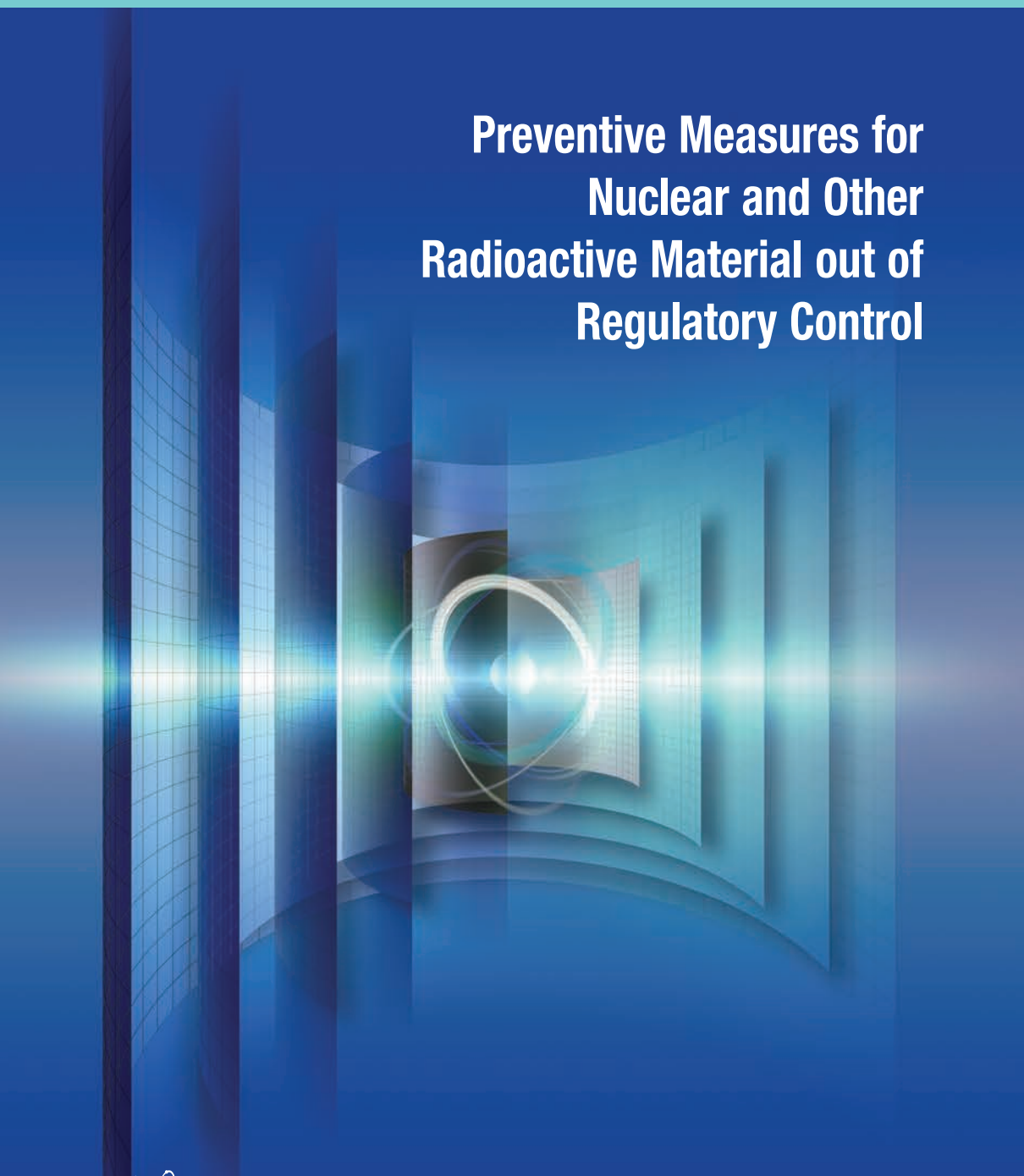
IAEA Nuclear Security Series No. 36-G

Implementing Guide

Preventive Measures for Nuclear and Other Radioactive Material out of Regulatory Control



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 MEASURES FOR NUCLEAR AND OTHER RADIOACTIVE MATERIAL OUT OF REGULATORY CONTROL

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
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. 36-G

PREVENTIVE MEASURES FOR NUCLEAR AND OTHER RADIOACTIVE MATERIAL OUT OF REGULATORY CONTROL

IMPLEMENTING GUIDE

INTERNATIONAL ATOMIC ENERGY AGENCY
VIENNA, 2019

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/books

Printed by the IAEA in Austria
July 2019
STI/PUB/1855

IAEA Library Cataloguing in Publication Data

Names: International Atomic Energy Agency.
Title: Preventive measures for nuclear and other radioactive material out of regulatory control / International Atomic Energy Agency.
Description: Vienna : International Atomic Energy Agency, 2019. | Series: IAEA nuclear security series ; ISSN 1816–9317 ; no. 36-G | Includes bibliographical references.
Identifiers: IAEAL 19-01248 | ISBN 978–92–0–102619–4 (paperback : alk. paper)
Subjects: LCSH: Nuclear industry — Security measures. | Radioactive substances — Detection. | Nuclear terrorism — Prevention.
Classification: UDC 341.67 | STI/PUB/1855

FOREWORD

By Yukiya Amano, Director General

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

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. A comprehensive national nuclear security regime includes effective nuclear security systems and measures for nuclear and other radioactive materials that are either under or out of regulatory control. Paragraph 2.1 of the Nuclear Security Fundamentals, IAEA Nuclear Security Series No. 20, Objective and Essential Elements of a State's Nuclear Security Regime [1], states that "The objective of a State's *nuclear security regime* is to protect persons, property, society, and the environment from harmful consequences of a *nuclear security event*." This objective can be achieved by applying the principles set out in the Nuclear Security Fundamentals, Recommendations and Implementing Guides contained in the IAEA Nuclear Security Series [2–4].

1.2. A nuclear security event involving nuclear or other radioactive material out of regulatory control (hereafter referred to as 'material out of regulatory control') may result in harmful health, economic, environmental and societal consequences. Therefore, a defence in depth approach for the design and implementation of nuclear security systems and measures is essential for prevention and detection of and response to nuclear security events.

1.3. Measures to prevent a nuclear security event are an integral part of a comprehensive nuclear security regime, and complement measures for detecting and responding to nuclear security events. Such preventive measures may be intended:

(a) To prevent nuclear material or radioactive material that is under regulatory control from becoming out of regulatory control by preventing its unauthorized removal from associated facilities or associated activities. Such measures are addressed within the IAEA Nuclear Security Series (see Refs [2] and [3]).
(b) To prevent nuclear material or radioactive material that is out of regulatory control from being used in a criminal or intentional unauthorized act. Such measures are addressed within the IAEA Nuclear Security Series (see Ref. [4]).

