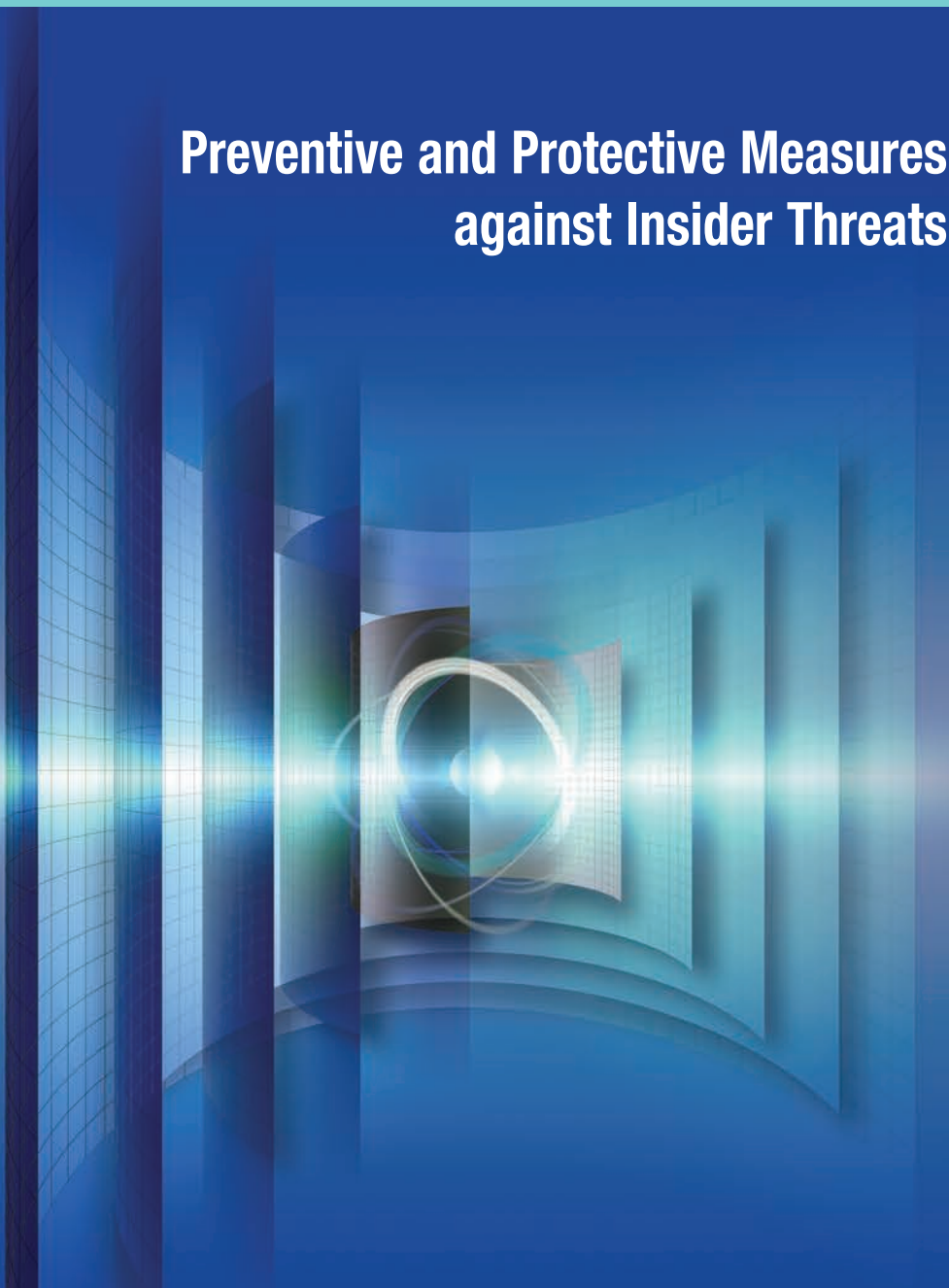
IAEA Nuclear Security Series No. 8-G (Rev. 1)

Implementing Guide

Preventive and Protective Measures against Insider Threats



IAEA
International Atomic Energy Agency

IAEA NUCLEAR SECURITY SERIES

Nuclear security issues relating to the prevention and detection of, and response to, criminal or intentional unauthorized acts involving, or directed at, nuclear material, other radioactive material, associated facilities or associated activities are addressed in the **IAEA Nuclear Security Series**. These publications are consistent with, and complement, international nuclear security instruments, such as the Convention on the Physical Protection of Nuclear Material and its Amendment, the International Convention for the Suppression of Acts of Nuclear Terrorism, United Nations Security Council resolutions 1373 and 1540, and the Code of Conduct on the Safety and Security of Radioactive Sources.

CATEGORIES IN THE IAEA NUCLEAR SECURITY SERIES

Publications in the IAEA Nuclear Security Series are issued in the following categories:

- **Nuclear Security Fundamentals** specify the objective of a State's nuclear security regime and the essential elements of such a regime. They provide the basis for the Nuclear Security Recommendations.
- **Nuclear Security Recommendations** set out measures that States should take to achieve and maintain an effective national nuclear security regime consistent with the Nuclear Security Fundamentals.
- **Implementing Guides** provide guidance on the means by which States could implement the measures set out in the Nuclear Security Recommendations. As such, they focus on how to meet the recommendations relating to broad areas of nuclear security.
- **Technical Guidance** provides guidance on specific technical subjects to supplement the guidance set out in the Implementing Guides. They focus on details of how to implement the necessary measures.

DRAFTING AND REVIEW

The preparation and review of Nuclear Security Series publications involves the IAEA Secretariat, experts from Member States (who assist the Secretariat in drafting the publications) and the Nuclear Security Guidance Committee (NSGC), which reviews and approves draft publications. Where appropriate, open-ended technical meetings are also held during drafting to provide an opportunity for specialists from Member States and relevant international organizations to review and discuss the draft text. In addition, to ensure a high level of international review and consensus, the Secretariat submits the draft texts to all Member States for a period of 120 days for formal review.

For each publication, the Secretariat prepares the following, which the NSGC approves at successive stages in the preparation and review process:

- An outline and work plan describing the intended new or revised publication, its intended purpose, scope and content;
- A draft publication for submission to Member States for comment during the 120 day consultation period;
- A final draft publication taking account of Member States' comments.

The process for drafting and reviewing publications in the IAEA Nuclear Security Series takes account of confidentiality considerations and recognizes that nuclear security is inseparably linked with general and specific national security concerns.

An underlying consideration is that related IAEA safety standards and safeguards activities should be taken into account in the technical content of the publications. In particular, Nuclear Security Series publications addressing areas in which there are interfaces with safety — known as interface documents — are reviewed at each of the stages set out above by relevant Safety Standards Committees as well as by the NSGC.

PREVENTIVE AND PROTECTIVE MEASURES AGAINST INSIDER THREATS

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

AFGHANISTAN
ALBANIA
ALGERIA
ANGOLA
ANTIGUA AND BARBUDA
ARGENTINA
ARMENIA
AUSTRALIA
AUSTRIA
AZERBAIJAN
BAHAMAS
BAHRAIN
BANGLADESH
BARBADOS
BELARUS
BELGIUM
BELIZE
BENIN
BOLIVIA, PLURINATIONAL STATE OF
BOSNIA AND HERZEGOVINA
BOTSWANA
BRAZIL
BRUNEI DARUSSALAM
BULGARIA
BURKINA FASO
BURUNDI
CAMBODIA
CAMEROON
CANADA
CENTRAL AFRICAN REPUBLIC
CHAD
CHILE
CHINA
COLOMBIA
COMOROS
CONGO
COSTA RICA
CÔTE D'IVOIRE
CROATIA
CUBA
CYPRUS
CZECH REPUBLIC
DEMOCRATIC REPUBLIC OF THE CONGO
DENMARK
DJIBOUTI
DOMINICA
DOMINICAN REPUBLIC
ECUADOR
EGYPT
EL SALVADOR
ERITREA
ESTONIA
ESWATINI
ETHIOPIA
FIJI
FINLAND
FRANCE
GABON
GEORGIA
GERMANY
GHANA
GREECE
GRENADA
GUATEMALA
GUYANA
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
LAO PEOPLE'S DEMOCRATIC REPUBLIC
LATVIA
LEBANON
LESOTHO
LIBERIA
LIBYA
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
NORTH MACEDONIA
NORWAY
OMAN
PAKISTAN
PALAU
PANAMA
PAPUA NEW GUINEA
PARAGUAY
PERU
PHILIPPINES
POLAND
PORTUGAL
QATAR
REPUBLIC OF MOLDOVA
ROMANIA
RUSSIAN FEDERATION
RWANDA
SAINT LUCIA
SAINT VINCENT AND THE GRENADINES
SAN MARINO
SAUDI ARABIA
SENEGAL
SERBIA
SEYCHELLES
SIERRA LEONE
SINGAPORE
SLOVAKIA
SLOVENIA
SOUTH AFRICA
SPAIN
SRI LANKA
SUDAN
SWEDEN
SWITZERLAND
SYRIAN ARAB REPUBLIC
TAJIKISTAN
THAILAND
TOGO
TRINIDAD AND TOBAGO
TUNISIA
TURKEY
TURKMENISTAN
UGANDA
UKRAINE
UNITED ARAB EMIRATES
UNITED KINGDOM OF GREAT BRITAIN AND NORTHERN IRELAND
UNITED REPUBLIC OF TANZANIA
UNITED STATES OF AMERICA
URUGUAY
UZBEKISTAN
VANUATU
VENEZUELA, BOLIVARIAN REPUBLIC OF
VIET NAM
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-G (Rev. 1)

PREVENTIVE AND PROTECTIVE MEASURES AGAINST INSIDER THREATS

IMPLEMENTING GUIDE

INTERNATIONAL ATOMIC ENERGY AGENCY
VIENNA, 2020

COPYRIGHT NOTICE

Marketing and Sales Unit, Publishing Section
International Atomic Energy Agency
Vienna International Centre
PO Box 100
1400 Vienna, Austria
fax: +43 1 26007 22529
tel.: +43 1 2600 22417
email: sales.publications@iaea.org
www.iaea.org/publications

Printed by the IAEA in Austria
January 2020
STI/PUB/1858

IAEA Library Cataloguing in Publication Data

Names: International Atomic Energy Agency.
Title: Preventive and protective measures against insider threats / International Atomic Energy Agency.
Description: Vienna : International Atomic Energy Agency, 2020. | Series: IAEA nuclear security series, ISSN 1816–9317 ; no. 8-G (rev. 1) | Includes bibliographical references.
Identifiers: IAEAL 19-01249 | ISBN 978–92–0–103419–9 (paperback : alk. paper) | ISBN 978–92–0–101120–6 (pdf) | ISBN 978–92–0–103821–0 (epub) | ISBN 978–92–0–103921–7 (mobipocket)
Subjects: LCSH: Nuclear facilities. | Radioactive substances. | Internal security.
Classification: UDC 341.67 | STI/PUB/1858

FOREWORD

The IAEA's principal objective under its Statute is "to accelerate and enlarge the contribution of atomic energy to peace, health and prosperity throughout the world." Our work involves both preventing the spread of nuclear weapons and ensuring that nuclear technology is made available for peaceful purposes in areas such as health and agriculture. It is essential that all nuclear and other radioactive materials, and the facilities at which they are held, are managed in a safe manner and properly protected against criminal or intentional unauthorized acts.

