducted to rank the identified targets according to the severity of the consequences. This ranking will provide the basis for implementing graded preventive and protective measures.

4.2. SABOTAGE TARGETS

The levels of unacceptable radiological consequences are established by the State or the competent authority and may vary from State to State. It is desirable that, in specifying the radiological consequence levels used for malicious incidents, the safety criteria are taken into account. However, levels of unacceptable radiological consequences for malicious acts could differ from those considered in the facility safety analysis and may need to be graded in levels below or above those of the safety analysis.

Identifying sabotage targets at a facility begins by using the safety analysis report, including the probabilistic safety analysis for external events if it exists, and other sources that could assist in identifying potential accident sequences that could have significant radiological consequences for workers, the public and the environment. An accident sequence is a series of events resulting from one or more initiating events (human error or the failure of one or more components or functions) that place the facility in a degraded situation despite its installed engineered safety systems and mitigation devices.

However, sabotage is not considered in a probabilistic safety analysis, and therefore it must be considered, since other events that could be initiated by a malicious act may also lead to significant radiological consequences. For example, in some cases the simultaneous failure of the redundant equipment of a safety related system is not considered probable in probabilistic safety analysis. However, such a failure could credibly be caused by an act of sabotage

and could give rise to radiological consequences. Components, systems or functions whose loss or failure caused by a malicious act could have serious consequences should be identified.

This approach enables the identification of the most sensitive elements in the facility (components, systems or functions) and their locations.

4.3. TARGETS FOR UNAUTHORIZED REMOVAL

The identification of potential targets for unauthorized removal of nuclear material should take into account both:

(a) The repeated unauthorized removal of small quantities of nuclear material during several events (protracted theft); and
(b) The unauthorized removal of a large quantity of nuclear material during a single event (abrupt theft).

To consider both of these, the inventory of all nuclear material at a facility or in transport should be considered. The inventory list should include the amount, form, type, location and condition of all nuclear material at the facility or in transport.

Targets for theft should be identified through information or criteria contained in a State level document. Alternatively, targets may be grouped in one of three categories (I, II and III) as drawn from the categorization table of nuclear material in both the CPPNM [1] and INFCIRC/225 [4]. This grouping should be based on the risk of the material being used for a nuclear explosive device, which itself depends on: the type of material, for example plutonium, uranium; isotopic composition, that is content of fissile isotopes; physical and chemical form; degree of dilution; radiation level; and quantity. In addition, in identifying the targets for unauthorized removal of nuclear material by insiders, the possibility of an adversary collecting an amount equivalent to a higher categorization from several locations of lower categorization should be considered.

5. MEASURES AGAINST POSSIBLE INSIDERS

This section describes an approach to countering the insider threat and recommends some specific preventive measures and protective measures.

5.1. GENERAL APPROACH

The term 'preventive measures' is used to describe measures to preclude or remove possible insider threats, or to minimize threat opportunities, or to prevent a malicious act from being carried out. The term 'protective measures' is used to describe measures to detect, delay and respond to malicious acts that are carried out, and to mitigate or minimize their consequences. Protective measures should be coordinated with the overall emergency response plans in accordance with agreed procedures. Emergency response plans should also include recovery provisions in the event of unauthorized removal of nuclear material. Preventive and protective measures should provide defence in depth and should be fully integrated into a well developed security programme. The approach to take to prevent and protect against malicious acts by insiders is described in Fig. 2.

Figure 2 introduces the following steps, represented by the arrows between the boxes, describing the prevention and protection approach against the potential insiders identified in Section 2.

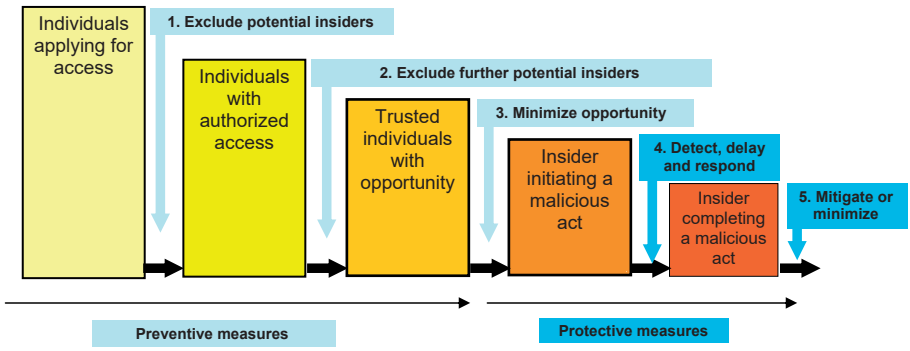


FIG. 2. The approach to preventing and protecting against malicious acts by insiders.