1.4. This publication provides guidance for implementing the preventive measures described in IAEA Nuclear Security Series No. 15, Nuclear Security Recommendations on Nuclear and Other Radioactive Material out of Regulatory

Control [4]. It is fully consistent with the Nuclear Security Fundamentals [1] and Nuclear Security Recommendations publications [2, 3], and is complementary to the Implementing Guides that address detection of and response to nuclear security events [5, 6].

OBJECTIVE

1.5. The objective of this publication is to provide guidance on the development and establishment of technical and administrative measures to prevent criminal or intentional unauthorized acts with nuclear security implications involving material out of regulatory control. This guidance is intended for national legislators, policy makers, competent authorities, law enforcement agencies, organizations and individuals involved in the establishment, implementation, maintenance and sustainability of a State's nuclear security regime.

SCOPE

1.6. This publication addresses measures (referred to as 'preventive measures' in this publication) that aim to prevent criminal or intentional unauthorized acts involving nuclear and other radioactive material that is already out of regulatory control. These measures include those aimed at preventing a potential adversary from attempting criminal or intentional unauthorized acts, for example, deterrence measures, and those aimed at preventing an adversary from successfully completing such an act, for example measures complementary to those for detection of material out of regulatory control and response to nuclear security events.

1.7. This publication complements guidance on the design and implementation of nuclear security systems and measures for the detection of and response to nuclear security events [5, 6]. It does not repeat or elaborate upon such guidance except to the extent that detection or response measures may also have a preventive effect, for example by deterring potential adversaries.

1.8. Guidance on nuclear security systems and measures for nuclear material, other radioactive material, associated facilities or associated activities that are under regulatory control is provided in other Nuclear Security Series publications. This publication does not address such systems and measures, but such measures also may contribute towards preventing criminal or intentional unauthorized acts

with nuclear security implications involving material out of regulatory control by preventing material from leaving regulatory control.

STRUCTURE

1.9. Following this introduction, Section 2 covers general considerations for preventive measures. Section 3 covers deterrence measures, including deterrence by punishment and deterrence by denial. Section 4 covers information security. Section 5 covers the promotion of nuclear security culture. Section 6 covers measures for addressing the insider threat, including measures to promote the trustworthiness of personnel. Section 7 provides guidance for international cooperation and assistance to strengthen preventive measures.

2. GENERAL CONSIDERATIONS FOR PREVENTIVE MEASURES

GENERAL

2.1. This publication addresses a range of measures that may be used by a State to prevent criminal or intentional unauthorized acts involving nuclear and other radioactive material that is already out of regulatory control. Preventive measures as described in this publication complement each other and should be considered as an integral set of measures to be implemented together.

BASIS FOR ESTABLISHING PREVENTIVE MEASURES

2.2. A basis for measures aimed to prevent nuclear security events that involve material out of regulatory control from occurring needs to be established within the State. This basis involves three elements: a comprehensive and effective legislative and regulatory framework for nuclear security; the establishment or assignment of relevant competent authorities, as well as a coordinating body or mechanism; and the use of a threat assessment and risk informed approach. While these elements are relevant to all areas of nuclear security, aspects related to the nuclear security of material out of regulatory control are highlighted in the following sections.

Legal and regulatory framework

2.3. An effective legislative and regulatory framework is essential for implementing nuclear security systems and measures for material out of regulatory control. Further detailed guidance on designing and implementing a legal and regulatory framework for nuclear security, including offences and penalties can be found in Ref. [7], including guidance specific to establishing a legal and regulatory framework specific to detection and response.

2.4. As described in Ref. [1], Essential Element 5 of a State's nuclear security regime is offences and penalties including criminalization. Paragraph 3.5 of Ref. [1] states that:

> "3.5. A *nuclear security regime* includes measures for:
>
> (a) Defining as offences or violations under domestic laws or regulations those criminal or intentional unauthorized acts involving or directed at *nuclear material, other radioactive material, associated facilities or associated activities*;
> (b) Appropriately dealing with other acts determined by the State to have an adverse impact on nuclear security;
> (c) Establishing appropriate penalties that are proportionate to the gravity of the harm that could be caused by commission of the offences or violations;
> (d) Establishing the jurisdiction of the State over such offences or violations;
> (e) Providing for the prosecution or, as appropriate, extradition of alleged offenders."

The potential for the prosecution of persons charged with offences involving material out of regulatory control may have a deterrent (and hence preventive) effect, underlining the importance of an effective legal and regulatory framework that empowers appropriate authorities to arrest and prosecute those who commit such acts.

2.5 Paragraph 3.2 of Ref. [4] states that:

> "3.2. As part of an overall framework, the State should establish and maintain effective executive, judicial, legislative and regulatory frameworks to govern the *detection* of and *response* to a criminal act, or an unauthorized act, with nuclear security implications involving any nuclear or other *radioactive*

material that is out of *regulatory control*. Responsibilities should be clearly defined for implementing various elements of nuclear security and assigned to the relevant *competent authorities*".

In particular, Ref. [4] provides several recommendations regarding a legal and regulatory framework for material out of regulatory control.

(a) Paragraph 3.4 of Ref. [4] states that:

"3.4. The State should establish criminal offences under domestic law which should include the wilful, unauthorized acquisition, possession, use, transfer or transport of nuclear or other *radioactive material* consistent with international treaties, conventions and legally binding United Nations Security Council resolutions."

(b) Paragraph 3.5 of Ref. [4] states that:

"3.5. The State should also establish as criminal offences a threat or attempt to commit an offence as described in paragraph 3.4."

(c) Paragraph 3.6 of Ref. [4] states that:

"3.6. The State should consider establishing as criminal offences, unlawful scams or hoaxes[4] with nuclear security implications."

"[4] Historically, scams and hoaxes constitute a portion of the cases of illicit trafficking. Despite the absence of nuclear or other *radioactive material*, such scams and hoaxes can necessitate responses that potentially expose operational and/or *detection* vulnerabilities that could be exploited by smugglers. Scams and hoaxes can perpetuate the belief that smuggling such material can be profitable and may encourage the criminal or unauthorized possession of nuclear or other radioactive material."

(d) Paragraph 3.7 of Ref. [4] states that:

"3.7. The State should establish its jurisdiction over any criminal act associated with a *nuclear security event* when the offence is committed in the territory of that State or on board a ship or aircraft registered in that State or when the alleged offender is a national of that State or when the alleged offender is present in its territory and it does not extradite the alleged offender."

