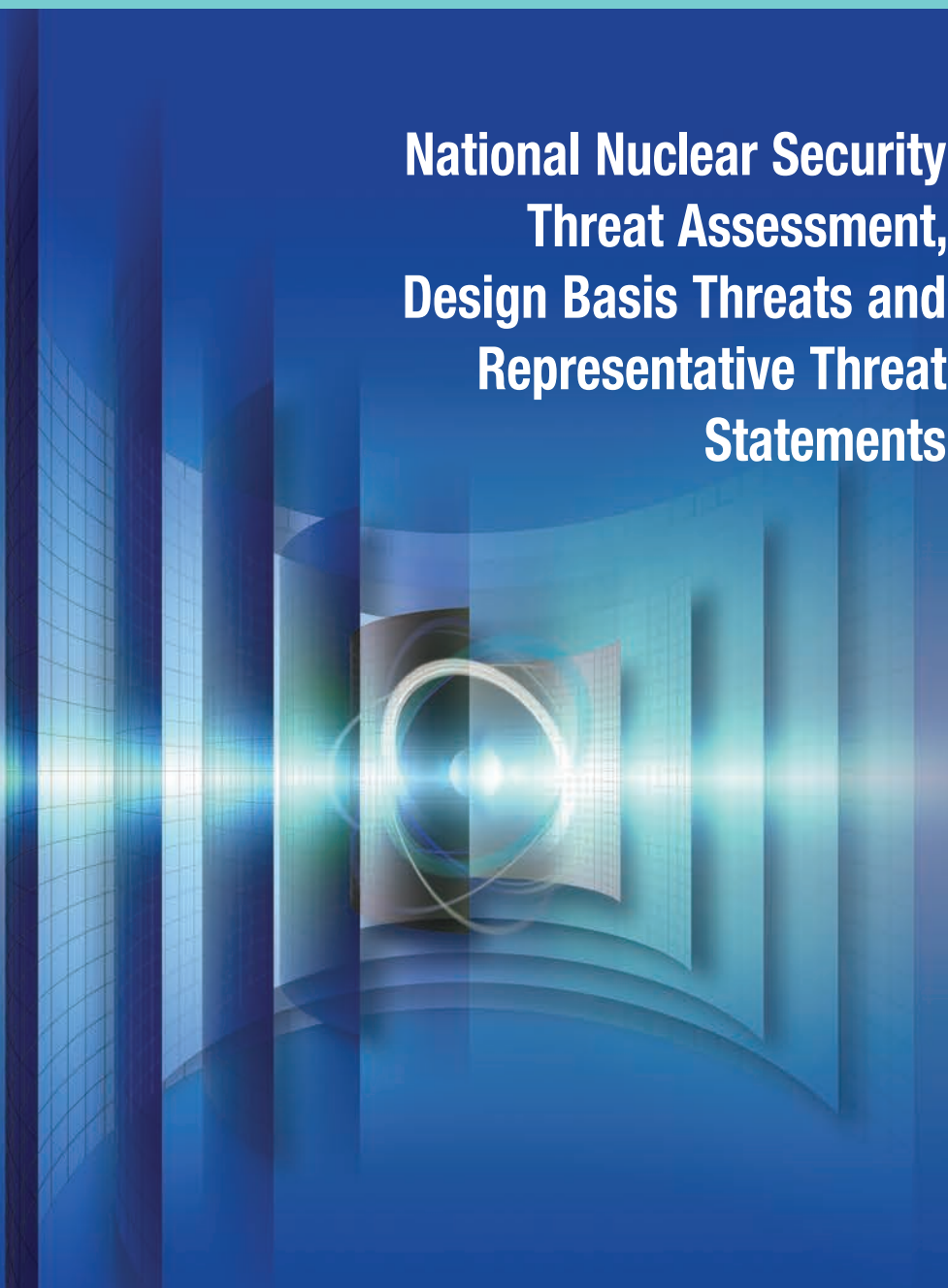
IAEA Nuclear Security Series No. 10-G (Rev. 1)

Implementing Guide

National Nuclear Security Threat Assessment, Design Basis Threats and Representative Threat Statements



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.