Prevention:

(1) Exclude potential insiders by identifying undesirable behaviour or characteristics, which may indicate motivation, prior to allowing them access;
(2) Exclude further potential insiders by identifying undesirable behaviour or characteristics, which may indicate motivation, after they have access;
(3) Minimize opportunities for malicious acts by limiting access, authority and knowledge, and by other measures.

Protection:

(4) Detect, delay and respond to malicious acts;
(5) Mitigate or minimize consequences.

Many measures listed in Sections 5.3 and 5.4 can be considered as both preventive and protective measures. The proposed list should be seen only as a possible grouping. It is recommended that each proposed measure be considered and implemented for its prevention or protection characteristics.

5.2. DEVELOPMENT OF A COMPREHENSIVE APPROACH

The overall approach consists of implementing several layers of defence, including both administrative aspects (procedures, instructions, administrative sanctions, access control rules, confidentiality rules) and technical aspects (multiple protection layers fitted with detection and delay) that insiders would have to overcome or circumvent in order to achieve their objectives.

Implementing preventive and protective measures to counter the insider threat is usually much more difficult than implementing measures to counter the outsider threat, due to the access, knowledge, authority and attributes of insiders (as defined in Section 2). Thus, although already partially addressed for the outsider threat, any elements that could provide protection against the insider threat should be considered. These elements include detection, delay, response and mitigation capacities of safety, radiation protection and MC&A provisions. Their synergetic effect should be established and formally integrated within the comprehensive approach.

For nuclear safety purposes, design criteria such as redundancy or diversity in systems and equipment that are important to safety, or layout criteria such as physical or geographical separation or segregation of these systems or equipment, are introduced at the design phase of the facility or

transport package. These provisions can improve protection against sabotage by requiring more preparation, more means and more time for an insider to commit a malicious act. Consequently, they could be of significant efficiency to deter, prevent or delay acts of sabotage by insiders or to mitigate or minimize the radiological consequences.

Radiation protection measures, such as the limitation of access to specific areas and radiation protection devices, could contribute to both deterring and preventing unauthorized removal or sabotage by insiders.

MC&A provisions are designed to keep a strict inventory of all nuclear material and to register an alarm if the material balance shows a discrepancy. MC&A also enables the operators to: (a) know precisely the quantity and type of all inputs and outputs of nuclear material in their facilities; (b) always be aware of the location, use, movement and transformation of nuclear material; and (c) detect any anomalies concerning the management of nuclear material. The nuclear material accountancy system should be able to detect unauthorized transfers in or the repeated unauthorized removal of small quantities of nuclear material from a facility, which might not be detected by the physical protection system. The detection of anomalies should be supported by, in particular, the use of seals, tamper indicating devices and a computerized accounting system. An analysis of the MC&A system is necessary to understand the limits and vulnerabilities of such systems.

5.3. PREVENTIVE MEASURES

The aim of preventive measures is to exclude potential adversaries and to minimize the likelihood of insiders attempting a malicious act. The following are recommended as preventive measures:

(a) Identity verification. Identity verifications[2] authenticate an individual's identity. This confirms that the name and personal particulars of the individual in question are correct.
(b) Trustworthiness assessment. Trustworthiness assessments[2] are initial and ongoing assessments of an individual's integrity, honesty and reliability in pre-employment checks and checks during employment that are intended

[2] National laws may restrict the scope or conduct of identity verification and trustworthiness assessments in a State. The provisions of this Implementing Guide are without prejudice to the legal rights of individuals, including the right to due process, under national and/or international law.

to identify the motivation or behaviour of persons who could become insiders. These checks attempt to identify motivational factors such as greed, financial factors, ideological interests, psychological factors, desire for revenge (e.g. due to perceived injustice), physical dependency (e.g. on drugs, alcohol or sex) and factors due to which an individual could be coerced by outsiders. Such factors might be indicated by a review of criminal records, references, past work history, financial records, medical records and psychological examinations/records. Periodic checks should be conducted during employment as some of these conditions may not be apparent or may change over time. These reviews are of particular interest in the case of temporary employees and workers whose duties may place them close to sensitive targets. The depth of the trustworthiness checks should be graded according to the level of access the individual has (e.g. access to Category III material will require the lowest level of trustworthiness checks and access to Category I material or vital areas will require the highest level of trustworthiness checks). This should be determined in line with the actions described in Sections 2–4 of this guide, which show the reasoning for gathering the information.

(c) Escort and surveillance of infrequent workers and visitors. Temporary workers, such as maintenance, service or construction workers, often come from contracting or subcontracting companies. The trustworthiness of temporary workers and visitors may not have been determined prior to their being permitted access. Escorting such people is a way of making sure that they are in the right place and that they are performing their duties properly. To be effective, the escort should know about their approved activities, including access to specific places and actions they should not perform. In addition, guard patrols may deter or detect any attempt by individuals to carry out malicious acts.