(e) Paragraph 3.8 of Ref. [4] states that:

> "3.8. Effective and sustainable *detection* and *response* measures rely on multidisciplinary infrastructures implemented by several independent *competent authorities* in the State. The State should ensure proper cooperation, coordination, information exchange and integration of activities and clearly defined responsibilities across multiple *competent authorities*, and establish a coordinating mechanism or identify an existing governmental body, committee or organization to act as the coordinating body, as described in paragraphs 3.12–3.14. In carrying out the *nuclear security measures*, the State should take into consideration the results of the threat assessment."

2.6. The State's legal and regulatory framework should be periodically reviewed to consider the deterrent effect it may have and how that effect could be enhanced. The framework should be revised to address weaknesses disclosed by the review.

Competent authorities and coordination mechanism

2.7 As noted in the preceding section, para. 3.2 of Ref. [4] states that:

> "[r]esponsibilities should be clearly defined for implementing various elements of nuclear security and assigned to the relevant *competent authorities*".

2.8 Paragraph 3.8 of Ref. [4] also notes that:

> "[t]he State should ensure proper cooperation, coordination, information exchange and integration of activities and clearly defined responsibilities across multiple *competent authorities*, and establish a coordinating mechanism or identify an existing governmental body, committee or organization to act as the coordinating body".

2.9. In addition, para. 3.9 of Ref. [4] states that, "[t]he State should ensure effective coordination among the different levels and jurisdictions of federal, state, and local authorities". The establishment of an effective coordination body or mechanism and the close cooperation between competent authorities are particularly important for effective nuclear security of material out of regulatory control.

2.10. Paragraph 2.1 of Ref. [4] also states that the objectives of the parts of the nuclear security regime for material out of regulatory control are achieved by, among other elements, the "[p]rovision of sufficient and sustained resources to the various *competent authorities* to enable them to carry out their assigned functions…"

2.11. The implementation of the elements listed above can demonstrate the State's determination in combating criminal or intentional unauthorized acts with nuclear security implications involving nuclear and other radioactive material out of regulatory control, and may deter the commission of such acts. Further guidance regarding competent authorities and coordination can be found in Refs [4, 7, 8].

Threat assessment and risk informed approach

2.12. An important step to prevent criminal or intentional unauthorized acts with nuclear security implications involving material out of regulatory control is to develop an accurate and up to date assessment of threats and associated risks related to such material. Further detailed guidance on developing a risk informed approach and conducting threat and risk assessments as the basis for the design and implementation of nuclear security systems and measures for prevention of, detection of and response to criminal or intentional unauthorized acts with nuclear security implications involving material out of regulatory control can be found in Ref. [9].

2.13. States may alter their threat and risk assessments during a major public event, or higher alert situation. During such an event, the State may consider expanding its prevention, detection and response measures for nuclear security to deter adversaries from committing criminal or intentional unauthorized acts [5, 6].

PREVENTIVE EFFECTS OF DETECTION AND RESPONSE MEASURES

2.14. Detection and response measures are primarily designed to identify when a nuclear security event is taking place and to respond appropriately if such an event occurs. However, these measures may also have a preventive effect when they are, and are seen to be, effective. Detection measures may contribute to preventing a criminal or intentional unauthorized act with nuclear security implications involving material out of regulatory control by detecting material that is out of regulatory control before it can be used for such an act. Effective

detection and response measures can also contribute to the same objective by deterring adversaries from attempting to undertake a criminal act and by reducing the likelihood of such an attempt being successful.

2.15. Detailed guidance on implementing measures for detection of and response to nuclear security events is outside the scope of this Implementing Guide and is provided in other publications [5, 6].

3. DETERRENCE MEASURES

GENERAL

3.1. This section describes approaches and methods to designing and implementing deterrence measures, which may be tailored to national circumstances and conditions. Deterrence measures are measures taken to prevent a criminal or intentional unauthorized act by attempting to affect adversary decision making. Combined with other preventive measures, deterrence measures can increase the effectiveness of the nuclear security regime.

3.2. An integrated and effective set of deterrence measures may lead the adversary to:

— Permanently or temporarily abandon plans for a particular criminal or intentional unauthorized act involving material out of regulatory control;
— Change plans (if the deterrence measures are well targeted) to focus on a less attractive target or less effective approach;
— Continually delay an act.

3.3. In addition to front end preventive measures, deterrence measures may be broadly divided into two categories: those that rely on convincing a potential adversary that there is a realistic possibility of severe punishment for attempting criminal or intentional unauthorized acts; and those that rely on convincing a potential adversary that succeeding in committing such acts will be prohibitively difficult, unlikely or dangerous to the adversary. These two types of deterrence are referred to in this publication, respectively, as ‘deterrence by

punishment'[1] and 'deterrence by denial'. The two types of deterrence may be useful against different types of adversary, and for some adversaries, they may be complementary.

3.4. In addition, the adversary's plans and actions typically need funding. Eliminating or reducing the supply of financial support for adversaries will complicate their plans and may delay any actions, thus potentially resulting in enhanced deterrence.

3.5. Deterrence measures may be tailored to specific types of adversary identified and characterized in the national threat assessment. Individual motivations (e.g. personal, financial, political) of an adversary will influence how they interpret and respond to different deterrence measures. Other factors that may influence decision making include the adversary's capabilities and specific intentions, the costs and benefits of attempting such an act, and the adversary's tolerance of risk. For example, the perception that there is a high likelihood of detection and prosecution will be more likely to deter a risk averse adversary than an adversary who is not risk averse. The possibility of identification might deter some adversaries, but not others. For example, some adversaries may identify themselves after the occurrence of a nuclear security event as part of a deliberate strategy. In this case, the risk of failure (including discovery before the act) is likely to be a greater deterrent than the risk of discovery after the act.

3.6. A State's national threat assessment provides specific information on the types of adversary that should be considered in designing nuclear security systems and measures, including those for material out of regulatory control. Table 1 provides an overview of common types of adversary motivation for engaging in criminal or intentional unauthorized acts with nuclear security implications involving material out of regulatory control, which should be considered by States when considering deterrence measures [9].

3.7. Table 2 provides an overview of common types of adversary capabilities needed for planning and carrying out criminal or intentional unauthorized acts with nuclear security implications involving material out of regulatory control, which should be considered by States when considering preventive measures [9].

3.8. The adversary may be supported by actors who are not directly involved in the execution of the act. Each of these types of actor might have a different

[1] In this context, the term 'punishment' refers to the cumulative effect of one or more penalties inflicted on an offender through a judicial procedure.