Nuclear security is the responsibility of each individual State, but international cooperation is vital to support States in establishing and maintaining effective nuclear security regimes. The central role of the IAEA in facilitating such cooperation and providing assistance to States is well recognized. The IAEA's role reflects its broad membership, its mandate, its unique expertise and its long experience of providing technical assistance and specialist, practical guidance to States.

Since 2006, the IAEA has issued Nuclear Security Series publications to help States to establish effective national nuclear security regimes. These publications complement international legal instruments on nuclear security, such as the Convention on the Physical Protection of Nuclear Material and its Amendment, the International Convention for the Suppression of Acts of Nuclear Terrorism, United Nations Security Council resolutions 1373 and 1540, and the Code of Conduct on the Safety and Security of Radioactive Sources.

Guidance is developed with the active involvement of experts from IAEA Member States, which ensures that it reflects a consensus on good practices in nuclear security. The IAEA Nuclear Security Guidance Committee, established in March 2012 and made up of Member States' representatives, reviews and approves draft publications in the Nuclear Security Series as they are developed.

The IAEA will continue to work with its Member States to ensure that the benefits of peaceful nuclear technology are made available to improve the health, well-being and prosperity of people worldwide.

EDITORIAL NOTE

This publication does not address questions of responsibility, legal or otherwise, for acts or omissions on the part of any person.

Guidance issued in the IAEA Nuclear Security Series is not binding on States, but States may use the guidance to assist them in meeting their obligations under international legal instruments and in discharging their responsibility for nuclear security within the State. Guidance expressed as 'should' statements is intended to present international good practices and to indicate an international consensus that it is necessary for States to take the measures recommended or equivalent alternative measures.

Security related terms are to be understood as defined in the publication in which they appear, or in the higher level guidance that the publication supports. Otherwise, words are used with their commonly understood meanings.

An appendix is considered to form an integral part of the publication. Material in an appendix has the same status as the body text. Annexes are used to provide practical examples or additional information or explanation. Annexes are not integral parts of the main text.

Although great care has been taken to maintain the accuracy of information contained in this publication, neither the IAEA nor its Member States assume any responsibility for consequences which may arise from its use.

The use of particular designations of countries or territories does not imply any judgement by the publisher, the IAEA, as to the legal status of such countries or territories, of their authorities and institutions or of the delimitation of their boundaries.

The mention of names of specific companies or products (whether or not indicated as registered) does not imply any intention to infringe proprietary rights, nor should it be construed as an endorsement or recommendation on the part of the IAEA.

CONTENTS

1. INTRODUCTION

BACKGROUND

1.1. The IAEA Nuclear Security Series provides guidance for States to assist them in implementing, reviewing and, when necessary, strengthening a national nuclear security regime. The series also provides guidance for States on fulfilling their obligations and commitments with respect to binding and non-binding international instruments. The Nuclear Security Fundamentals publication (IAEA Nuclear Security Series No. 20 [1]) provides the objective and essential elements for the entire nuclear security regime. Recommendations publications indicate what a nuclear security regime should address for the physical protection of nuclear material and nuclear facilities [2], radioactive material and associated facilities [3], and nuclear and other radioactive material out of regulatory control [4]. These publications, as well as many others in the IAEA Nuclear Security Series (Refs [5–12]), recognize the particular threats that could be posed by insiders, as well as the need to implement specific measures against insider threats and to evaluate those measures accordingly.

1.2. This publication is an update of IAEA Nuclear Security Series No. 8, Preventive and Protective Measures against Insider Threats, published by the IAEA in 2008[1]. This revision was undertaken to better align this Implementing Guide with the Nuclear Security Fundamentals and with the Recommendations that were published after 2008, to cross-reference other relevant Implementing Guides published since 2008, and to add further detail on certain topics based on the experience of the IAEA and Member States in using IAEA Nuclear Security Series No. 8.

OBJECTIVE

1.3. The objective of this Implementing Guide is to provide updated guidance to States, their competent authorities and operators[2], shippers, and carriers on

---

[1] INTERNATIONAL ATOMIC ENERGY AGENCY, Preventive and Protective Measures against Insider Threats, IAEA Nuclear Security Series No. 8, IAEA, Vienna (2008).

[2] 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.

selecting, implementing and evaluating measures for addressing insider threats. Threats to nuclear facilities can involve external or insider adversaries or both together in collusion (cooperation for an illegal or malicious purpose with another insider adversary or with an external adversary).

SCOPE

1.4. This publication applies to preventing and protecting against unauthorized removal of nuclear material and sabotage of nuclear material and facilities by insiders. This publication 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, storage facilities) — whether in design, redesign, construction, commissioning, operation, shutdown or decommissioning.

1.5. The guidance in this publication on insider threats may also be applied to preventing and protecting against unauthorized removal and sabotage of radioactive material and associated facilities [3]; securing nuclear and radioactive materials undergoing transport [6, 13]; and the prevention and detection of, and response to, nuclear and other radioactive material out of regulatory control [4]. This guidance may also be applied to securing facility information held or obtained by other stakeholders, including the competent authority [8].

1.6. For the purposes of this publication, insider access to a facility includes physical access to locations and material; internal or authorized remote computer or network access; and access to sensitive information about the facility.

1.7. While safety considerations are not addressed in this publication, the preventive and protective measures described should be implemented in a balanced manner that is compatible with safety considerations and that considers worker radiation protection. Security measures and safety measures should be designed and implemented in an integrated manner to develop synergy between these two areas and in such a way that security measures do not compromise safety and safety measures do not compromise security [1].

STRUCTURE

1.8. After this introduction, this publication is separated into four sections. Section 2 introduces insider threats and ways to categorize insiders. Section 3

identifies the targets and facility systems to be protected against malicious acts by insiders. Section 4 discusses implementation at the facility level of preventive and protective measures to address insider threats. Section 5 discusses the evaluation of the measures discussed in Section 4.

2. IDENTIFICATION OF INSIDER THREATS

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

2.2. The term 'insider' is used to describe

> "an individual with authorized access to [nuclear material,] *associated facilities* or *associated activities* or to *sensitive information* or *sensitive information assets*, who could commit, or facilitate the commission of criminal or intentional unauthorized acts involving or directed at *nuclear material*, *other radioactive material*, *associated facilities* or *associated activities* or other acts determined by the State to have an adverse impact on nuclear security" [1].

The term 'external adversary' is used to describe an adversary other than an insider.

ATTRIBUTES OF INSIDERS

2.3. Insiders possess at least one of the following attributes that provide advantages over external adversaries when attempting malicious activities:

(a) Access: Insiders have authorized access to the areas, equipment and information needed to perform their work. Access includes physical access to nuclear facilities; nuclear materials and associated systems, components and equipment; and computer systems. Access also includes remote computer access to a facility, such as access to computer systems and networks that control processes, provide safety, contain sensitive information or otherwise contribute to nuclear security. The operator should not permit remote access to critical systems, such as systems relevant to safety.

(b) Authority: Insiders are authorized to conduct operations as part of their assigned duties and may also have the authority to direct other employees. This authority may be used to support malicious acts, including either physical or computer based acts such as digital file or process manipulation.
(c) Knowledge: Insiders may possess knowledge of the facility, associated activities or systems, ranging from limited to expert knowledge. This may include knowledge that could enable an insider to bypass or defeat dedicated physical protection systems and other facility systems that contribute to nuclear security, such as safety and nuclear material accounting and control (NMAC) systems, operating procedures and response capabilities.

These attributes may also include access to, or knowledge of, sensitive information or sensitive information assets, including information regarding the transport or movement of nuclear material [13].

2.4. An insider might not possess all three attributes but might still have sufficient capability to conduct a malicious act. For example, a headquarters manager may have limited physical access to a facility but could have the authority to issue a counterfeit delivery order to an outside location. Insider adversaries may use feigned authority or knowledge to facilitate or initiate a malicious act. An insider adversary may act independently or in collusion with another insider adversary or with an external adversary.

2.5. Owing to their access, authority and knowledge, insiders have the opportunity to select the most vulnerable target and the best time to attempt or perform a malicious act. To maximize the likelihood of success, an insider adversary might extend a malicious act over a long period of time. This tactic could consist of (a) tampering with physical protection equipment or safety equipment to prepare for an act of sabotage, (b) falsifying records so that the insider adversary is able to repeatedly remove without authorization small amounts of lower category nuclear material that has less robust protection than higher category nuclear material without being detected or (c) removing nuclear material without authorization in amounts below measurement system detection thresholds. Insider adversaries may have the opportunity to commit a malicious act during normal or abnormal conditions of a facility, including during maintenance, or during the movement of nuclear material, and may select the most favourable time to do so [14].

MOTIVATIONS OF INSIDERS

2.6. Insiders may have different motivations for initiating malicious acts, including money, ideology, revenge, ego, coercion or a combination of these motivations.

2.7. An insider may independently develop sufficient motivation to perform a malicious act, including as the result of a mental health issue. An insider may also be recruited by an external adversary seeking to exploit the insider's access, authority or knowledge. An insider could be forced to commit a malicious act through coercion (e.g. blackmail).

2.8. An insider could hold any position within an organization, from the highest level to the lowest. Insiders at all levels could have sufficient motivation to perform a malicious act. Other personnel not directly employed by the operator, shipper or carrier but who have authorized access on a periodic basis to the facility or its systems (e.g. vendors, first responders, contractors, inspectors from regulatory bodies or other competent authorities) should also be considered to be potential insider threats.