(d) Security awareness. Implementing a strong security awareness programme for staff and contractors contributes to an ongoing security culture within the organization. A strong security awareness programme requires clear security policies, the enforcement of security practices and continuous training. The purpose of the training programme is to establish an environment in which all employees are mindful of security policies and procedures, so that they can aid in detecting and reporting inappropriate behaviour or acts. Everyone, irrespective of their role or function, should be aware of the threats and potential consequences of malicious acts and of their own role in reducing the risks and in developing a comprehensive and effective security framework. Security awareness programmes should also provide for measures to reduce risks of blackmail, coercion, extortion or other threats to employees and their

families, and should promote the reporting of such coercions or attempts thereof to the security management. Finally, security awareness programmes should be developed in a coordinated manner with safety awareness programmes in order to establish effective and complementary safety and security cultures.

(e) Confidentiality (security of information). Information on security measures or sensitive targets (e.g. the location of the nuclear material inventory, site maps or specific drawings of equipment, systems or devices that represent the design features of specific targets, lock combinations, passwords and mechanical key designs) could help insiders successfully to perform a malicious act. This information should be kept confidential so that only those who need to know are permitted access to it. In addition, information addressing potential vulnerabilities in physical protection systems should be highly protected and compartmentalized, as it could facilitate the unauthorized removal of nuclear material or an act of sabotage. Compartmentalization means dividing information into separately controlled parts to prevent insiders from collecting all the information necessary to attempt a malicious act. Special attention should be paid to electronic information. Ensuring confidentiality will mean that insiders would have to make additional efforts to carry out unauthorized removal of nuclear material or an act of sabotage, during which they could be deterred or detected.

(f) Quality assurance. A quality assurance policy and programmes should be established and implemented with a view to providing confidence that specified requirements for all activities important for the prevention of and protection against insider threats are satisfied. This applies not only to prevention but also to the other primary functions.

(g) Employee satisfaction. It cannot be assumed that just because an individual is an employee or a contractor, he or she will be free from dissatisfaction. Therefore, good relations among workers and between management and workers should be given due consideration and should be part of the security culture. Managers should be trained to identify and raise any concerns about an employee's behaviour with an appropriate person, for example a senior manager, security manager or human resource adviser. The implementation of a career enhancement policy that has the goal of training all employees for the next higher position in the organization will help to create a pool of trained experts who may replace an incumbent leaving the organization even at short notice, and will also support quality assurance.

(h) Physical compartmentalization of areas. Compartmentalizing facility access by means of measures for access control minimizes the opportunity

for sabotage or the unauthorized removal of nuclear material by insiders by making it more difficult to obtain data dealing with security, targets and the full capability needed to perform a malicious act. Every effort should be made to ensure that a single person does not acquire all the necessary access authorizations that would enable such an individual to commit a malicious act. The significance of the physical compartmentalization of areas has to be consistent with the potential risks; therefore, the most sensitive targets should be located in well protected areas, whereas less sensitive targets could be located in less secure areas. Need-to-access rules, similar to the need-to-know rules that apply to sensitive documents and information, should apply to compartmentalized areas. Strictly limiting the number of persons with access to a sensitive area and also the number of persons empowered to give access authorization to sensitive areas can minimize opportunities for insiders. In the design phase, specific attention should be paid to minimizing unnecessary access to protected areas.

(i) Compartmentalization of activities. Compartmentalization of activities will limit the ability of insiders to obtain the set of capabilities necessary to conduct a malicious act. Such capabilities might include the ability to use special tools and equipment required for operations or for handling material. Transfer of tools, material and equipment between areas should be formalized and should involve more than one person in order to minimize opportunities for unauthorized removal of nuclear material by insiders.

(j) Sanctions (disciplinary actions and prosecution). It is important that potential insiders be aware that deliberate violation of laws and regulations or the instructions of the operator may be severely sanctioned. The certainty of disciplinary action and prosecution may deter insiders from committing malicious acts. In addition, requiring operators to inform the competent authority of every malicious act or attempt would provide, after proper analysis, a basis for feedback to other operators and for a possible need for updating of regulatory requirements.

5.4. PROTECTIVE MEASURES

The aim of protective measures is to detect, delay and respond to malicious acts after their initiation, and to mitigate or minimize their consequences. When designing and implementing protective measures, efforts should be made to ensure that these measures have minimal impact on

radiation protection, safety or emergency response systems. In case of conflict, a solution must be reached in which the overall risk to the workers and the public is minimized. The following items are recommended as protective measures.