TABLE 1. TYPES OF ADVERSARY MOTIVATION

Type of motivation	Description
Financial	An individual or a group that commits or facilitates illegal acts for financial gain.
Personal	An individual or group that commits illegal acts for personal satisfaction, retribution or for coercion.
Political or ideological	An individual or group of individuals prepared to commit illegal acts in support of a political or ideological view, either of general philosophy or on a specific issue.

motivation and might be deterred or influenced by different means. For example, some actors might not be aware that they are contributing to a criminal or intentional unauthorized act, while others might be acting under duress, which might override considerations that would otherwise deter them from contributing to the act. These actors may be made up of specialists and intermediaries.

3.9. Specialists include actors with specialized knowledge and relevant skills, such as scientists and technicians with nuclear training and experience working with nuclear or other radioactive material. These specialists may be needed to handle nuclear or other radioactive material, to design a device intended to be used in committing a criminal or intentional unauthorized act, or to overcome security measures to facilitate such an act. An increased likelihood of identification might deter those who provide specialized assistance to an adversary.

3.10. Intermediaries include actors providing various types of support to an adversary. For example, intermediaries might supply nuclear or other radioactive material or other materials and equipment, or might provide a safe place to work, instruments, transport (including across borders), or people to assist in evading law enforcement in the target country (e.g. with local language ability). Intermediaries may be motivated by money, conviction or fear, and may be deterred by means that would not deter the primary adversary. For example, a politically or ideologically motivated adversary may be most effectively deterred by the perception that success of the act is prohibitively difficult or unlikely, while specialists or intermediaries may be more influenced by the risk of punishment.

3.11. While there are many benefits of using deterrence as part of a State's strategy for considering preventive measures for material out of regulatory

TABLE 2. TYPES OF ADVERSARY CAPABILITY

Type of capability	Description
Organization	Structure/leadership: Chain of command, coordination Group size and distribution Adaptability: Ability to evolve to changing environments
Skills	Technical skills: Related to handling, transport, manipulation of nuclear and other radioactive material out of regulatory control and associated threat devices Cyber and communication skills: Using computers and automated control systems for purposes including direct support of physical attacks, intelligence gathering, computer based attacks, money collection and communication Operational skills: Familiarity with targets, site plans and procedures, security measures, operations and tactics; knowlege of nuclear or other radioactive material
Financial	Amount Source Availability
Equipment	Weapons: Type, number, availability Tools: Mechanical, thermal, manual, power, electronic and electromagnetic tools; communications equipment; vehicles
Access	Modes of transport: Public, private; land, sea, air; type, number, availability Insider issues: Collusion (passive/active), violent/non-violent, number of insiders Support structure: Local sympathizers, support organization, logistics

control, the State should not rely solely or primarily on deterrence as a nuclear security strategy. Deterrence alone is not sufficient to prevent criminal or intentional unauthorized acts with nuclear security implications involving material out of regulatory control and should be based on and integrated with effective detection and response systems and measures. This is owing to the limitations intrinsic to deterrence, including the likelihood of having incomplete or inaccurate understanding of the adversary's rationale for decision making, the uncertainty in judging the effectiveness of deterrence — it is difficult to know whether or not an adversary was deterred — and because some adversaries may not be able to be deterred.

DETERRENCE BY PUNISHMENT

3.12. To effectively implement deterrence by punishment, States should seek to improve their capabilities to successfully apprehend and prosecute adversaries.

3.13. An adversary may be deterred by the perceived risk of apprehension or the perception that, if caught, the penalty is too severe to warrant the act. A range of penalties should be developed and communicated to deter criminal or intentional unauthorized acts involving material out of regulatory control, because different adversaries may perceive or react to penalties differently. Penalties should be proportionate to the harm that could be caused by committing the offences or violations, and these penalties should be clearly set forth in national legislation.

3.14. An effective forensic capability may contribute to deterrence by increasing the likelihood of identifying, apprehending and prosecuting adversaries, including supporting actors. Further guidance on nuclear forensics applications and capabilities can be found in Ref. [10].

DETERRENCE BY DENIAL

3.15. To effectively implement deterrence by denial, States should seek to make an impact on an adversary's perceptions of the likelihood of a successful criminal or intentional unauthorized act with nuclear security implications involving material out of regulatory control by establishing and communicating about its effective nuclear security measures.

3.16. Adversaries may be deterred if the perceived likelihood of success is low or the costs of success are perceived to be prohibitively high. While some adversaries may not fear penalties, it is likely that they want to succeed in the actions they undertake to achieve their objectives. If an adversary is aware of effective nuclear security measures against intentional unauthorized acts involving material out of regulatory control, he or she might choose not to undertake the planned act.

3.17. Detection systems and measures at borders, within the State's interior and near potential targets may help to deter adversaries from the commission of criminal or intentional unauthorized acts involving material out of regulatory control by demonstrating to a potential adversary that such an act would be detected during transportation of these materials through these locations [4, 9]. Measures for responding to a criminal or intentional unauthorized act may deter the commission of such acts if adversaries perceive that the State's or facility's

response capabilities will significantly reduce the likelihood of success or involve a cost and effort that exceeds the perceived benefits of the act to the adversary [4, 6, 11, 12].

3.18. Where appropriate, States may also seek to incorporate elements of unpredictability into their nuclear security systems and measures, with the goal of causing the adversary to expend more resources or delay acts. Examples of unpredictability may include deploying highly visible security measures (such as personnel) at irregular times and locations, withholding tactical information about where mobile detection systems are deployed at a given time or constructing detection systems so that the presence or absence of the capability cannot be determined with certainty by an adversary. These methods have the added benefit of allowing a State to rotate limited resources among many locations, if necessary.

3.19. Even nuclear security systems and measures with limited effectiveness might deter an adversary, depending on the circumstances. For deterrence by denial to be effective, nuclear security systems and measures need to be sufficient to convince an adversary that an act would be unlikely to succeed or would be too costly to warrant the act. If an adversary is prepared to undertake an act only if it has a high probability of success, nuclear security capabilities that pose even a limited risk of failure could have a deterrent effect. Inadequate knowledge of a State's nuclear security capabilities could lead the adversary to exaggerate the extent of implemented measures and to decide against an act. Overcoming nuclear security systems and measures may appear to be more difficult, risky or costly to an external adversary than to an internal adversary (for more on internal threats, see Section 6) who designed, built and operated these systems and measures and who is familiar with their weaknesses. In such cases, information security (see Section 4) may also be crucial.

3.20. States should be aware that deterrence can lead adversaries to change their targets and methods. For example, if an adversary is deterred from a target, he or she may decide to attack a different target or to use an alternative route or method rather than abandon the plan altogether. Competent authorities should consider all targets, routes or methods that an adversary might select. Competent authorities should ensure that adequate measures are taken in relation to all targets, routes or methods because nuclear security measures can only contribute to deterrence if the adversary believes that they cannot easily be bypassed or defeated.