NATIONAL NUCLEAR SECURITY THREAT ASSESSMENT, DESIGN BASIS THREATS AND REPRESENTATIVE THREAT STATEMENTS

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
SAMOA
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. 10-G (Rev. 1)

NATIONAL NUCLEAR SECURITY THREAT ASSESSMENT, DESIGN BASIS THREATS AND REPRESENTATIVE THREAT STATEMENTS

IMPLEMENTING GUIDE

INTERNATIONAL ATOMIC ENERGY AGENCY
VIENNA, 2021

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
May 2021
STI/PUB/1926

IAEA Library Cataloguing in Publication Data

Names: International Atomic Energy Agency.
Title: National nuclear security threat assessment, design basis threats and representative threat statements. / International Atomic Energy Agency.
Description: Vienna : International Atomic Energy Agency, 2021. | Series: IAEA nuclear security series, ISSN 1816–9317 ; no. 10-G (Rev. 1) | Includes bibliographical references.
Identifiers: IAEAL 21-01391 | ISBN 978-92-0-131020-0 (paperback : alk. paper) | ISBN 978-92-0-131120-7 (pdf) | ISBN 978-92-0-131220-4 (epub) | ISBN 978-92-0-131320-1 (mobipocket)
Subjects: LCSH: Risk assessment. | Nuclear facilities — Security measures. | Radioactive substances — Security measures.
Classification: UDC 621.039.58 | STI/PUB/1926

FOREWORD

by Rafael Mariano Grossi
Director General

The IAEA Nuclear Security Series provides international consensus guidance on all aspects of nuclear security to support States as they work to fulfil their responsibility for nuclear security. The IAEA establishes and maintains this guidance as part of its central role in providing nuclear security related international support and coordination.

The IAEA Nuclear Security Series was launched in 2006 and is continuously updated by the IAEA in cooperation with experts from Member States. As Director General, I am committed to ensuring that the IAEA maintains and improves upon this integrated, comprehensive and consistent set of up to date, user friendly and fit for purpose security guidance publications of high quality. The proper application of this guidance in the use of nuclear science and technology should offer a high level of nuclear security and provide the confidence necessary to allow for the ongoing use of nuclear technology for the benefit of all.

Nuclear security is a national responsibility. The IAEA Nuclear Security Series complements international legal instruments on nuclear security and serves as a global reference to help parties meet their obligations. While the security guidance is not legally binding on Member States, it is widely applied. It has become an indispensable reference point and a common denominator for the vast majority of Member States that have adopted this guidance for use in national regulations to enhance nuclear security in nuclear power generation, research reactors and fuel cycle facilities as well as in nuclear applications in medicine, industry, agriculture and research.

The guidance provided in the IAEA Nuclear Security Series is based on the practical experience of its Member States and produced through international consensus. The involvement of the members of the Nuclear Security Guidance Committee and others is particularly important, and I am grateful to all those who contribute their knowledge and expertise to this endeavour.

The IAEA also uses the guidance in the IAEA Nuclear Security Series when it assists Member States through its review missions and advisory services. This helps Member States in the application of this guidance and enables valuable experience and insight to be shared. Feedback from these missions and services, and lessons identified from events and experience in the use and application of security guidance, are taken into account during their periodic revision.

I believe the guidance provided in the IAEA Nuclear Security Series and its application make an invaluable contribution to ensuring a high level of nuclear security in the use of nuclear technology. I encourage all Member States to promote and apply this guidance, and to work with the IAEA to uphold its quality now and in the future.

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. The Nuclear Security Fundamentals set out the objective of a nuclear security regime and its essential elements [1]. The Nuclear Security Recommendations indicate what a nuclear security regime should address regarding the following material and associated facilities:

(a) Nuclear material and nuclear facilities [2];
(b) Radioactive material and associated facilities [3];
(c) Nuclear and other radioactive material out of regulatory control [4].

1.2. The identification and assessment of threats provides an essential basis for the selection, design and implementation of nuclear security measures. For nuclear material and other radioactive material that is under regulatory control, and associated facilities and associated activities, the results of this identification and assessment are expressed as a design basis threat or a representative threat statement describing the intentions and capabilities of potential adversaries against which the materials, associated facilities and associated activities are to be protected.

1.3. This publication is a revision of IAEA Nuclear Security Series No. 10, Development, Use and Maintenance of the Design Basis Threat[1], intended to take into account developments in the field and to ensure consistency in terminology with Refs [1–4], which were published after 2009.

1.4. In addition, the scope of this publication has been broadened to clarify the use of an alternative approach to the design basis threat, to explain how to develop application specific design basis threats and to better address threats involving cyber-attacks [5].

[1] INTERNATIONAL ATOMIC ENERGY AGENCY, Development, Use and Maintenance of the Design Basis Threat, IAEA Nuclear Security Series No. 10, IAEA, Vienna (2009).