5.4.1. Detection

Malicious acts can be detected by means of security sensors, personnel surveillance and/or monitoring of operational processes. In the case of outsiders, detection measures focus on detecting penetration of protective layers by adversaries. Detection of malicious acts committed by insiders is more difficult. Insiders may be able to bypass many detection measures, owing to their access or by other available means. Therefore, protection measures in respect of insider threats should focus on the detection of insiders both during acts and during preparatory (unauthorized) acts such as the manipulation of safety equipment or the falsification of MC&A records. Therefore, the detection of insiders may occur far later in the incident sequence than the detection of outsiders.

To be effective, detection must be assessed. It may be difficult to assess properly and quickly the nature of an act committed by an insider. This difficulty may seriously weaken the ability to respond in a timely manner.

Since detection of malicious acts by insiders is heavily dependent on observation and surveillance, enforcing a longer delay on the actions of an insider may result in a higher probability of detection; therefore, an increase in a physical barrier or the complexity of achieving the malicious act can provide additional opportunities for detection or even deter insiders from attempting the malicious act.

The objectives of surveillance measures are to ensure that the activities of any authorized employee are always monitored by at least one other experienced, authorized employee in order that unauthorized acts on the part of one can be immediately detected and reported (the ‘two person rule’). This method of detection can afford a rapid means of both generating and assessing an alarm. Surveillance may be provided through co-workers, managers or closed circuit television coverage. In the event of a malicious act, recorded videos can be useful to put together a list of possible suspects. In fact, without monitoring, timely assessment of malicious acts may be difficult. A method that may be used to detect insiders is on the job surveillance to check whether unauthorized activities are occurring. This method would be useful in cases such as an individual who does an incomplete job of equipment servicing, or a certain quantity of nuclear material being taken to perform a duty and another quantity being reported.

The two person rule requires at least two experienced persons to monitor one another in a sensitive area. This basic procedure is extended to require that at least two persons be present in a sensitive area in order for each person to verify that all actions are performed as authorized. Each of the two persons involved in the task should be technically qualified to immediately detect unauthorized activities. In addition, means should be provided to immediately report suspected malicious acts or suspicious activity. If subsequent investigation shows that no malicious acts were carried out, it is important that no penalty be imposed on either party for the false alarm, otherwise partners will be hesitant to report suspicious behaviour. This should be emphasized in security awareness training. To be effective, the two people must remain in full view of each other at all times, and must be fully informed about the authorized activities of the other. Ideally, the two person rule would assign two competent persons to perform a one person job. The two person rule is effective as long as the individuals do not become complacent through long term friendship or association. Whenever possible, managers should ensure that the members of such two person teams are rotated. Enforcing the two person rule for access to sensitive areas is a deterrent and may be an aid to detection. In addition, the two person rule can help to protect against insiders tampering with sensors.

Access control is used to allow only authorized entry or exit, and to prevent or detect unauthorized entry and exit. Access control is achieved by identifying individuals by means of an identifying device (one or more badges or keys), an access code (a lock combination or a personal identification number) and/or a personal identifier (biometrics). Access control provisions should also cover vehicles. Further, access control can be used to find out when people are present in different areas. If appropriately recorded, access control records can be used during the investigation of a malicious act to determine a list of possible suspects. Specific criteria should be established before authorizing access to a sensitive area (such as need to do a duty, need to be escorted, need to know and trustworthiness). Individuals granted access to a sensitive area should meet these criteria. Equipment used to generate badges and systems to assign access should be protected to prevent unauthorized assignment of access. Further, an access system should be periodically checked to ensure that it is effective.

Tracking the movement and location of personnel within the facility assists in protecting against violation of access rules and also in providing useful information after an incident. Existing technology makes it possible to track each worker throughout a facility by recording the locations and areas visited each day by the worker and the times that each location was visited. Awareness that a facility has a tracking system may deter a worker from carrying out

unauthorized activities. Further, tracking records may be used during the investigation of a malicious act to generate an initial list of suspects.

Insiders may require tools, material and weapons that are unavailable or not allowed within the facility to carry out a malicious act. Therefore, checks should be made to prevent and detect the introduction of contraband items into sensitive areas. Contraband items may include unauthorized tools and material, radiation shielding material, weapons and explosives, as these could be used to gain access to or cause damage to sensitive components as well as to steal nuclear material. The stringency of searches should be commensurate with the sensitivity of the area, and searches performed close to the target should also be more stringent.

Methods of contraband detection include manual searches of personnel, packages and vehicles; use of metal detectors, X ray machines and radiation detectors; and use of dogs and explosives detectors. These methods should take into account the specifics of the facility and the threats against which protection is required. In specifying the locations at which searches are to be carried out, care should be taken not to place them so far from the sensitive areas that it would be easy to bypass the checks. For example, insiders might bypass checks on the protected area boundary by throwing contraband over the protected area fence for later retrieval. Since vehicles are more difficult to search than personnel, it is advantageous to significantly limit the number of authorized vehicles permitted to enter the sensitive areas.