CATEGORIES OF INSIDERS

2.9. An unwitting insider is an insider without the intent and motivation to commit a malicious act who is exploited by an adversary without the unwitting insider's awareness. For example, in a computer based attack, an unwitting insider may not be aware that certain actions (e.g. clicking a malicious link in an email that is disguised as being from a trusted source) may provide information or authenticated access to an adversary.

2.10. An insider adversary is an insider that commits malicious activities with awareness, intent and motivation. An insider adversary may be passive or active, and an active insider adversary may be either violent or non-violent. This categorization is useful for assessment purposes, such as during the development of adversary profiles in the threat assessment or design basis threat (DBT), or when creating scenarios to be used to test nuclear security measures as part of an evaluation process for the nuclear security system.

2.11. A passive insider adversary assists another adversary by providing information to be used in performing a malicious act. A passive insider adversary

would not participate in the malicious act in any other way and would likely cease involvement if there was a high probablility of being identified.

2.12. An active, non-violent insider adversary uses stealth or deceit to facilitate or conduct a malicious act and may provide information to another adversary. For example, an active, non-violent insider adversary may attempt an abrupt or protracted theft of nuclear material or may assist external adversaries in performing a malicious act by disabling or ignoring alarms or by opening doors. It is likely that an active, non-violent insider adversary would terminate the malicious act if there was a high probability of being identified (i.e. this type of insider adversary might risk being detected but would likely not risk being identified).

2.13. An active, violent insider adversary is similar to an active, non-violent insider adversary but is also willing to use physical force against personnel to facilitate or conduct a malicious act. Depending on the circumstances, an insider adversary may move from non-violent to violent.

IDENTIFICATION OF POTENTIAL INSIDER THREATS

2.14. The guidance contained in this section may be useful for the operator in identifying potential insider threats and should be used in conjunction with other insider threat identification processes, such as developing plausible scenarios as part of an evaluation of the nuclear security system.

2.15. Reference [2] recommends that "The appropriate State authorities, using various credible information sources, should define the *threat* and associated capabilities in the form of a *threat assessment* and, if appropriate, a *design basis threat*."[3] A State should consider the attributes, motivations and categories of insiders and describe any credible insider threats in the national threat assessment or DBT.

2.16. A threat and risk assessment may also help identify potential insider threats. In addition to the general information about insider threats contained in the national threat assessment or DBT, local threat information from the area around a particular facility should be considered in the facility specific assessment. This information may highlight relevant conditions (e.g. crime levels) or situations

[3] The DBT refers to the "attributes and characteristics of potential *insider* and/or external adversaries, who might attempt *unauthorized removal* or *sabotage*, against which a *physical protection system* is designed and evaluated" [2].

outside the facility (e.g. general attitude of the community, presence of organized hostile groups) that may be favourable to insider adversaries.

2.17. Potential insider threats may also be identified by determining which insiders have remote or on-site authorized access to facility systems through computer networks. Modern facility systems, including those that contribute to nuclear security, rely on computer based controls and networks. These systems should be protected against computer based attacks as described in Ref. [7]. Personnel with access to these systems should be considered when identifying insider threats.

3. TARGET IDENTIFICATION

3.1. Target identification, as described in Ref. [15], determines which material and equipment needs to be protected from an adversary. Targets may include nuclear material, associated areas, buildings, equipment, components, information, systems and functions. Guidance on target identification for facilities and for nuclear and radioactive material is provided in Refs [2–4, 8, 15, 16].

3.2. Assets (e.g. surveillance systems, portal monitors) that are not themselves identified as targets but are critical for the protection of identified targets may also require protection. An insider adversary could bypass or compromise these assets to conduct a malicious act.

TARGETS FOR UNAUTHORIZED REMOVAL

3.3. Nuclear material targets for unauthorized removal can be assigned to one of three categories (I–III) according to the relative attractiveness and characteristics of the nuclear material as well as the potential consequences if it were used in a nuclear explosive device. This categorization is defined in table 1 of Ref. [2]. The unauthorized removal of nuclear or radioactive material for the construction of a radiological dispersal device should also be considered [3]. In addition to nuclear and other radioactive material, theft targets may include sensitive information and sensitive information assets.

3.4. The identification of potential targets for unauthorized removal of nuclear material by an insider adversary should take into account the possibility of both abrupt and protracted theft. ‘Abrupt theft’ is the unauthorized removal of a target

or a significant quantity of nuclear material during a single act. 'Protracted theft' is the repeated unauthorized removal of potentially small quantities of nuclear material from either a single location or multiple locations.

3.5. An insider adversary might use protracted theft of nuclear material to remain undetected by repeatedly removing small quantities of material that are within the detection limits of NMAC and physical protection systems. Protracted theft may be accomplished either by removing the nuclear material from the facility with each acquisition or by accumulating the nuclear material in a hidden location for later, possibly abrupt, removal from the facility. The possibility that an insider adversary could collect an amount of nuclear material equivalent to a higher category by collecting sufficient amounts of lower category nuclear material should be considered during target identification. Factors such as the element, the physical form of the material, how it is used, the quantity that is used during processing and the amount stored should also be considered during target identification when determining if protracted theft scenarios are possible and credible. Similar considerations should be made for abrupt theft scenarios as well.

SABOTAGE TARGETS

3.6. Sabotage targets in a facility are determined by analysing the potential for the facility's radioactive material inventory and waste, including nuclear material and radioactive sources [3], to result in unacceptable radiological consequences or high radiological consequences. Further details regarding nuclear security measures that should be taken to protect against sabotage as well as to perform an analysis of sabotage targets can be found in Refs [2, 15].

3.7. The identification of possible combinations of actions (scenarios) an insider adversary might take to degrade facility structures, systems and components that may result in unacceptable radiological consequences or high radiological consequences should be part of the target identification process.

IDENTIFICATION OF SYSTEMS THAT CONTRIBUTE TO NUCLEAR SECURITY

3.8. A target identification process should consider all systems that could require additional protection from insider threats. Physical protection systems, NMAC systems and safety and process control systems should be considered as potential targets for malicious acts, including those initiated by an insider adversary.

3.9. An insider adversary may have authorized access to the facility or to information about the facility and might attack other structures, systems or components to indirectly perpetrate an attack, mask malicious acts or aid an external adversary. Depending on the facility or operation, computer based systems may be exploited by the insider adversary (e.g. office networks or communication computers might be used to acquire sensitive information).

3.10. The compromise of computer based systems in a facility could adversely affect safety, the security of nuclear material or accident mitigation. The operator should evaluate and protect computer based systems that contain information related to safety or security in accordance with the risk and the potential consequences of the release of this information. This evaluation should aim to identify critical computer based systems that may be the most vulnerable to a malicious act and whose failure could result in a nuclear security event.

3.11. The operator should consider providing additional training to employees and contractors with access to sensitive systems to raise security awareness. External adversaries may target insiders with access to a facility, sensitive information, sensitive information assets or the facility's networks to gain assistance in facilitating or masking malicious activities.

4. MEASURES AGAINST POTENTIAL INSIDER THREATS

4.1. Nuclear security measures used to protect against insider threats should include both preventive and protective measures. The term 'preventive measures' refers to measures used to reduce the number of potential insiders before individuals are granted access, to minimize opportunities for an insider to undertake a malicious act if access is granted or to prevent a potential insider adversary from carrying out a malicious act. The term 'protective measures' refers to measures used to detect or delay malicious acts, respond to malicious acts or mitigate the consequences of a malicious act.

4.2. This guidance does not include all measures that could be used against an insider threat. However, the use of preventive and protective measures can help counter insider threats if the threat is properly defined, the target identification process is thorough and the measures are effectively implemented and evaluated.

4.3. Information regarding measures used against insider threats and incidents involving malicious acts by insider adversaries should be collected by competent authorities to analyse trends, weaknesses and good practices. If appropriate, the information should be shared with authorized international agencies to better understand the scope and nature of the security challenge posed by insider adversaries.

GENERAL APPROACH TO IMPLEMENTATION

4.4. As stated in Ref. [2], nuclear security requirements should be based on a graded approach, taking into account the current evaluation of the threat, the relative attractiveness and nature of the material, and the potential consequences associated with unauthorized removal of nuclear material or sabotage of nuclear material or nuclear facilities. General guidance on the implementation of a graded approach to protect nuclear materials and facilities against insider and external threats can be found in Ref. [15].

4.5. Implementing nuclear security measures to protect against insider threats involves selecting a combination of preventive and protective measures[4] and implementing them in accordance with a graded approach. It is important that the measures selected be implemented and evaluated effectively so that they perform as desired. Not all measures are appropriate for every facility or operation.

4.6. Layers of preventive and protective measures should be implemented in accordance with the concept of defence in depth, such that insider adversaries would need to overcome or circumvent multiple layers of measures or technologies to achieve their objectives. These layers may consist of administrative measures (e.g. procedures, instructions, access control rules, confidentiality rules), technical measures or a combination of both. Both types of measure should integrate people and equipment.

4.7. The operator should prepare a security plan as part of its application to obtain a licence, as described in Ref. [2], and ensure that it describes the measures needed to address insider threats, including measures that address insider threats to information and computer security (e.g. a cyber-attack conducted by an insider adversary [7, 8]). The operator should consider insider threats during the design, evaluation, implementation and maintenance of nuclear security systems at the facility level.

[4] Some measures may have both preventive and protective effects.

4.8. The security plan should define how nuclear security systems are implemented at the facility and identify the measures used to protect identified targets from insider threats. The plan should include information about these measures. For example, technical measures might include containment and surveillance measures intended to detect and delay an insider adversary, measures to monitor and harden networks and associated devices, and measures to enforce access control. Administrative measures might include procedures, instructions, administrative sanctions, the two person rule, confidentiality rules and administrative checks, as well as planned, unplanned or unannounced inspections of the implementation of preventive and protective measures. Inspections should be performed by the operator or by independent teams. The security plan should specify how the measures will be evaluated (see Section 5).

4.9. Security systems at existing operating facilities may need to be upgraded to respond to evolving insider threats.

IMPLEMENTING MEASURES AGAINST INSIDER THREATS

4.10. Preventive and protective measures should both be used to protect against potential insider threats. Preventive measures can be used as follows:

(a) To reduce potential insider threats before allowing individuals access by identifying undesirable behaviours or characteristics that may indicate motivation;
(b) To further reduce potential insider threats after insiders have gained access by identifying undesirable behaviours or characteristics that may indicate motivation;
(c) To minimize opportunities for malicious acts by limiting access, authority and knowledge of insiders.