PUBLIC INFORMATION FOR IMPROVING DETERRENCE EFFECTS

3.21. A State should determine the appropriate type and level of information to communicate, particularly about material out of regulatory control, as well as the appropriate mechanisms to use for this communication. The messages should be intended to convince adversaries that the likelihood of failure (deterrence by denial) or of being detected, identified and punished or injured in the course of handling such material (deterrence by punishment) outweighs the perceived benefits of their actions.

3.22. States may manage the potential deterrent effect of nuclear security systems through several communication mechanisms, including:

— Observation: Some security systems can be seen by an adversary directly. For example, radiation portal monitors can be observed at international border crossings or personal radiation detectors can be visible on the belts of law enforcement officers.
— Demonstration: Some security systems may not be directly observable or permanently deployed. In this case, the State can use observable training and exercises to demonstrate detection and response capabilities.
— Public communication: States may choose to release information about detection and response capabilities through public communication mechanisms such as the media.

3.23. When managing communication mechanisms, States need to balance information security and deterrence efforts. Communication mechanisms might provide general and accurate information on security systems, but should not provide sufficient information to enable an adversary to circumvent the system.

3.24. Routine public communications can be used as an opportunity to communicate for deterrence purposes. Some specific public messages and narratives might be tailored to specific types of adversary to achieve a desired deterrent effect. However, the primary audience for such communication mechanisms is usually the general public. Communications aimed at potential adversaries might be perceived as propaganda, might not be considered credible and might not have any deterrent impact. Communications need to be credible in order to be effective.

3.25. States should consider undertaking efforts to raise public awareness of the risks of nuclear security events, and the measures taken to prevent, detect and respond to them. Raising public awareness of nuclear security should be an

important part of nuclear security efforts at the national level. In particular, States should raise awareness of the prevention of, detection of and response to criminal or intentional unauthorized acts with nuclear security implications involving material out of regulatory control, as members of the public might be affected by or otherwise encounter material out of regulatory control and related activities.

3.26. As discussed in the next section, a State's internal policy and procedures should consider the need for information security when considering the dissemination of appropriate information to the public through appropriate media. For example, these media may be routinely accessed by adversaries for reconnaissance activities before planning a nuclear security event. Therefore, competent authorities and the organizations involved need to carefully consider how best to implement internal policies, standards and procedures for disseminating public information without compromising nuclear security.

4. INFORMATION SECURITY

4.1. Information security, as described in para. 2.10 of Ref. [13], "refers to the system, programme or set of rules in place to ensure the confidentiality, integrity and availability of information in any form." Information security should be implemented as part of an overall risk informed approach, in conjunction with human resource development within all competent authorities and all stakeholders involved in the design, development and implementation of nuclear security systems and measures for material out of regulatory control.

4.2. Further guidance on security of nuclear information is provided in Ref. [13]. While Ref. [13] is in large part specific to nuclear and other radioactive material under regulatory control and associated facilities and activities, many of the general considerations it contains are also relevant to material out of regulatory control. A summary of relevant information provided in Ref. [13] on this topic is provided here, along with some considerations specific to material out of regulatory control.

4.3. Paragraph 2.2 of Ref. [13] states that:

> "2.2. Information is knowledge, irrespective of its form of existence or expression. It includes ideas, concepts, events, processes, thoughts, facts and patterns. Information can be recorded on material such as paper, film,

magnetic or optical media, or held in electronic systems. Information can be represented and communicated by almost any means."

4.4. Paragraph 2.5 of Ref. [13] states that:

"2.5. Sensitive information is information, the unauthorized disclosure (or modification, alteration, destruction or denial of use) of which could compromise nuclear security or otherwise assist in the carrying out of a malicious act against a nuclear facility, organization or transport."

Sensitive information related to material out of regulatory control includes information on nuclear security systems and measures for prevention of, detection of and response to criminal or intentional unauthorized acts with nuclear security implications involving material out of regulatory control, and information that may otherwise assist in carrying out such acts.

4.5. Paragraph 6.6 of Ref. [13] states that:

"6.6. Management responsibilities typically include:

(a) Assuming overall responsibility for securing sensitive information and sensitive information assets;
(b) Ensuring compliance with relevant laws and regulations;
(c) Assigning organizational security responsibilities;
(d) Providing effective security training and education;
(e) Ensuring that an effective information security policy is established;
(f) Providing adequate resources to implement an effective information security programme;
(g) Ensuring development of the information security programme and associated plans and procedures;
(h) Ensuring effective change management related to plans, procedures and policies;
(i) Ensuring periodic audits, reviews and revisions of information security policy and procedures."

4.6. While these responsibilities are discussed more generally in Ref. [13], they also apply to information security for nuclear security systems and measures for material out of regulatory control. Ensuring adequate communication among all involved parties and individuals is of particular importance for information security in organizations with responsibilities related to material out of regulatory

control, due to the many different organizations typically involved in efforts to detect such material and respond to nuclear security events.

4.7. Paragraph 3.16 of Ref. [13] states that:

> "3.16. A national system of classification should be established and maintained to group information into classes, such that the unauthorized disclosure of any of the information within a class would have similar consequences, and therefore that all information in a particular class should be subject to similar security requirements. This should be a national system, not specific to a particular industry or devised by a single facility."

The appropriate identification, classification, protection and management of sensitive nuclear security information in all forms, covering all phases of the lifetime of information (creation, classification, use, storage, destruction), are essential for the prevention of criminal or intentional unauthorized acts involving material out of regulatory control.

4.8. Paragraph 6.7 of Ref. [13] states that:

> "6.7. Guidance on the classification to be applied to an information object should be provided by the relevant competent authorities in the form of a classification guide or guidance."

While intended in Ref. [13] for facilities, this guidance also applies to activities related to material out of regulatory control. In particular, each organization's policy and procedures based on the national legal and regulatory framework should include classification of information, including the level to which the information should be protected, and the access to procedures and protocols.

4.9. Paragraph 6.12 of Ref. [13] states that:

> "6.12. Responsibility for information security should be included in an organization's hierarchy of policies and procedures. As a minimum, the following should be addressed:
>
> (a) A definition of information security and a statement of its overall objectives, scope and importance.
> (b) A definition of roles and responsibilities, including the establishment of a focal point to direct and manage information security.