For certain types of nuclear material, radiation detectors should be used to detect its unauthorized removal on persons, in packages or in vehicles leaving a protected area. Radiation detectors could be placed at pedestrian exits in tandem with metal detectors to enhance their effectiveness, as shielding material can be used to remove nuclear material from the nuclear facility. Manual searches may also be used for monitoring persons and material exiting from an area. Random searches can be used to deter the unauthorized removal of nuclear material. If this is not in violation of safety rules, the exit should be locked on actuation of a security alarm. Particular attention should be paid to emergency evacuation conditions, including exercises, to prevent the unauthorized removal of nuclear material. Special care should be taken during the detailed search of a load vehicle prior to loading and shipment to ensure that those persons carrying out the search are not able to introduce items that would aid a malicious act.

Monitoring the normal operation of processes or activities can be used to survey an area, to detect an unauthorized action or to provide an early assessment of alarms. The operating parameters of a nuclear facility (temperatures, pressures, flows, radiation monitoring, etc.) are checked continuously to ensure that they remain within the operating limits. An alarm should be

activated when one of these parameters exceeds a specified threshold. Since sabotage can cause an abnormal situation of the operating parameters, surveillance of operating parameters may help to detect malicious acts.

It is critical that a procedure for reporting of alarms be established between operations personnel and security personnel to ensure that alarms are quickly communicated to security personnel in the central alarm station. The actuation of an alarm should be communicated even prior to operations personnel assessing its cause (malicious or accidental).

Operations personnel should monitor sensitive equipment, systems or devices to verify that no tampering or interference has taken place, or to provide for the timely detection of such tampering or interference.

Routine testing and maintenance operations have a significant impact on equipment availability and the prevention or correction of a deficiency or failure that could have a malicious origin. These operations may be very effective in detecting possible malicious acts on equipment or systems in relation to protecting nuclear material or sensitive areas. When a routine testing or maintenance operation leads to a modification of the initial conditions of a system, a requalification of this system should be performed. It is advisable to perform the requalification independently of the operation (test or maintenance) leading to the modification. This approach contributes to both prevention by deterrence (for fear of the consequences) and detection.

One measure to mitigate the consequences of a malicious act is to have the capability rapidly to replace parts that have been damaged. To achieve the desired goal successfully, it is prudent to provide protection for spare parts so that it would be difficult to destroy or compromise both the installed parts and the spare parts for vital equipment. Protection can be provided by, for example, installing barriers, storing the spare part at a distance from the installed part and frequently monitoring storage.

Inspections and audits, in particular unannounced inspections and audits, might be an efficient way to prevent and protect against unauthorized removal of nuclear material and sabotage. Inspections and audits can detect compromised equipment or abnormal conditions and, thus, can provide assurance to operators, the competent authority or the State that preventative and protective measures are effectively implemented.

5.4.2. Delay

Delay is provided by personnel, procedures or physical barriers that increase the task time of an adversary. Most barriers are designed to delay penetration of areas, rather than to delay the carrying out of malicious acts, and thus have only limited impact on insiders. However, it is possible to develop

barriers to delay malicious acts close to equipment or material. For example, locking a piece of equipment, such as a valve or a switchboard, creates a delay for insiders attempting to carry out an act of sabotage. Barriers close to equipment or material are especially effective when the area is under continuous surveillance.

For insiders who do not have access to certain areas or material, installing barriers that an adversary could not overcome without using contraband items or highly specialized skills further strengthens prevention by deterrence and increases the likelihood of detection. Multiple layers of different physical or procedural barriers along all possible insider paths will complicate the progress of an insider by requiring a variety of tools and skills. Upgrading a barrier to force insiders to use more sophisticated tools complicates the requirements for resources, logistics, training and skills. Sophisticated resources may not be available at the facility and may have to be introduced on the site by insiders. By delaying the malicious act in this manner, insiders could be detected and defeated.

Delays can also be accomplished by the use of specially trained security personnel, such as guards. In some cases, the presence of such personnel may result in a significant delay in order to circumvent them, particularly for insiders with limited resources.

As a result of system safety designs that provide for some level of system self-protection, such as redundant equipment, automatic equipment shutdown and automatic valve closure, the task of an insider may be complicated by requiring the insider to defeat multiple redundant and dispersed facilities and equipment. These features can delay a malicious act and prevent it from being successfully carried out.

5.4.3. Response

Response to a malicious act by an insider can be made by both operations personnel and security personnel. Typically, operations personnel respond to the malicious act in order to reverse, mitigate or minimize it, and security personnel respond to insiders.