Protective measures can be used as follows:

(1) To detect, delay and respond to malicious acts;
(2) To mitigate or minimize the consequences of a nuclear security event and, if necessary, locate or recover the material.

Figure 1 illustrates how these steps may be used to address insider threats.

4.11. Many of the measures listed in the two sections that follow can be considered as both preventive and protective. As part of the selection and evaluation process,

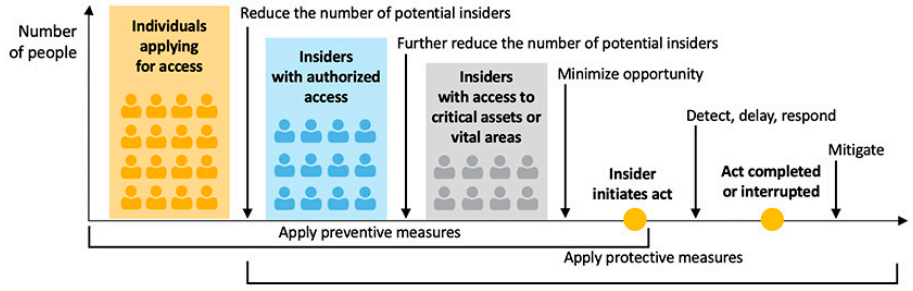


FIG. 1. Steps for using preventive and protective measures against potential insider threats.

the potential value of each proposed measure for both protection and prevention should be considered.

Implementing preventive measures

4.12. The goal of preventive measures is to reduce the number of potential insider threats and to minimize the opportunity for insiders to perform a malicious act. Preventive measures should be applied before employment, during employment and upon termination. In addition, preventive measures include quality assurance and specific computer security measures. Operators should apply the preventive measures described in this section.

Measures to be applied before employment

4.13. Individuals applying for work that requires access to a facility should be subject to identity verification, personal document verification and trustworthiness assessments.

4.14. Identity verification is used to confirm that the personal details of the individual in question are correct and genuine.

4.15. Personal document verification is used to authenticate the details of an applicant's work history, educational background and possession of the skill set required for the work to be performed. Verification and validation of documents and qualifications may be accomplished by contacting prior employers, educational institutions and references.

4.16. Trustworthiness assessments are used to provide an initial assessment (during the hiring process) and ongoing assessments (periodically throughout

the employment period) of an individual's integrity, honesty and reliability. As recommended in Ref. [2]:

> "Taking into consideration State laws, regulations, or policies regarding personal privacy and job requirements, the State should determine the trustworthiness policy intended to identify the circumstances in which a trustworthiness determination is required and how it is made, using a *graded approach*."

4.17. The assessments should review the individual's observance of the law and adherence to facility rules, as well as any behaviours or motivational factors of concern. For example, the assessment should seek to identify motivational factors such as financial problems or pressures (e.g. debts, wage cuts), adherence to an ideology of concern, desire for revenge (e.g. a perceived injustice against the individual), physical dependency (e.g. drugs, alcohol, sex), psychological or psychiatric conditions, severe dissatisfaction with private or professional life, or other factors owing to which an individual could be coerced to commit a malicious act. These motivational factors may be identified by a review of information such as criminal records, personal and professional references, past work history, financial records, on-line and other social networks, medical records or job performance reports, as well as information from colleagues about observed behaviour.

4.18. National laws might restrict the scope or conduct of identity verification, personal document verification and trustworthiness assessments in a State.

Measures to be applied during employment

4.19. Insiders who have passed the pre-employment checks and have been granted authorized access, including access to critical assets, sensitive information and vital areas, should be subject to the measures described in the following paragraphs.

4.20. Escorting procedures should be developed and implemented. Persons whose trustworthiness has not been determined or whose duties do not require a trustworthiness assessment (e.g. temporary repair staff, administrative staff, maintenance staff, construction workers, visitors) should be escorted into vital areas or inner areas by persons who have authorized access and are not required to be themselves escorted. The escort should be knowledgeable about approved actions, including which areas and systems the escorted individual should be allowed access to and which activities he or she is authorized to perform.

4.21. Periodic reassessment of the trustworthiness of insiders should be conducted during employment. Certain behaviours and motivational factors of concern may not have previously been apparent or may develop over time. For example, random testing for drug or alcohol use during a work shift should be considered as a way to ensure a worker is reliable. The extent of the trustworthiness checks should be graded according to the level of access and authority the insider has to the facility and its assets. For example, insiders who perform network administration, who facilitate remote access to sensitive information assets and who work with nuclear material should be subject to more frequent and thorough trustworthiness checks than those who work in human resources.

4.22. Employees whose trustworthiness assessment has changed owing to personal circumstances might have their level of access temporarily demoted or they might be removed from management responsibilities until they are assessed again. Security awareness programmes and employee satisfaction and rewards, discussed below, may be used to maintain the trustworthiness of employees.

4.23. Sensitive information should be kept confidential so that only those who need to know the information are permitted to access it. Acquiring information on sensitive targets or regarding security procedures or measures (e.g. the location of the nuclear material inventory or transportation plans and schedules) might help insider adversaries successfully perform a malicious act. A record of persons accessing sensitive information, including the date and time at which the information was accessed, should be maintained and should also be protected against modification. Information addressing potential vulnerabilities in nuclear security systems should be highly protected and compartmentalized (as described in para. 4.30), since this information could facilitate a subsequent unauthorized removal or act of sabotage.

4.24. Access to nuclear facilities, nuclear material, nuclear facility systems and sensitive information should be controlled. A documented process for authorizing and revoking such access should be established and implemented. This process should apply to anyone who requires either remote or on-site access to a facility or its operations, including transportation. An individual's personal details could be verified through government issued identification documents and biometrics (e.g. retina, palm prints, finger prints, facial recognition). The process should apply strict need-to-know and need-to-access rules, as defined by the competent authority. Individuals should be permitted unescorted access only to the areas that they need to enter to complete assigned work. The number of persons with authorized access to designated areas should be kept to the minimum necessary.

4.25. The processing or movement of nuclear and other radioactive material should be authorized before processing or movement to minimize opportunities for the unauthorized removal of material and to detect unauthorized activities [6, 13]. For example, the facility operator should have a written procedure that specifies who can remove nuclear material from a storage vault for use in processing, when it can be removed and how the removal should be authorized and recorded. A daily or weekly schedule of activities coordinated and approved by operations staff may reduce opportunities for unauthorized activities by personnel who normally perform those activities.

4.26. Physical areas, duties, time and information should be compartmentalized so that one insider is unlikely to have sufficient access, authority or knowledge to complete a malicious act. Compartmentalization increases the effort that an insider would need to expend to complete a malicious act and increases the likelihood that an insider would need to exceed his or her normal authorized activities to complete a malicious act.

4.27. The facility operator should seek to ensure that physical areas are compartmentalized such that a single insider does not have access to all the systems, components and equipment that would enable him or her to complete a malicious act. The number of individuals with access to any area requiring protection should be limited. Rules should be defined to establish which personnel have a need to access compartmentalized areas; these rules should be applied to each compartmentalized area. These rules should be reviewed and changed when processes or configurations within the compartmentalized area are changed. Additionally, the number of persons permitted access to each of the compartmentalized areas should be strictly limited. Inspections and performance tests should be performed to ensure procedural adherence to the access rules.

4.28. Separation of duties compartmentalizes the work activities of insiders to limit an insider's ability to obtain sufficient authorized access, authority or knowledge to conduct a malicious act. Separation of duties includes applying the principle of least privilege to computer based systems, through which an insider is assigned only those privileges that are essential to his or her work.

4.29. Time should be compartmentalized by limiting authorized access during different periods of activity in a facility (e.g. working hours, maintenance, outages, non-routine conditions). For example, an insider's access to a critical area should be limited to his or her shifts.

4.30. Information should be compartmentalized by dividing information stored both in hard copy and electronically into separately controlled pieces and using administrative and technical measures to control access to the information. The purpose of compartmentalizing information is to prevent insiders from collecting all the information necessary to attempt a malicious act. Personnel need-to-know rules for sensitive information should be used when compartmentalizing information.

4.31. Standard operating procedures should be adhered to. Standard operating procedures are written instructions that govern recurring tasks according to approved specifications in order to produce a specified outcome. Standard operating procedures minimize variation and promote quality assurance through the consistent implementation of a process within an organization regardless of personnel changes. Standard operating procedures can assist in detecting, and thus preventing, an insider adversary's malicious act because they provide a baseline of predetermined activities from which deviations in procedure can be more readily detected and challenged by others.

4.32. A security awareness programme for staff and contractors should be developed and implemented. Such a programme contributes to the organization's nuclear security culture and can help prevent insider threats if security awareness of such threats is integrated into the facility's nuclear security culture. All personnel, regardless of job title or function, should be aware of the threats and potential consequences of malicious acts and their role in reducing the risk of a malicious act. Security awareness programmes may reduce the risk of blackmail, coercion, extortion or other threats to employees and their families, and should encourage the reporting of potential intimidation to the security management. 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.

4.33. The security awareness programme should include clear security policies, the enforcement of security practices and continuous training. The purpose of training is to establish an environment in which all employees are aware of security policies and procedures so that they are able to aid in detecting and reporting suspicious or erroneous behaviour as well as unauthorized acts. Training should include methods to evaluate security awareness and training effectiveness as well as processes for continuous improvement or retraining. In addition to preparing personnel for the possibility of a physical incident at the facility or against its assets, the training should prepare personnel for the possibility of a cyber-attack.

4.34. A fitness for duty programme should be developed and implemented. Managers should be trained to identify concerns about an employee's behaviour and report them to the appropriate person. Fitness for duty programmes may be considered in order to monitor employees' health on a periodic basis. The facility operator may also consider offering assistance to employees who are in challenging situations (e.g. financial, medical, psychological).

4.35. Incidents of security concern (i.e. incidents at a facility that involve violations or irregularities associated with facility security policies, procedures or systems) should be reported and investigated. The reporting and investigation of incidents of security concern can help facilities develop corrective actions and prevent insider threats. An incident may be caused by an insider adversary as a precursor to a malicious act, either to prepare for the act or to test the response of a system. Thoroughly investigating these incidents might act as a deterrent to insiders and could identify personnel who might be insider adversaries.