(c) Compliance with information security requirements, including legal, regulatory and contractual requirements.
(d) The establishment of a risk management plan to reduce risks to an acceptable level, defined by the State, by applying adequate controls based on a risk assessment approach. For a nuclear facility, the risk management plan should be approved by the competent authority or other authority designated by the State.
(e) Regular monitoring and review of the arrangements in place to ensure that policy, standards and procedures remain relevant and effective.
(f) Requirements for education and training to ensure that staff, contractors and other personnel have an appropriate awareness of policy, procedures and practice to the extent necessary for their duties, and that they fully understand their responsibilities (including their legal obligations).
(g) The consequences (i.e. penalties or sanctions) for non-compliance with information security requirements or wilful negligence in securing sensitive information.
(h) Reference documentation that supports the policy, for example more detailed procedures for specific systems or security rules to which users should adhere."

4.10. Paragraph 6.13 of Ref. [13] states that:

"6.13. With specific reference to securing sensitive information, the plan should also cover:

(a) The information life cycle: definition of the processes to create, identify, classify, mark, handle, use, store, transmit, reclassify, reproduce and destroy sensitive information;
(b) The security requirements for sensitive information, giving due consideration to the security objectives of confidentiality, integrity and availability of the information;
(c) Restriction of access to sensitive information and sensitive information assets to those who need such access to perform their duties, who have the necessary authority and who have been subjected to a trustworthiness check commensurate with the classification level of the information;
(d) The transmission of sensitive information in a manner that reduces any risk of compromise, unauthorized interception, modification or disruption to an acceptable level."

4.11. As indicated by the definition of information in para. 4.3, policies and procedures for information protection should include protection of electronic data and the means of communication to be used during the detection of material out of regulatory control and during response to nuclear security events.

4.12. To implement effective detection and response measures, it is essential to share information among the relevant competent authorities and other organizations as well as with the public, other States (particularly neighbouring States) and relevant international organizations. Possible reasons for sharing information relevant to material out of regulatory control include:

(a) Enabling personnel of competent authorities and other relevant organizations to maintain awareness of the functions and needs of other organizations and to use knowledge and information from multiple reliable sources to support nuclear security efforts;
(b) Integrating information from various nuclear security activities, including preventive and protective measures, detection measures, criminal investigation activities, event preparedness and response to nuclear security events;
(c) Enabling relevant competent authorities and responsible individuals to establish procedures, processes, systems and measures that draw upon the integrated technical and administrative capabilities of multiple organizations and are consistent with established authorities and responsibilities;
(d) Allowing deployed assets for the detection of material out of regulatory control to function effectively. Paragraph 3.18 of Ref. [5] states that, "[d]eployed assets, such as detectors, technical support and analysis centres, should have the ability to exchange accurate and timely data."

4.13. Paragraph 5.3 of Ref. [13] states that:

> "5.3. The nature and extent of sharing such information should be based firstly on compliance with national laws or regulations and then on a balance between the benefits obtained from sharing and the needs of security. Rules on the passing of information between such authorities should be governed by the security procedures that pertain in that State. Establishing a common approach within the State can ensure that sensitive information is not disclosed inappropriately."

4.14. Each organization's policies and procedures should include conditions and arrangements for the sharing of sensitive information among the State's competent authorities that are responsible for material out of regulatory control,

and with other relevant organizations responsible for assisting law enforcement and prosecutorial bodies. These policies and procedures should also consider the formats and protocols regarding the information to be shared with the public, other States (particularly neighbouring States) and relevant international organizations.

4.15. If a State's competent authority is aware of a loss or theft of nuclear or other radioactive material, it should take measures to protect information on the characteristics of this material and the potential consequences of its malicious use, as well as the relevant detection and response measures.

4.16. The protection level of this information should be graded in accordance with the potential consequences of malicious use of the lost or stolen material.

5. PROMOTION OF NUCLEAR SECURITY CULTURE

5.1. It is essential that a robust nuclear security culture is embedded within all competent authorities and other organizations involved in nuclear security for material out of regulatory control (e.g. law enforcement, customs, intelligence agencies and emergency response agencies). Nuclear security culture plays a key role in ensuring that individuals, organizations and institutions remain vigilant and that sustained measures are taken to counter threats. A robust nuclear security culture can, therefore, contribute effectively to the prevention of nuclear security events.

5.2. Further guidance on the security of nuclear information is provided in Ref. [14]. While Ref. [14] is in large part specific to nuclear and other radioactive material under regulatory control and associated facilities and activities, many of the general considerations in this publication are also relevant to material out of regulatory control. A summary of relevant information provided in Ref. [14] on this topic is provided in this section, along with some considerations specific to material out of regulatory control.

5.3. Managers of competent authorities and organizations involved in nuclear security for material out of regulatory control should demonstrate commitment to nuclear security culture through actions and should provide firm and unambiguous support for the implementation of a policy on nuclear security culture. Actions should foster a corresponding commitment to high levels of performance by all individuals.

5.4. Effective nuclear security relies on personnel to operate, and maintain the nuclear security systems and measures for prevention of, detection of and response to nuclear security events. Section 3.4 of Ref. [14] states that:

> "[Personnel] should be expected to conduct themselves in a manner that recognizes the circumstances and potential consequences of their behaviour. This requires adopting a rigorous and prudent approach to their security responsibilities, with continuous regard for the protection of radioactive material and their associated facilities, including other sensitive locations and transport. Effective nuclear security culture is characterized by compliance with rules, regulations and procedures, and also constant vigilance and a proactive questioning attitude on the part of personnel."

Such conduct is also important within organizations responsible for material out of regulatory control.

5.5. Some challenges related to the creation of a robust and effective nuclear security culture are general, such as a lack of understanding of roles and responsibilities for nuclear security at all levels and resistance to changing attitudes and behaviours. Others, however, are specific to situations when multiple competent authorities and other organizations need to work together, as in the detection of and response to nuclear security events. Such challenges might include:

(a) Differing levels of awareness of the importance of nuclear security culture in different organizations;
(b) Inconsistent practices in management systems among organizations;
(c) Differences in personnel background;
(d) Limits of communication and cooperation, both horizontally and vertically;
(e) Competing priorities among the organizations.

All relevant competent authorities and other organizations involved in nuclear security of material out of regulatory control should consider the above challenges and seek to foster a robust and effective nuclear security culture.

6. ADDRESSING THE INSIDER THREAT

6.1. Insiders within relevant competent authorities or support organizations may have motivations that could lead to a willingness to participate in a criminal or intentional unauthorized act with nuclear security implications. This section describes the concepts and procedures for addressing the insider threat as part of preventive measures for material out of regulatory control. A formal process should be used to assess and adopt appropriate measures to prevent personnel involved in nuclear security of material out of regulatory control from committing acts that could jeopardize nuclear security [4]. This process should confirm the trustworthiness of personnel involved in detection and response measures. It is essential that personnel who have access, authority or knowledge that could be misused, are trustworthy to the level appropriate to their role, thereby reducing the risk of authorized personnel becoming insider threats and engaging in illegal activities.