Classical analysis of response to outsider threats compares the response force time with the time required for a sequence of outsider acts necessary to complete a malicious action. The implicit assumption in an outsider threat analysis is that the outsider will be easily identified anywhere on the site. None of this may be true for insiders, since a malicious act committed by an insider can consist of several acts separated in both time and space. Unless insiders are identified when detected, it may be difficult to apprehend them among the workers.

As mentioned above, an insider would not necessarily need to perform all the acts in a prescribed order, nor in quick succession. An insider may commit single acts and then wait to see if they are detected. The non-continuous nature of acts that insiders might attempt can seriously complicate the security response necessary to identify and apprehend them. As a result, investigation will play a more important role in response to insider threats. Furthermore, operations specialists may be required to assist in the investigation to predict, from the abnormal event, what further malicious acts might be attempted.

Every employee and contractor on the facility site not only should be prepared to detect a malicious act but also should be trained to react appropriately to protect themselves and the facility, and should know that the first action to take after detecting an event is to transmit the alarm according to a specified set of procedures. The procedures for transmitting the alarm should be a part of security awareness training.

It is important to recognize that any persons involved in response may themselves be insiders, and therefore response procedures should be developed with this assumption. For example, an insider in the response team might use an emergency exercise, simulate an emergency or create an actual emergency to mask a malicious act.

5.4.4. Emergency plans

Emergency plans should be developed to recover stolen nuclear material and to mitigate or minimize the radiological consequences of sabotage. Emergency plans do not usually differentiate between insiders and outsiders. Consideration should be given to the fact that insiders could be members of the emergency response team and could disrupt recovery or mitigation efforts.

Emergency plans for recovery or mitigation should be prepared to effectively counter the consequences of sabotage or unauthorized removal. They should describe communication, provisions for recovery or mitigation, and immediate countermeasures to be applied in the event of unauthorized removal of nuclear material or sabotage.

Such plans should provide for the training of guards and response forces to perform their actions in the event of a malicious act. In addition, other facility or transport personnel should be trained and prepared to act in full coordination with guards, response forces and emergency response teams for the implementation of contingency plans.

To ensure that no nuclear material is removed without authorization, the emergency plans should specify procedures to rapidly verify that all nuclear material is still present in the facility or in the transport unit. The MC&A procedures should verify both the presence and quality of nuclear material to

be sure that there is no substitution of inert or dummy material. These provisions could be complemented by actions taken at the State level to provide information and technical assistance to locate and recover missing nuclear material, if necessary.

Emergency plans should ensure coordination and protocols for operational interfaces between operators and local, regional and national authorities. Emergency plans developed for malicious incidents should be designed and coordinated within the general emergency response arrangements. In particular, emergency plans should be developed and implemented in compliance with the international requirements for preparedness and response for a nuclear or radiological emergency [8, 9].

6. EVALUATION OF PREVENTIVE AND PROTECTIVE MEASURES

6.1. OBJECTIVES AND OVERVIEW OF THE EVALUATION PROCESS

This section provides guidance on the process of evaluating the risk in relation to the targets of concern that have been identified. This evaluation process is a key component of a risk assessment that is intended to identify vulnerabilities of systems to insider threats. The result of the evaluation process is an evaluation of the effectiveness of preventive and protective measures in countering possible insider actions that could lead to the unauthorized removal of nuclear material or sabotage.

The results of the evaluation of the effectiveness of the measures should be compared with previously established acceptance criteria. The acceptance criteria are usually established by the State or competent authority and are based on the potential consequences of the malicious action and its likelihood of success. If the evaluation indicates that preventive and protective measures do not meet the required acceptance criteria, upgrades should be implemented.

In addition, consideration should be given to:

(a) The relative ease of performing a malicious action. A scenario for which the consequences are deemed acceptable but which is relatively easy to perform may be unacceptable (e.g. unauthorized alteration of a threshold

in the process or unauthorized alignment of a circuit) and may require corrective action.

(b) The level of risk. The risk may be deemed acceptable but may be close to the threshold beyond which the level of the risk is no longer acceptable. Such a case should not be disregarded and prudent management may require additional protective measures.

The effectiveness of the protective and preventive measures should be re-evaluated periodically, in particular whenever there are changes in the design basis threat, in the preventive and protective measures or in the operating conditions.

This guidance addresses both preventive and protective measures, and the evaluation process should also address both in order to ensure that security measures are effective.

6.2. EVALUATION OF PREVENTIVE MEASURES

Rigorous evaluation of steps 1 and 2 (exclusion of potential insiders) described in Section 5.1 is difficult as with all preventive measures, but the measures applied (such as trustworthiness checks prior to and during employment) are believed to be effective in reducing — but not completely eliminating — the possibility of insiders. These measures are reasonable and prudent precautions even if their effect cannot be quantitatively evaluated.