4.36. Employees should be provided with good working conditions, rewards and recognition. Good working conditions, rewards and recognition are an important part of maintaining and increasing employee morale and loyalty, which contributes to an effective security culture.

4.37. Insiders should be made aware that deliberate violations of work instructions, regulations or laws will be sanctioned. The chance of disciplinary action or legal prosecution might deter insiders from committing malicious acts. In addition, requiring operators to inform the competent authority of attempted or completed malicious acts may provide, after proper evaluation, a basis for information sharing among operators as well as a source of needed modifications to regulatory requirements.

Measures to be applied upon termination

4.38. An individual's access and authority, including computer access, should be cancelled upon termination of the individual's position, employment or contract. Termination procedures should be established and should include revoking physical access to the facility; using a non-disclosure agreement to protect sensitive information; and changing encryption keys, passwords and access codes.

Quality assurance policy and programmes

4.39. The facility's quality assurance policy and programmes for nuclear security should address insider threats, as described in the threat assessment or DBT. As stated in para. 3.52 of Ref. [2]:

> "The quality assurance policy and programmes for physical protection should ensure that a *physical protection system* is designed, implemented, operated and maintained in a condition capable of effectively responding to the *threat assessment* or *design basis threat* and that it meets the State's regulations, including its prescriptive and/or performance based requirements."

4.40. The quality assurance programmes should include all facility systems that contribute to nuclear security to ensure adequate protection against insider threats. Quality assurance should require configuration management of the nuclear security systems to ensure that they continue to meet the desired performance criteria of these systems and to understand any potential consequences when changes are made to the systems, for example by an insider.

Measures for computer based systems

4.41. While certain measures, such as escorting, may be effective in limiting insider access to nuclear and radioactive material, they do not provide sufficient protection against potential insider threats to computer and network systems; such protection may be provided by information security measures [7, 8]. For example, third parties and vendors may have physical access on the site to sensitive information and assets during the development and maintenance of computer and network systems. While these third parties and vendors may wish to maintain remote access during all of the life cycle stages of the computer and network systems, such access should only be granted in accordance with the risk informed approach [1].

4.42. The facility operator should define and implement a policy addressing the acceptable use of computer based systems. This policy may define the approved use of computer based systems, outline employer expectations for monitoring approved use of these systems, provide for training and explicitly identify prohibited actions on computing systems. The facility operator should also consider the use of technical measures to enforce or enhance the systems policy. For example, the facility operator might define a social media policy and provide computer based training on the use of social media to reduce the likelihood of adversaries using employees as unwitting insiders.

Implementing protective measures

4.43. The purpose of protective measures against insider threats is to detect, delay and respond to a malicious act after it has been initiated and may include mitigation of consequences and recovery of nuclear or radioactive material. When designing and implementing protective measures, efforts should be made to ensure that these measures are supportive of and do not have an adverse effect on facility operations and safety. In case of conflict, particularly with safety, a solution should be reached in which the overall risk to the workers and the public is minimized and sufficient security is maintained.

4.44. Protective measures against insider threats should be applied using a graded approach for identified targets. In addition to protecting against unauthorized removal, as stated in para. 5.12 of Ref. [2], "The *operator* should design a *physical protection system* that is effective against the defined *sabotage* scenarios and complies with the required level of protection for the *nuclear facility* and *nuclear material*." Sabotage scenarios should include scenarios involving one or more insider adversaries. The following sections address protective measures against insider threats that should be considered during the design of a nuclear security system.

Detection measures

4.45. The detection of malicious acts attempted by external adversaries focuses on detecting the penetration of any one of a facility's protective measures. By contrast, insiders could bypass or defeat certain physical protection and NMAC measures owing to their authorized access, authority and knowledge. Operators should implement multiple and diverse protective measures for these systems to detect potential malicious acts performed by an insider and to provide the information needed for investigation and analysis. The facility operator should investigate all of the information provided by these detection measures in a comprehensive manner. Individual signals that seem insignificant might produce an indication of a malicious act when examined together.

4.46. An investigation might include reviewing recorded footage and network monitoring data, verifying tamper indicating devices or measurement data associated with nuclear materials, inspecting access logs or performing an emergency inventory. The personnel performing the investigation and analysis of the possible malicious act should be qualified. The time required to perform the investigation and analysis following detection directly affects the facility operator's ability to respond to a malicious act in a timely manner.

4.47. Suspicious or unauthorized activities should be detected and investigated because they might indicate that a malicious act is in the exploratory or preparatory phase. For example, an insider might attempt to bypass procedures (e.g. bringing prohibited items into an area), attempt to access an area that he or she is not authorized to access (e.g. entering through an emergency door), trigger an alarm to observe the timing and nature of the response, or attempt to obtain sensitive or otherwise need-to-know information to which the insider has not been granted access.

4.48. Protective measures to detect insider threats need to be designed to identify, correctly assess and report suspicious or malicious acts. Facility detection measures implemented against insider threats typically include measures related to access control, personnel tracking, detection of prohibited items, surveillance, NMAC systems and computer security. These types of measure are discussed in the following sections.

Access control

4.49. The operator should establish and document strict access control rules and procedures applicable to nuclear material, equipment used for processing or handling nuclear material, and data about nuclear material or systems relevant to safety or security. The robust implementation of access control rules and procedures minimizes insiders' access to material, systems and equipment. Access control rules and procedures may also act as a deterrent owing to the possibility of detection or identification if an insider attempts to access material, equipment or data for which he or she is not authorized.

4.50. Access control rules and procedures should be applicable to a variety of situations, including authorizing access to areas containing nuclear material and controlling nuclear material in routine and non-routine conditions, such as during actual or simulated emergency situations. For example, access control rules could apply to controlling and disseminating key and lock combinations in manual access control systems and to printing badges, enrolling personal identification numbers, gathering biometrics and controlling locks in electronic systems.

4.51. The operator should protect from unauthorized access (a) equipment that generates badges, (b) support equipment and associated spare parts and (c) systems used to grant access permissions. The facility operator should strictly control access to security equipment or equipment that contributes to security, calibration and maintenance. The operator should also establish procedures to ensure that this equipment remains intact. For example, to ensure that it has

not been tampered with, equipment should be subject to testing by authorized personnel after maintenance has been performed and before the equipment is returned to service.

4.52. Access control rules should be defined for visitors and escorts and for abnormal conditions, such as response to emergencies and system outages.

4.53. Specific criteria, such as a personnel need-to-know and trustworthiness determination, should be verified before authorizing access to any area to which access is controlled. Establishment of rules for access control should be coordinated with NMAC, operations, safety and physical protection organizations.

4.54. Each access or attempted access to sensitive physical locations and computer systems should be recorded in access control records. Malicious acts committed by insider adversaries may be identified in the course of monitoring or inspecting these access control records. For example, inspections of access control records may identify events such as an unscheduled storage vault access, each failed personal identification number entry attempt, failed biometric authentification for an authorized badge or other indications of entry attempts by unauthorized individuals. Once identified, the irregularity or suspicious activity can be assessed as a potential malicious act. Detection measures and associated procedures used to monitor and inspect access control records should be considered as technical and administrative measures for access control during system design or upgrade.

4.55. Access control records should also be maintained of all persons who access vital areas or who have access to, or are in possession of, keys, key cards and other credentials relevant for accessing other systems, including computer systems that control access to inner areas, vital areas and other areas containing nuclear material [2].

4.56. If appropriately documented, access control records can be used during the investigation of a malicious act to determine a list of possible suspects. Requests for authorized access to security areas or systems relevant to safety or security, whether approved or denied, should also be reviewed and inspected to identify potential malicious activity.

Personnel tracking

4.57. Tracking the movement and location of personnel within a facility enables the operator to detect an attempted or actual violation of access control rules, such as multiple people exiting the facility using a single access control badge.

Existing technology makes it possible to track individuals either in real time or after the fact by recording the locations and areas they visit each day, along with the corresponding time and duration of each visit.

4.58. Awareness that a facility has a tracking system may deter insiders from carrying out unauthorized activities. Further, tracking records and access control records may be used during the investigation of a malicious act for assessment purposes or after an incident to generate an initial list of suspects.

Detection of prohibited items

4.59. As recommended in para. 4.43 of Ref. [2]:

> "Vehicles, persons and packages should be subject to search on entering both the *protected* and *inner areas* for *detection* and prevention of unauthorized access and of introduction of prohibited items. Vehicles, persons and packages leaving the *inner area* should be subject to search for *detection* and prevention of *unauthorized removal*."

4.60. The operator should identify and document prohibited items for limited areas, protected areas, inner areas and vital areas. Prohibited items may include unauthorized tools and material, such as computers, cell phones, tablets and other media or information technology devices with cameras; radiation shielding material; weapons; or explosives. These items could be used to gain access or cause damage to sensitive systems or equipment, or their components, or to enable the unauthorized removal or sabotage of nuclear material. Other prohibited items may be specifically identified by a facility to protect its physical protection, NMAC, safety and operational systems or to protect information against insider adversaries.

4.61. The operator should immediately investigate the detection of prohibited items entering or exiting an area as a potential malicious act performed by an insider. When preparing to perform a malicious act, an insider adversary might test the prohibited item detection system to ascertain the sensitivity of detectors or the strength of assessment procedures. Suspicious or repeated detections of prohibited items should be identified, assessed, reported and investigated.

4.62. Measures for the detection of prohibited items include manual searches of personnel, packages and vehicles (both periodic and random); use of metal detectors, X ray machines and radiation detectors; and use of dogs or other types of detector for chemicals and explosives. These measures should take into account

the specifics of the facility and the threats against which protection is required according to the threat assessment or DBT, if applicable.

4.63. The operator should develop and implement policies identifying prohibited items and associated search and detection procedures. Personnel performing searches or using equipment to detect prohibited items should be trained to use the equipment and appropriately respond after identifying a prohibited item. Responses may include confirming an authorized exception, detaining the potential insider adversary or recording the event for the purpose of detecting potential malicious acts at a later date.

4.64. The stringency of searches and the determination of locations where they will be carried out should be commensurate with the sensitivity of the area where the search was triggered and the proximity of the area to the target. Searches should be carried out near the areas where the search was triggered. Periodic and random searches should be used to further deter the unauthorized removal or sabotage of nuclear and radioactive material. Searches should also be performed during emergency evacuation conditions, including exercises.