6.2. Insiders may be willing to provide information that could assist in committing a criminal or intentional unauthorized act with nuclear security implications, while others may be willing to take actions to facilitate such an act (for example, providing access for an unauthorized person, or shutting down a detection instrument). Others may be prepared to actually carry out the act themselves, or may act as a result of blackmail/coercion. As a potential deterrent, personnel should be made aware that violation of laws and regulations related to nuclear security will be severely punished, even if such actions only facilitate or assist the commission of the main offence.

6.3. Section 2 of Ref. [15] states that:

> "Insiders may hold any position in an organization (e.g. experimenter, physical protection system designer, security guard, material handler, clerk, custodian, safeguards officer, operational and maintenance worker or senior manager). Others not directly employed by the operator but who also have access (such as vendors, emergency personnel, including firefighters and first responders, contractors, subcontractors and inspectors from regulatory organizations) should also be considered."

6.4. In addition, insider threats may possess attributes that provide advantages over outsider threats when attempting malicious activities, such as authorized access, authority and knowledge [15]. When applied to organizations responsible for material out of regulatory control, these attributes might include access

to detection and response systems and measures, and related equipment or information; authority over operations or personnel to acquire, use or maintain detection and response systems and measures; knowledge of the design of these systems and measures; access to sensitive information; or the possession of technical skills and experience.

6.5. The goal of preventive measures in this context is to reduce the number of potential insider threats and to minimize the opportunity for insiders to perform a criminal or intentional unauthorized act. Supervisors should apply several preventive measures, prior to employment, during employment and after employment to reach this goal.

6.6. Measures taken prior to employment include identity verification, personal document verification and trustworthiness assessments [15].

6.7. Measures considered particularly relevant to material out of regulatory control are discussed in para. 4.10 of Ref. [4], which states that:

> "Taking into consideration State laws, regulations, or policies regarding personal privacy and job requirements, the *competent authorities* should ensure that the personnel involved in nuclear security activities in the areas of *detection* and *response*, are explicitly deemed trustworthy, to the appropriate levels for their roles, by a formal process. This formal process should serve to assist in reducing the risk of authorized personnel engaging in illegal activities, e.g. insider threats. The State should adopt measures and procedures to ensure that the trustworthiness of personnel is regularly revalidated."

6.8. As described in Ref. [15], trustworthiness assessments are used to provide an initial assessment (during the hiring process) and ongoing assessments (occurring periodically throughout the employment period) of an individual's integrity, honesty and reliability. In addition, 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.

6.9. Measures to be applied during employment should include [15]:

(a) Development and implementation of escorting procedures;
(b) Periodic reassessment of the trustworthiness of insiders;
(c) Protection of sensitive information;
(d) Implementation of appropriate access controls;

(e) Authorization of activities;
(f) Compartmentalization of areas, duties, time and information;
(g) Adherence to standard operating procedures;
(h) A strong security awareness programme;
(i) A fitness for duty programme;
(j) Reporting and investigation of incidents of security concern;
(k) Provision of good working conditions;
(l) Rewards and recognition to employees;
(m) Use of sanctions.

Reassessing the trustworthiness of insiders and separation of duties are of particular importance to preventive measures for material out of regulatory control, and are discussed in more detail in the following paragraphs.

6.10. Reference [15] notes that the 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. In addition, 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. Particular attention should be paid to temporary or infrequent workers among the personnel of an organization or its subcontractors. Such workers may be more frequently employed by the many organizations involved in nuclear security systems and measures related to material out of regulatory control than by those operating regulated facilities and activities.

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

6.12. Separation of duties compartmentalizes the work activities of insiders to limit an insider's ability to obtain sufficient authorized access, authority, and/or knowledge needed to conduct a malicious act. Separation of duties includes applying the principle of least privilege to computer systems, through which an individual is assigned only those privileges that are essential to that individual's work. For example, one person could be assigned to observe the operation of a radiation portal monitor at a border crossing, while a second person, acting independently from the first, monitors local data and the resulting alarms.

6.13. This separation of duties may reduce the likelihood of an insider assisting a criminal or intentional unauthorized act, and increase the likelihood of detection of such an insider act. Separation of duties might also have a deterrent effect for insiders by increasing the difficulty of performing a successful act.

7. INTERNATIONAL COOPERATION AND ASSISTANCE TO STRENGTHEN PREVENTIVE MEASURES

7.1. International cooperation and assistance can contribute to strengthening a State's nuclear security regime. Criminal or intentional unauthorized acts need to be considered on an international level. Adversaries may seek to shield themselves and the evidence of their activities from detection by dividing those activities between different jurisdictions and by dispersing or concealing their resources over national boundaries. If effective arrangements for cooperation to address transboundary offences among States exist, adversaries may be less likely to protect themselves from detection and prosecution, potentially deterring them from attempting an act due to decreased likelihood of success.

7.2. Further guidance on international cooperation and assistance is provided in Refs [6] and [7]. A summary of relevant information provided by these publications on this topic is provided here, along with some considerations specific to material out of regulatory control.

7.3. States should seek to strengthen international cooperation and assistance to enhance preventive measures, including legal measures such as the assertion of jurisdiction over alleged offenders, prosecution and extradition, and internationally mutual legal assistance, discussed in the paragraphs to follow.

7.4. Paragraph 4.95 of Ref. [7] states that:

> "4.95. International instruments, such as the [Convention on the Physical Protection of Nuclear Material] CPPNM and the [International Convention for the Suppression of Acts of Nuclear Terrorism] ICSANT, require States Parties to assert jurisdiction over persons suspected of having committed offences involving nuclear and other radioactive materials, associated facilities or associated activities. This typically involves the apprehension

and arrest of suspects and detention until a decision is taken on jurisdiction over the alleged offence. This can be of particular importance for offences related to nuclear security, to prevent suspected offenders from evading prosecution by seeking a safe haven in a State other than that in which an offence has been committed or threatened."

7.5. Paragraph 4.98 of Ref. [7] states that:

"4.98. A fundamental principle of international criminal law, as reflected in instruments such as the CPPNM and the ICSANT, is that alleged offenders must either be prosecuted by States Parties or transferred through extradition to a State Party having jurisdiction over the offence. Extradition treaties between States Parties should include provisions for offences related to nuclear security. However, the CPPNM and the ICSANT contain provisions that make offences of the types defined in these Conventions extraditable from one State Party to another, even in the absence of a relevant extradition treaty between the affected States Parties. Implementing mechanisms, such as national laws and regulations governing criminal procedure, should provide for the extradition, where necessary, of persons alleged to have committed offences related to nuclear security, even in the absence of a relevant extradition treaty between the States involved."