However, the effective implementation of preventive measures can be checked and criteria can be specified and analysed to ensure that the preventive measures are implemented as designed. For example, analyses can be made of the number of individuals refused access to a facility site, of individuals no longer authorized to have access to the facility site after employment termination, and of incidents reported.

Step 3 (minimization of opportunity) in the approach to prevent and protect against malicious acts by insiders (described in Section 5.1) is accomplished by reducing the possibility of an insider gaining the access, authority or knowledge necessary to successfully carry out a malicious act leading to unacceptable radiological consequences. The degree and manner of limitation of opportunity is an important element in guiding the development of credible scenarios. Therefore, in addition, a systematic review should be performed to indicate which preventive measures, such as those proposed in Section 5.3, are in place and are properly applied.

6.3. EVALUATION OF PROTECTIVE MEASURES

The measures used to detect, delay and respond to malicious acts can be quantitatively analysed. Likelihood of detection and timeliness of response are often quantifiable and thus provide a basis for an analysis of the effectiveness of the protective measures.

The process presented recognizes the value of steps 1, 2 and 3 (see Section 5.1) and encourages their prudent application, but the emphasis is on assessing the effectiveness of the protective measures to counter a malicious act. The approach involves developing credible insider scenarios, including scenarios of collusion with outsiders, as appropriate, and then evaluating the effectiveness of the protection system against them.

The development of credible scenarios consists of identifying the combination of events necessary to accomplish the malicious act. For sabotage, consideration should be given to the actions that must be accomplished to initiate a sequence leading to unacceptable radiological consequences. Sabotage scenarios should include attacks on both single and multiple targets. For unauthorized removal of nuclear material, the actions that must be successively accomplished to remove nuclear material from the facility should be identified. Scenarios involving unauthorized removal of nuclear material should include situations in which insiders leave the facility directly with nuclear material or hide material on the facility site, removing it later under more favourable circumstances. Both protracted and abrupt theft should be considered.

To develop comprehensive scenarios, pairing identified targets (Section 4) with defined insider groups (Section 2) should be considered. Taking into account the design basis threat, the tasks that an insider would need to carry out should be defined in specific terms, for example the set of actions that must be taken to achieve the goal. The set of actions should include both general actions and the areas where they are performed. The actions may occur along paths within the facility. All the protection elements that could be encountered by insiders along each of these paths or sets of actions should be defined. The paths, the set of actions along the path and the protective elements encountered should all be taken into consideration. As insiders can perform the actions required for the malicious act over an extended period, and may not follow a predictable sequence, the concept of a path may not always be relevant.

The effectiveness of the protection elements against the various defeat strategies that may be used by insiders should be assessed. Defeat strategies are developed by considering the access, authority and knowledge of insiders to overcome the detection and delay features. By combining protection elements and insider defeat strategies for a set of insider actions, a credible insider

scenario can be developed. It should be noted that paths for contraband material into a facility or unauthorized removal of nuclear material from a facility may not be the same as the paths used by insiders.

Once a detailed insider scenario has been developed, the effectiveness of the protective measures is evaluated by considering the accumulated impact of detection, assessment and delay, and by overlaying the response and mitigation measures on the insider scenario. The effectiveness of the response will depend on both the effectiveness of interrupting the malicious act and the effectiveness of preventing the consequences. Possible efforts by insiders to reduce the effectiveness of the response should be considered in the evaluation.

The evaluation process should be repeated for every credible scenario. Conclusions on the effectiveness of protective measures should reflect the results of all the evaluations above.

After the evaluation of protective measures has been completed, the results can be combined to provide a broad view of the status of protection in the facility or transport unit.

Scenario analysis provides insight into possible improvements of protective measures. The scenarios should be prioritized by tabulating the effectiveness of the protective system for each target/insider pair and then applying predetermined criteria to establish priorities for each target/insider pair scenario. The criteria for establishing priorities should be based on both the system effectiveness for the scenario at hand and the potential consequences of its successful completion. For example, scenarios with low system effectiveness and high resulting consequences should be given high priority, while scenarios with high system effectiveness and low consequences would have much lower priority. The highest priority scenarios should be evaluated first to determine possible system improvements that would increase the effectiveness of the system. The scenarios should be examined in detail for possible improvements. Actions where little or no detection, assessment and delay could be implemented should be identified. Scenarios in which the response would be slow or ineffective should be evaluated for possible response improvements. Possible solutions for these situations could range from procedural changes to equipment applications.

As improvements are developed, care should be taken to ensure that improvements in protection for certain scenarios do not degrade the system performance for other scenarios and do not have unacceptable effects on operational and safety systems. The proposed improvements should be added and another analysis carried out to determine the degree of improvement that could be gained. This process may need to be repeated several times before satisfactory, defendable solutions can be formulated, and performance based rationales should be documented to support recommendations for improvements.