4.65. Monitoring procedures should be implemented during the detailed search of a transport vehicle before loading and shipment to ensure that those persons carrying out the search are not able to introduce prohibited items that would aid a malicious act.

4.66. Fixed or handheld radiation detectors should be used to detect the unauthorized removal of nuclear material on persons, in packages or in vehicles entering and leaving protected, inner and vital areas. Metal detectors should be placed in tandem with radiation detectors at pedestrian entrances and exits to enhance the effectiveness of the radiation detection, since shielding material might be used to block radioactive signatures from being detected if nuclear material is removed from the facility.

4.67. Procedures for approving exceptions to the introduction of prohibited or controlled items (e.g. radioactive calibration sources) into the facility should be specifically established [3].

Surveillance

4.68. Surveillance measures can be used to continuously monitor the activities of individuals inside the designated areas of the facility where a malicious act could occur so that unauthorized activities are identified, reported and assessed.

4.69. Surveillance includes visual observation, monitoring of live video footage or review of recorded footage gathered by automated surveillance systems. Surveillance can be useful not only as a detection measure but also for the deterrence and investigation of potential malicious acts performed by an insider.

4.70. Personnel performing surveillance activities should be capable of detecting authorized and unauthorized actions and should have the means to rapidly and safely report the observation of any unauthorized activity.

4.71. In the event of a reported unauthorized activity, recorded surveillance footage can be used to provide a correct assessment of a malicious act or identify possible suspects. Timely assessment of malicious acts may be difficult without surveillance information.

4.72. As recommended in para. 4.48 of Ref. [2], "whenever an *inner area* is occupied, *detection* of unauthorized action should be achieved by constant surveillance (e.g. the *two person rule*)." Surveillance measures should be considered for use during operations such as maintenance and particularly during packing, shipping and transfer operations [14]. Surveillance can be provided through co-workers, managers, automated surveillance systems or a combination thereof.

4.73. Periodic checks should be established and implemented by the operator to confirm that material control or other protective measures are applied according to the established procedures and that equipment is used correctly.

4.74. When the two person rule is the selected surveillance method in an area (e.g. in an area containing Category I material), the two authorized, knowledgeable persons should be physically located where they have an unobstructed view of each other and the nuclear material. Furthermore, each person should be trained and technically qualified to detect unauthorized activities or incorrect procedures. For visual surveillance to be effective, the persons observing need to be capable of recognizing unauthorized activities, correctly assessing the situation and reporting the activities to appropriate response personnel in time for them to prevent unauthorized removal. If the two person rule is applied in such surveillance, the two authorized individuals will both need to have appropriate training, have unobstructed views of the material and of each other, and be able to detect unauthorized or incorrect procedures [1].

4.75. In addition, the two person rule is only effective when the individuals do not become complacent, for example through long term friendship or association.

Whenever possible, managers should ensure that the members of each two person team are rotated. Enforcing the two person rule for access to designated areas may deter insider adversaries and assist with timely detection. In addition, the two person rule can help protect against insider adversaries tampering with physical protection systems. Attempts to defeat the two person rule should be reported and investigated.

Nuclear material accounting and control systems

4.76. The contribution of NMAC systems to nuclear security mainly derives from their ability to maintain precise knowledge of the types, quantities and locations of nuclear material at the facility; to conduct efficient physical inventory of the nuclear material; and, in some cases, to ensure that the activities performed in connection with the nuclear material have been properly authorized [9]. There are multiple measures through which an NMAC system can assist in detecting insider threats. These measures are described in more detail in Ref. [9].

4.77. NMAC and other detection measures should also be rigorously applied to prevent the unauthorized removal of additional nuclear material from a facility by, or with the assistance of, an insider adversary while an authorized shipment is in process. Other detection measures can include the use of (a) the two person rule during movement preparation, (b) material measurements, (c) tamper indicating devices, (d) document checks, (e) radiation monitors and (f) standard operating procedures.

Detection measures for computer based systems

4.78. Technical measures involving both hardware and software should be used to detect malicious acts. These measures may involve the following example activities:

(a) Establishing a baseline for and characterization of the network traffic of sensitive computer assets, and inspecting to the baseline.
(b) Implementing software intrusion detection tools to detect abnormal patterns of user behaviour.
(c) Monitoring, inspecting and assessing computer based systems to test for insider compliance with policies and procedures and to detect suspicious actions. For example, the operator might establish false targets and monitor them to detect attempts to gain unauthorized access to sensitive information, thus revealing a potential insider adversary while ensuring that no sensitive data are exposed.

(d) Restricting potential pathways that could be used to access data so that only authorized personnel are permitted to use those pathways, and ensuring that the pathways are controlled and monitored to protect against malicious use. This could include monitoring, physically blocking, prohibiting the use of removable media and mobile devices to limit access to sensitive systems by an insider, or using computer security zones to isolate nuclear security systems and their networks from other facility networks [7].

Delay measures

4.79. Multiple layers of different physical protection or procedural measures, including compartmentalization and separation of duties, can complicate the progress of an insider adversary by requiring a variety of tools and skills, thus providing additional time and opportunity for detection. By delaying the malicious act in this manner, an insider adversary could be detected and defeated. Delay may also deter insiders from attempting malicious acts.

4.80. Measures implemented close to equipment or nuclear material (e.g. tie-downs, restraints, locks) can be effective delay measures against insider adversaries when an area is under continuous surveillance or when other appropriate detection measures are in place. Such delay measures should be designed so that it is difficult for an insider adversary to use them to delay the response to a malicious act, particularly an act of sabotage.

4.81. Keeping nuclear material in a secure location can increase the delay for an insider adversary attempting to complete a malicious act. During production or usage, the minimum amount of nuclear material needed for production or usage should be removed from locked storage at one time, and measures should be taken to control the nuclear material between process steps. When material cannot be moved to a secure storage location during non-working hours, additional physical protection and surveillance measures should be implemented until the material is properly returned and stored in a normal secure location.

4.82. Certain types of delay measure may force insider adversaries to use more sophisticated tools, resources, logistics, training and skills to defeat the measure. Those sophisticated resources may not be available at the facility and may need to be introduced into the facility by the insider adversary or learned elsewhere.

4.83. System safety designs that provide for system self-protection (e.g. backup equipment, automatic equipment shutdown, automatic valve closure) may force the insider adversary to defeat multiple, redundant and dispersed equipment and

systems. These features may delay a malicious act and prevent it from being successfully carried out. To the extent possible, access to information about the system safety designs should be restricted on a need-to-know basis to prevent it from being used to conduct a malicious act.

Delay measures in computer based systems

4.84. Physical security measures implemented to delay adversaries may not effectively protect computer based systems owing to the remote access to, and connectivity between, some computer based systems. For example, an insider with privileged access to sensitive computer based systems might be able to compromise physically separated assets remotely and simultaneously. Delays may also not be effective against an insider adversary who can use existing credentials to gain privileged access. Therefore, measures for computer based systems should emphasize prevention and, to a greater extent, detection and response.

4.85. The design and implementation of computer security zones and computer security levels at a facility can increase the complexity required to complete a malicious act using computer systems and provide security controls that may also increase the probability of detection [7].

Response measures

4.86. Both operations and security personnel may respond to an irregularity (e.g. an inventory difference, an opened door that should be locked). Typically, operations personnel respond to an irregularity to investigate its cause. If an irregularity is suspected to be due to a malicious act, security personnel should be notified and should respond if necessary. For example:

(a) Response to a passive insider adversary should depend on when detection occurs (when the information is obtained, when the information is passed on or when the investigation is completed).
(b) Response to an active, non-violent insider adversary should be by operations or security personnel depending on when detection occurs, since an active, non-violent insider adversary will stop a malicious act if confronted or challenged.
(c) Response to an active, violent insider adversary should be the same as for an external adversary.

4.87. Compared with an external adversary, an insider adversary is more difficult to identify and may not be easily identified as a threat anywhere within the

facility. In addition, a malicious act committed by an insider adversary might consist of several acts separated by both time and space. Therefore, unless an insider adversary is identified when a suspicious or malicious act is detected, it may be difficult to identify him or her later among the other insiders.

4.88. To enable an effective response to be made, a protracted theft needs to be detected before the insider adversary accumulates a target quantity of material on or off the site. Scenarios should account for security systems and measures in place in the building and in any possible material balance areas, as well as for specific nuclear security procedures that could be used to detect unauthorized activities involving nuclear material early enough for an effective response to be made. For facilities where protracted theft might occur, scenarios should be analysed for the likelihood of detection if material were (a) taken off the site each time a quantity of the material was stolen or (b) accumulated in the facility or inside a process area to be taken off the site at one time in an abrupt theft.

4.89. An insider adversary might perform a set of acts ultimately intended to lead to unauthorized removal or sabotage in an unexpected order or with periods of inactivity between the individual acts. For example, an insider adversary might commit a single act and then wait to see if he or she is detected. This may complicate the security response necessary to identify and apprehend the insider adversary and increase the importance of investigation. Operations specialists may be needed to assist in the investigation by analysing the abnormal or irregular event to predict what further malicious acts might be attempted.

4.90. Insiders with access to a facility should be trained in detecting malicious acts and responding so that they protect themselves and transmit alarms according to a specified set of procedures. These procedures should be documented and used as part of the security awareness training provided to facility personnel by the operator. Response procedures should be based on the assumption that someone involved in response could be an adversary. For example, an insider adversary might report a fictitious emergency to distract others and prevent them from detecting a malicious act, or an insider adversary on the response team might use an emergency exercise or create an emergency to disguise a malicious act.

Response measures in computer based systems

4.91. For computer security incidents with the potential to adversely impact systems that contribute to nuclear security, response activities should be coordinated with nuclear security response personnel and documented. For example, the detection of unauthorized changes to access control by an insider should be responded

to in a coordinated manner involving site security personnel and computer security personnel because such changes might facilitate unauthorized removal or sabotage. In the event of such a computer security incident, compensatory measures that involve site security and other appropriate facility organizations should also be considered.

COMPREHENSIVE ELEMENTS THAT REINFORCE PREVENTIVE AND PROTECTIVE MEASURES

Nuclear security culture

4.92. The foundation of nuclear security culture is the recognition that a credible threat exists and that nuclear security is important [11].

4.93. Nuclear security culture plays a key role in ensuring that individuals, organizations and institutions remain vigilant and that sustained measures are taken to counter insider threats. The effectiveness of preventive and protective measures against insider threats depends on the attitudes, behaviours and actions of individuals [17].