7.6. In some cases, alleged offences related to nuclear security may have a transboundary aspect. For example, an alleged offender, forensic evidence or witnesses may be located in a State other than the one in which the offence is alleged to have occurred. The CPPNM and the ICSANT mandate the greatest measure of assistance for criminal proceedings regarding offences related to nuclear security, including the supply of evidence and expert witness, when necessary. States that have not already done so may wish to negotiate bilateral or multilateral mutual legal assistance treaties or agreements, particularly if they have close geographical connections or commercial relationships in the nuclear field [7].

7.7. In addition to such legal measures, international cooperation to improve the availability of nuclear forensics expertise and resources can assist States in establishing and implementing effective nuclear security systems and measures. In particular, international cooperation could support preventive measures by enhancing nuclear forensics capabilities through encouraging the establishment of a national nuclear forensics library and associated material databases, and directory of States with nuclear forensics assistance capabilities.

7.8. Paragraph 7.1 of Ref. [4] states that:

> "7.1. States should exchange accurate and verified information on *nuclear security events* in accordance with international obligations and national legislation, taking into account the designation of roles and responsibilities described in paragraph 3.11 and information security measures described in paragraphs 4.5–4.9."

Such shared information could be vital in assisting States in their efforts to prevent criminal or intentional unauthorized acts involving material out of regulatory control.

7.9. Reference [4] also recommends that the State should participate in and report relevant nuclear security events to applicable regional and international information databases in accordance with its international obligations and national legislation. One example is the IAEA's Incident and Trafficking Database[2].

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, Nuclear Security Systems and Measures for the Detection of Nuclear and Other Radioactive Material out of Regulatory Control, IAEA Nuclear Security Series No. 21, IAEA, Vienna (2013).

[2] https://www.iaea.org/resources/databases/itdb

[6] INTERNATIONAL ATOMIC ENERGY AGENCY, Developing a National Framework for Managing the Response to Nuclear Security Events, IAEA Nuclear Security Series No. 37-G, IAEA, Vienna (in preparation).
[7] INTERNATIONAL ATOMIC ENERGY AGENCY, Developing Regulations and Associated Administrative Measures for Nuclear Security, IAEA Nuclear Security Series No. 29-G, IAEA, Vienna (2018).
[8] INTERNATIONAL ATOMIC ENERGY AGENCY, The International Legal Framework for Nuclear Security, IAEA International Law Series No. 4, IAEA, Vienna (2011).
[9] INTERNATIONAL ATOMIC ENERGY AGENCY, INTERNATIONAL CRIMINAL POLICE ORGANIZATION–INTERPOL, Risk Informed Approach for Nuclear Security Measures for Nuclear and Other Radioactive Material out of Regulatory Control, IAEA Nuclear Security Series No. 24-G, IAEA, Vienna (2015).
[10] INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Forensics in Support of Investigations, IAEA Nuclear Security Series No. 2-G (Rev. 1), IAEA, Vienna (2015).
[11] INTERNATIONAL ATOMIC ENERGY AGENCY, INTERNATIONAL CRIMINAL POLICE ORGANIZATION–INTERPOL, UNITED NATIONS INTERREGIONAL CRIME AND JUSTICE RESEARCH INSTITUTE, Radiological Crime Scene Management, IAEA Nuclear Security Series No. 22-G, IAEA, Vienna (2014).
[12] INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Forensics in Support of Investigations, IAEA Nuclear Security Series No. 2-G (Rev. 1), IAEA, Vienna (2015).
[13] INTERNATIONAL ATOMIC ENERGY AGENCY, Security of Nuclear Information, IAEA Nuclear Security Series No. 23-G, IAEA, Vienna (2015).
[14] INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Culture, IAEA Nuclear Security Series No. 7, IAEA, Vienna (2008).
[15] INTERNATIONAL ATOMIC ENERGY AGENCY, Preventive and Protective Measures against Insider Threats, IAEA Nuclear Security Series No. 8, IAEA, Vienna (2008).

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

Renouf Publishing Co. Ltd
22-1010 Polytek Street, Ottawa, ON K1J 9J1, CANADA
Telephone: +1 613 745 2665 • Fax: +1 613 745 7660
Email: orders@renoufbooks.com • Web site: www.renoufbooks.com

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

OBJECTIVE AND ESSENTIAL ELEMENTS OF A STATE'S NUCLEAR SECURITY REGIME
IAEA Nuclear Security Series No. 20
STI/PUB/1590 (15 pp.; 2013)
ISBN 978–92–0–137810–1 Price: €20.00

NUCLEAR SECURITY RECOMMENDATIONS ON NUCLEAR AND OTHER RADIOACTIVE MATERIAL OUT OF REGULATORY CONTROL
IAEA Nuclear Security Series No. 15
STI/PUB/1488 (33 pp.; 2011)
ISBN 978–92–0–112210–0 Price: €23.00

NUCLEAR SECURITY SYSTEMS AND MEASURES FOR MAJOR PUBLIC EVENTS
IAEA Nuclear Security Series No. 18
STI/PUB/1546 (62 pp.; 2018)
ISBN 978-92-0-305317-4 Price: € 30.00

NUCLEAR SECURITY SYSTEMS AND MEASURES FOR THE DETECTION OF NUCLEAR AND OTHER RADIOACTIVE MATERIAL OUT OF REGULATORY CONTROL
IAEA Nuclear Security Series No. 21
STI/PUB/1613 (60 pp.; 2013)
ISBN 978-92-0-142910-0 Price: € 30.00

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

PREVENTIVE AND PROTECTIVE MEASURES AGAINST INSIDER THREATS
IAEA Nuclear Security Series No. 8
STI/PUB/1359 (25 pp.; 2008)
ISBN 978-92-0-109908-2 Price: € 20.00

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

Measures to prevent a nuclear security event are an integral part of a comprehensive nuclear security regime, and complement measures for detecting and responding to nuclear security events. This publication provides guidance to States and their competent authorities on the development and establishment of technical and administrative measures to prevent criminal or intentional unauthorized acts with nuclear security implications involving nuclear and other radioactive material out of regulatory control. These measures include deterrence by punishment and deterrence by denial, information security, promoting nuclear security culture and addressing the insider threat, including measures to verify the trustworthiness of personnel. This publication also provides guidance on international cooperation and assistance to help strengthen preventive measures.

INTERNATIONAL ATOMIC ENERGY AGENCY
VIENNA
ISBN 978–92–0–102619–4
ISSN 1816–9317