REFERENCES

[1] Convention on the Physical Protection of Nuclear Material, INFCIRC/274/Rev.1, IAEA, Vienna (1980).

[2] Nuclear Security — Measures to Protect against Nuclear Terrorism, Amendment to the Convention on the Physical Protection of Nuclear Material, Report by the Director General, GOV/INF/2005/10-GC(49)/INF/6, IAEA, Vienna (2005).

[3] Physical Protection Objectives and Fundamental Principles, GOV/2001/41, IAEA, Vienna (2001).

[4] The Physical Protection of Nuclear Material and Nuclear Facilities, INFCIRC/225/Rev.4 (Corrected), IAEA, Vienna (1999).

[5] INTERNATIONAL ATOMIC ENERGY AGENCY, Guidance and Considerations for the Implementation of INFCIRC/225/Rev.4, IAEA-TECDOC-967 (Rev.1), IAEA, Vienna (2000).

[6] INTERNATIONAL ATOMIC ENERGY AGENCY, Handbook on the Physical Protection of Nuclear Material and Facilities, IAEA-TECDOC-1276, IAEA, Vienna (2002).

[7] INTERNATIONAL ATOMIC ENERGY AGENCY, IAEA Safeguards Glossary: 2001 Edition, International Nuclear Verification Series No. 3, IAEA, Vienna (2002).

[8] INTERNATIONAL ATOMIC ENERGY AGENCY, Preparedness and Response for a Nuclear or Radiological Emergency, IAEA Safety Standards Series No. GS-R-2, IAEA, Vienna (2002).

[9] INTERNATIONAL ATOMIC ENERGY AGENCY, Arrangements for Preparedness for a Nuclear or Radiological Emergency, IAEA Safety Standards Series No. GS-G-2.1, IAEA, Vienna (2007).

NUCLEAR SECURITY CULTURE
IAEA Nuclear Security Series No. 7
STI/PUB/1347 (38 pp.; 2008)
ISBN 978-92-0-107808-7 Price: €30.00

SECURITY IN THE TRANSPORT OF RADIOACTIVE MATERIAL
IAEA Nuclear Security Series No. 9
STI/PUB/1348 (40 pp.; 2008)
ISBN 978-92-0-107908-4 Price: €20.00

COMBATING ILLICIT TRAFFICKING IN NUCLEAR AND OTHER RADIOACTIVE MATERIAL
IAEA Nuclear Security Series No. 6
STI/PUB/1309 (143 pp.; 2007)
ISBN 978-92-0-109807-8 Price: €40.00

IDENTIFICATION OF RADIOACTIVE SOURCES AND DEVICES
IAEA Nuclear Security Series No. 5
STI/PUB/1278 (138 pp.; 2007)
ISBN 92-0-111406-0 Price: €45.00

ENGINEERING SAFETY ASPECTS OF THE PROTECTION OF NUCLEAR POWER PLANTS AGAINST SABOTAGE
IAEA Nuclear Security Series No. 4
STI/PUB/1271 (58 pp.; 2007)
ISBN 92-0-109906-1 Price: €30.00

MONITORING FOR RADIOACTIVE MATERIAL IN INTERNATIONAL MAIL TRANSPORTED BY PUBLIC POSTAL OPERATORS
IAEA Nuclear Security Series No. 3
STI/PUB/1242 (39 pp.; 2006)
ISBN 92-0-100406-0 Price: €23.00

NUCLEAR FORENSICS SUPPORT
IAEA Nuclear Security Series No. 2
STI/PUB/1241 (67 pp.; 2006)
ISBN 92-0-100306-4 Price: €26.00

CODE OF CONDUCT ON THE SAFETY AND SECURITY OF RADIOACTIVE SOURCES
IAEA/CODEOC/2004
(122 pp.: 2004) Price: Cost free

This Implementing Guide presents a comprehensive methodology for the development of preventive and protective measures against insider threats to nuclear facilities and nuclear material transport operations of all types. Institutional insiders who are privy to the inner workings of security systems present a unique challenge to the establishment of effective control systems for nuclear material. They generally possess access rights which, together with their authority and knowledge of facilities, grant them far greater opportunity than for any outsider to bypass dedicated physical protection elements or other provisions such as safety systems and operating procedures. Furthermore, insiders, as trusted persons, are capable of methods of defeat that are not available to outsiders. This publication provides guidance and measures for reducing these and other risks posed by insiders.

INTERNATIONAL ATOMIC ENERGY AGENCY
VIENNA
ISBN 978–92–0–109908–2
ISSN 1816–9317