4.94. Management should promote a robust nuclear security culture to counter insider and external threats. The nuclear security culture creates the overall conditions for personnel to implement both preventive and protective measures. A facility's nuclear security culture should improve loyalty and adherence to security policies. For example, management should emphasize the employees' responsibility to report unusual activities or suspicious behaviour without fear of suffering disciplinary actions [11].

Contingency plans

4.95. As stated in para. 3.58 of Ref. [2]:

> "The State should establish a *contingency plan*. The State's *competent authority* should ensure that the *operator* prepares *contingency plans* to effectively counter the *threat assessment* or *design basis threat* taking actions of the *response forces* into consideration."

Paragraph 3.62 of Ref. [2] states that "The *operator* should initiate its *contingency plan* after *detection* and assessment of any *malicious act*." Paragraph 5.44 of Ref. [2] states that "The *contingency plan* should include measures which focus

on preventing further damage, on securing the *nuclear facility* and on protecting emergency equipment and personnel."

4.96. The contingency plans developed by the State and the operator should address measures to respond to both insider and external threats. Protective measures against insider threats should be coordinated with contingency plans in accordance with agreed procedures. The contingency plan should require that personnel evacuating a building during a real or simulated emergency be controlled and examined for contamination and nuclear material to protect against insider threats.

4.97. Actions taken in response to suspected or confirmed malicious acts by an insider adversary may be different from the response to a malicious act by an external adversary.

System maintenance and recovery programme

4.98. A maintenance and recovery programme for all facility nuclear security systems that need to be protected may mitigate the consequences of a malicious act by an insider adversary. The maintenance programme should include the capability to rapidly repair operational and other vital systems, to rapidly replace parts that have been damaged and to implement compensatory measures as needed. Rapid repair and replacement limit the duration of the system outage and the time available for any subsequent malicious actions and may mitigate the consequences of the insider adversary's malicious act.

4.99. Operators should consider providing protection for spare parts (e.g. by installing barriers, storing the spare parts at a distance from the installed system and frequently monitoring the storage location) so that it would be difficult for an insider adversary to destroy or compromise both the installed parts and the spare parts for vital equipment.

4.100. Facility operating procedures and procedures for the recovery of security and operational systems should be validated and exercised to help ensure the rapid recovery of these systems, as well as to protect emergency equipment and personnel.

4.101. Procedures implemented for the protection of identified equipment should include the appropriate response to outages — such as implementing compensatory measures, investigating the cause of the outage and implementing a system for rapid repair (return to service) — to protect against the possibility of an unassessed and ongoing malicious act.

4.102. Secure backup and recovery processes should be implemented for sensitive computer based systems providing operation or security functions. System files used for recovery processes should be stored in a separate area with access control.

5. EVALUATION OF MEASURES

OBJECTIVES AND OVERVIEW OF THE EVALUATION PROCESS

5.1. Evaluating the effectiveness of preventive and protective measures against insider threats is a key component of a risk assessment that is intended to identify systems vulnerable to insider threats. The evaluation should use credible threat scenarios based on the threat assessment or DBT.

5.2. The results of the evaluation should be compared with previously established criteria for the effectiveness of preventive and protective measures. These criteria are usually established by the competent authority and are based on the potential consequences of a malicious act by an insider adversary and its likelihood of success. How the operator meets these criteria should be documented in the operator's comprehensive security plan, which includes plans for protecting both the NMAC and physical protection systems.

5.3. Evaluation of the effectiveness of the preventive and protective measures should be based on the operator's security plan. If the evaluation indicates that the preventive and protective measures defined in the security plan do not meet the criteria, upgrades should be implemented and the evaluation should be repeated until the criteria are met.

5.4. In the evaluation, consideration should be given by the operator to the relative ease of performing a malicious act and the level of risk associated with the potential malicious act. For example, a malicious act may have consequences that are deemed acceptable yet be relatively easy to perform (e.g. unauthorized alteration of the detection level of a radiation portal monitor); such an act may therefore be deemed unacceptable and require corrective action. Additionally, the risk may be deemed acceptable but may be close to the threshold beyond which the risk would no longer be acceptable. For example, an insider adversary might remove from a Category III process area small amounts of nuclear material that pose little risk, but if this unauthorized removal were repeated, the total quantity

removed might reach a quantity that falls within a higher category. Such a case should not be disregarded, and prudent management practices would lead to additional protective measures.

5.5. The effectiveness of the preventive and protective measures should be re-evaluated periodically, particularly when there are changes in the threat assessment or DBT, in the preventive and protective measures or in the operating processes and conditions.

5.6. The criteria and performance requirements for an NMAC system are established in the overall context of nuclear security and can be useful in assessing the nuclear security system's effectiveness against insider threats. These criteria and performance requirements should address the different types of nuclear material and the time frames for the detection of unauthorized removal of nuclear material.

5.7. Different methods can be used to evaluate the effectiveness of the nuclear security system against insider threats (e.g. inspections and assessments, performance testing, measurement quality control, scenario analysis). Scenario analysis is an effective method of evaluation against insider threats. Performance testing supports the scenario analysis process by providing information such as the probability of detection and subsequent response. Plans for performance testing should be developed and implemented to test employee, facility and competent authority readiness for response to a potential malicious act by an insider adversary.

EVALUATION OF PREVENTIVE MEASURES

5.8. The implementation of preventive measures should be evaluated to ensure that they are implemented as designed. Although difficult to evaluate quantitatively, preventive measures can be effective in reducing the possibility of insider threats. Preventive measures should be evaluated by conducting performance testing on procedures to determine whether the procedures are adequate to address the threat and whether employees follow the procedures.

5.9. The opportunity for an insider adversary to perform a malicious act can be minimized by reducing the possibility for an insider to gain the access, authority or knowledge necessary to successfully carry out a malicious act. Credible scenarios for evaluation will incorporate the degree to which and the manner in

which opportunity is minimized. A review should be performed to identify what preventive measures are in place and whether they are properly applied.

EVALUATION OF PROTECTIVE MEASURES

5.10. The effectiveness of the measures used to detect, delay and respond to malicious acts (protective measures) can be quantitatively or qualitatively analysed. The likelihood of detection and the timeliness of response are often quantifiable and can provide a basis for an evaluation of the effectiveness of the protective measures.

5.11. One way to evaluate the effectiveness of the protective measures against insider threats is to develop credible scenarios, including scenarios of collusion with other insider adversaries or with external adversaries, as appropriate. The effectiveness of the protective measures in countering these scenarios can then be evaluated.

5.12. The development of scenarios involves identifying the combination of actions necessary for an insider adversary to accomplish a malicious act. Operators should consider pairing identified targets (see Section 3) with a defined insider adversary (see Section 2) when developing scenarios. The set of actions that an insider adversary would need to take to achieve his or her goal should be defined, taking into account the threat assessment or DBT. These sets of actions should include the actions that would be performed and the locations where they would be performed, and all of the protective measures that could be encountered by insider adversaries while performing those actions should be identified. Because insider adversaries can perform the actions required for a malicious act over an extended period, and because the acts may not follow a predictable sequence, the concept of a path or timeline may or may not be relevant to the analysis.

5.13. For sabotage scenarios, the actions that need to be taken to initiate a sequence of events that would result in unacceptable radiological consequences should be identified. Sabotage scenarios should include attacks on both single and multiple targets.

5.14. For scenarios involving the unauthorized removal of nuclear material, the actions that need to be successfully taken to remove nuclear material from the facility should be identified. Scenarios involving unauthorized removal of nuclear material should consider both protracted and abrupt theft and should include situations in which the adversary leaves the facility directly with the nuclear

material or hides material at the facility in order to remove it from the facility later under more favourable circumstances. Scenarios should consider attacks on, or the compromise of, computer based systems, combinations of physical attacks and cyber-attacks, and attacks by violent and non-violent insider adversaries.

5.15. Strategies that may be used by insider adversaries to defeat protective measures should also be considered as part of the scenario development process. The operator can develop such strategies by considering how access, authority and knowledge could enable an insider adversary to thwart the detection and delay measures. Possible efforts by insider adversaries to reduce the effectiveness of the response should also be considered. Emergency conditions that result in a facility evacuation may create opportunities for an insider adversary to complete a malicious act and should be considered during scenario development.

5.16. Once detailed scenarios involving insider threats have been developed, the effectiveness of the protective measures can be evaluated by considering the accumulated impact of detection and delay, as well as the response to and mitigation of the consequences of the scenario. For an active, non-violent insider adversary, the effectiveness of the response will depend on the probability of interrupting or neutralizing[5] a malicious act.

5.17. The evaluation process should be repeated for credible scenarios that require further analysis. Conclusions about the effectiveness of protective measures should be based on the results of all the evaluations conducted.

EVALUATION OF MEASURES AGAINST COLLUSION BETWEEN INSIDERS

5.18. The development of sufficient scenarios addressing collusion between two or more insider adversaries is challenging owing to the many combinations of insiders with different access, authority and knowledge that need to be considered. Evaluation of the effectiveness of the measures that help prevent collusion (e.g. compartmentalization, surveillance, preventive measures) may provide a good approach.

[5] 'Interruption' means the response occurs in time to prevent the completion of a malicious act. For an active, violent insider adversary, 'neutralization' means that the response force stops or prevents the attack permanently. For an active, non-violent insider adversary, neutralization occurs when the insider adversary is identified.

EVALUATION OF MEASURES AGAINST PROTRACTED THEFT

5.19. The evaluation of measures against protracted theft may be approached in the same manner as the evaluation of measures against abrupt theft. However, the evaluation of measures against protracted theft should also take into account additional challenges encountered by the insider adversary when attempting the unauthorized removal of small amounts of material over an extended period of time. These complexities include periodic inventory taking, the potential for inventory differences to be detected, record tracking, concealment of the amounts of material accumulated and defeat of radiation portal monitors. The evaluation method should also consider the increased probability of detection when the same action is repeated multiple times.

EVALUATION OF MEASURES AGAINST SABOTAGE

5.20. The evaluation of measures against sabotage by an insider adversary may use the same process as the evaluation of measures against abrupt and protracted theft and may reference the logic model approach (fault tree or event tree) provided in Ref. [16].

5.21. Sabotage scenarios to be evaluated should include scenarios for both direct sabotage of nuclear material and indirect sabotage (i.e. sabotage of facility systems) that could result in unacceptable radiological consequences. The evaluation of sabotage scenarios should consider scenarios by individuals who do not have direct access to material or equipment.

5.22. To perform an act of sabotage, the insider adversary would not necessarily need to leave the facility to complete the malicious act. Therefore, the evaluation of preventive and protective measures against any insider exiting the facility would be applicable.

EVALUATION OF A FACILITY FOR PROTECTION AGAINST INSIDER THREATS

5.23. The process of evaluating a facility for protection against insider threats begins with characterizing insiders according to attributes, motivations and categories to identify potential insider threats. The next step is target identification, which involves an evaluation of the assets that need to be protected from unauthorized removal or sabotage. The result of this evaluation is a prioritized list of targets.

5.24. Preventive measures should be implemented using the concept of defence in depth and a graded approach to minimize opportunities for the identified threats and targets to be subject to malicious acts.

5.25. Protective measures should be identified to protect targets in protected, inner or vital areas in a prioritized manner. The measures to detect, delay and respond to the insider threat should be increased in depth by using the results of the evaluation.

5.26. Preventive and protective measures against sabotage and unauthorized removal of nuclear material should be evaluated using a method such as the development of credible scenarios. Scenarios should be consistent with the threat assessment or DBT and may include physical attacks, cyber-attacks or a combination of both at the facility, along transport routes and within supply chains.

5.27. The system should be re-evaluated periodically to ensure that the measures are effectively implemented and sustained. The timing of the re-evaluation might be cyclic, or it might be triggered by changes to the threat or to the facility and its operation.

REFERENCES

[1] INTERNATIONAL ATOMIC ENERGY AGENCY, Objective and Essential Elements of a State's Nuclear Security Regime, IAEA Nuclear Security Series No. 20, IAEA, Vienna (2013).

[2] INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5), IAEA Nuclear Security Series No. 13, IAEA, Vienna (2011).

[3] INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Recommendations on Radioactive Material and Associated Facilities, IAEA Nuclear Security Series No. 14, IAEA, Vienna (2011).

[4] EUROPEAN POLICE OFFICE, INTERNATIONAL ATOMIC ENERGY AGENCY, INTERNATIONAL CIVIL AVIATION ORGANIZATION, INTERNATIONAL CRIMINAL POLICE ORGANIZATION–INTERPOL, UNITED NATIONS INTERREGIONAL CRIME AND JUSTICE RESEARCH INSTITUTE, UNITED NATIONS OFFICE ON DRUGS AND CRIME, WORLD CUSTOMS ORGANIZATION, Nuclear Security Recommendations on Nuclear and Other Radioactive Material out of Regulatory Control, IAEA Nuclear Security Series No. 15, IAEA, Vienna (2011).

[5] INTERNATIONAL ATOMIC ENERGY AGENCY, Security of Radioactive Sources, IAEA Nuclear Security Series No. 11, IAEA, Vienna (2009).
[6] INTERNATIONAL ATOMIC ENERGY AGENCY, Security in the Transport of Radioactive Material, IAEA Nuclear Security Series No. 9, IAEA, Vienna (2008).
[7] INTERNATIONAL ATOMIC ENERGY AGENCY, Computer Security at Nuclear Facilities, IAEA Nuclear Security Series No. 17, IAEA, Vienna (2011).
[8] INTERNATIONAL ATOMIC ENERGY AGENCY, Security of Nuclear Information, IAEA Nuclear Security Series No. 23-G, IAEA, Vienna (2015).
[9] INTERNATIONAL ATOMIC ENERGY AGENCY, Use of Nuclear Material Accounting and Control for Nuclear Security Purposes at Facilities, IAEA Nuclear Security Series No. 25-G, IAEA, Vienna (2015).
[10] INTERNATIONAL ATOMIC ENERGY AGENCY, Engineering Safety Aspects of the Protection of Nuclear Power Plants against Sabotage, IAEA Nuclear Security Series No. 4, IAEA, Vienna (2007).
[11] INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Culture, IAEA Nuclear Security Series No. 7, IAEA, Vienna (2008).
[12] INTERNATIONAL ATOMIC ENERGY AGENCY, Development, Use and Maintenance of the Design Basis Threat, IAEA Nuclear Security Series No. 10, IAEA, Vienna (2009).
[13] INTERNATIONAL ATOMIC ENERGY AGENCY, Security of Nuclear Material in Transport, IAEA Nuclear Security Series No. 26-G, IAEA, Vienna (2015).
[14] INTERNATIONAL ATOMIC ENERGY AGENCY, Establishing a System for Control of Nuclear Material for Nuclear Security Purposes at a Facility during Use, Storage and Movement, IAEA Nuclear Security Series No. 32-T, IAEA, Vienna (2019).
[15] INTERNATIONAL ATOMIC ENERGY AGENCY, Physical Protection of Nuclear Material and Nuclear Facilities (Implementation of INFCIRC/225/Revision 5), IAEA Nuclear Security Series No. 27-G, IAEA, Vienna (2018).
[16] INTERNATIONAL ATOMIC ENERGY AGENCY, Identification of Vital Areas at Nuclear Facilities, IAEA Nuclear Security Series No. 16, IAEA, Vienna (2012).
[17] INTERNATIONAL ATOMIC ENERGY AGENCY, Self-assessment of Nuclear Security Culture in Facilities and Activities, IAEA Nuclear Security Series No. 28-T, IAEA, Vienna (2007).

IAEA
International Atomic Energy Agency

No. 26

ORDERING LOCALLY

IAEA priced publications may be purchased from the sources listed below or from major local booksellers.

Orders for unpriced publications should be made directly to the IAEA. The contact details are given at the end of this list.

NORTH AMERICA

Bernan / Rowman & Littlefield
15250 NBN Way, Blue Ridge Summit, PA 17214, USA
Telephone: +1 800 462 6420 • Fax: +1 800 338 4550
Email: orders@rowman.com • Web site: www.rowman.com/bernan

REST OF WORLD

Please contact your preferred local supplier, or our lead distributor:

Eurospan Group
Gray's Inn House
127 Clerkenwell Road
London EC1R 5DB
United Kingdom

Trade orders and enquiries:
Telephone: +44 (0)176 760 4972 • Fax: +44 (0)176 760 1640
Email: eurospan@turpin-distribution.com

Individual orders:
www.eurospanbookstore.com/iaea

For further information:
Telephone: +44 (0)207 240 0856 • Fax: +44 (0)207 379 0609
Email: info@eurospangroup.com • Web site: www.eurospangroup.com

Orders for both priced and unpriced publications may be addressed directly to:

Marketing and Sales Unit
International Atomic Energy Agency
Vienna International Centre, PO Box 100, 1400 Vienna, Austria
Telephone: +43 1 2600 22529 or 22530 • Fax: +43 1 26007 22529
Email: sales.publications@iaea.org • Web site: www.iaea.org/publications

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

NUCLEAR SECURITY CULTURE
IAEA Nuclear Security Series No. 7
STI/PUB/1347 (37 pp.; 2008)
ISBN 978-92-0-107808-7 Price: €30.00

DEVELOPMENT, USE AND MAINTENANCE OF THE DESIGN BASIS THREAT
IAEA Nuclear Security Series No. 10
STI/PUB/1386 (30 pp.; 2009)
ISBN 978-92-0-102509-8 Price: €18.00

SECURITY OF RADIOACTIVE SOURCES
IAEA Nuclear Security Series No. 11
STI/PUB/1387 (66 pp.; 2009)
ISBN 978-92-0-102609-5 Price: €25.00

NUCLEAR SECURITY RECOMMENDATIONS ON PHYSICAL PROTECTION OF NUCLEAR MATERIAL AND NUCLEAR FACILITIES (INFCIRC/225/Revision 5)
IAEA Nuclear Security Series No. 13
STI/PUB/1481 (57 pp.; 2011)
ISBN 978-92-0-111110-4 Price: €28.00

USE OF NUCLEAR MATERIAL ACCOUNTING AND CONTROL FOR NUCLEAR SECURITY PURPOSES AT FACILITIES
IAEA Nuclear Security Series No. 25-G
STI/PUB/1685 (63 pp.; 2015)
ISBN 978-92-0-137810-1 Price: €20.00

PHYSICAL PROTECTION OF NUCLEAR MATERIAL AND NUCLEAR FACILITIES (IMPLEMENTATION OF INFCIRC/225/Revision 5)
IAEA Nuclear Security Series No. 27-G
STI/PUB/1760 (120 pp.; 2018)
ISBN 978-92-0-101915-8 Price: €30.00

ESTABLISHING A SYSTEM FOR CONTROL OF NUCLEAR MATERIAL FOR NUCLEAR SECURITY PURPOSES AT A FACILITY DURING USE, STORAGE AND MOVEMENT
IAEA Nuclear Security Series No. 32-T
STI/PUB/1786 (47 pp.; 2019)
ISBN 978-92-0-103017-7 Price: €38.00

COMPUTER SECURITY AT NUCLEAR FACILITIES
IAEA Nuclear Security Series No. 17
STI/PUB/1527 (69 pp.; 2011)
ISBN 978-92-0-120110-2 Price: €33.00

SECURITY OF NUCLEAR INFORMATION
IAEA Nuclear Security Series No. 23-G
STI/PUB/1677 (54 pp.; 2015)
ISBN 978-92-0-110614-8 Price: €30.00

COMPUTER SECURITY OF INSTRUMENTATION AND CONTROL SYSTEMS AT NUCLEAR FACILITIES
IAEA Nuclear Security Series No. 33-T
STI/PUB/1787 (58 pp.; 2018)
ISBN 978-92-0-103117-4 Price: €42.00

This publication is an update of IAEA Nuclear Security Series No. 8, originally published in 2008. The revision was undertaken to better align this Implementing Guide with the Nuclear Security Fundamentals and with the Recommendations that were published after 2008, to cross-reference other relevant Implementing Guides published since 2008, and to add further detail on certain topics based on the experience of the IAEA and Member States in using IAEA Nuclear Security Series No. 8. This publication provides updated guidance to States, their competent authorities, and operators, shippers and carriers on selecting, implementing and evaluating measures for addressing insider threats. It 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 design, construction, commissioning, operation, shutdown or decommissioning.

INTERNATIONAL ATOMIC ENERGY AGENCY
VIENNA
ISBN 978–92–0–103419–9
ISSN 1816–9317