OBJECTIVE

1.5. The objective of this publication is to provide a step by step methodology for the conduct of a national nuclear security threat assessment, including both physical and computer security aspects, and for the development, use and maintenance of design basis threats and representative threat statements. This includes the following steps:

(a) Defining the roles and responsibilities of the State, competent authorities (including the regulatory body[2]) and operators;
(b) Identifying and assessing threats related to nuclear security;
(c) Developing threat statements such as design basis threats and representative threat statements using the results of the national nuclear security threat assessment;
(d) Using design basis threats and/or representative threat statements to develop nuclear security systems and measures as well as nuclear security requirements;
(e) Maintaining the validity of the national nuclear security threat assessment and its documentation;
(f) Maintaining the validity of design basis threats and representative threat statements.

1.6. This publication is intended for use by States, competent authorities (including the regulatory body), relevant technical and scientific support organizations, and the operators of facilities and activities associated with nuclear material and other radioactive material, including shippers and carriers.

SCOPE

1.7. The concept and methodology described in this publication apply to the conduct of a national nuclear security threat assessment, including both physical and computer security aspects, and to the development, use and maintenance of design basis threats and representative threat statements for protecting nuclear material and other radioactive material under regulatory control as well as associated facilities and associated activities.

---

[2] Some States have multiple regulatory bodies responsible for the nuclear security of nuclear material and other radioactive material as well as associated facilities and associated activities. In this publication, the term ‘regulatory body’ refers to the body (or bodies) relevant in the given context.

1.8. Guidance on developing a risk informed approach and conducting threat and risk assessments as the basis for the nuclear security of nuclear and other radioactive material out of regulatory control is not provided in this publication; guidance on this topic can be found in IAEA Nuclear Security Series No. 24-G, Risk Informed Approach for Nuclear Security Measures for Nuclear and Other Radioactive Material out of Regulatory Control [6].

STRUCTURE

1.9. Following this introduction, Section 2 addresses the national nuclear security threat assessment as part of the application of a risk informed approach. Section 3 provides an overview of the process of conducting a national nuclear security threat assessment and the development, use, and maintenance of the validity of that threat assessment and its documentation as well as design basis threats and representative threat statements. Section 4 outlines the roles and responsibilities of the organizations involved in the national nuclear security threat assessment process. Section 5 provides more detailed guidance on how to conduct a national nuclear security threat assessment. Section 6 describes the development of design basis threats and representative threat statements, and Section 7 provides guidance on their use. Section 8 provides guidance on maintaining the validity of the national nuclear security threat assessment and its documentation and the threat statements. A model design basis threat is provided in the Appendix to this publication.

2. NATIONAL NUCLEAR SECURITY THREAT ASSESSMENT AND THE USE OF A RISK INFORMED APPROACH

2.1. International conventions and IAEA Nuclear Security Series guidance underscore the importance of threat assessment and the use of a risk informed approach to nuclear security. Notably, Fundamental Principle G (Threat) of the Convention on the Physical Protection of Nuclear Material, as amended [7, 8], and Ref. [2] state that "**The State's physical protection should be based on the State's current evaluation of the threat.**"

2.2. Essential Element 9 of Ref. [1] is as follows:

> "A *nuclear security regime* uses risk informed approaches, including in the allocation of resources for *nuclear security systems* and *nuclear security measures* and in the conduct of nuclear security related activities that are based on a *graded approach* and *defence in depth*, which take into account the following:
>
> (a) The State's current assessment of the *nuclear security threats*, both internal and external;
> (b) The relative attractiveness and vulnerability of identified *targets* to *nuclear security threats*;
> (c) Characteristics of the *nuclear material*, *other radioactive material*, *associated facilities* and *associated activities*;
> (d) Potential harmful consequences from criminal or intentional unauthorized acts involving or directed at *nuclear material*, *other radioactive material*, *associated facilities*, *associated activities*, *sensitive information or sensitive information assets*, and other acts determined by the State to have an adverse impact on nuclear security."

2.3. Further, paragraph 3.10 of Ref. [2] states:

> "The State should define requirements — based on the *threat assessment* or *design basis threat* — for the physical protection of *nuclear material* in use, in storage, and during *transport*, and for *nuclear facilities* depending on the associated consequences of either *unauthorized removal* or *sabotage*."

And paras 3.17 and 3.18 of Ref. [3] state:

> "The State should assess its national *threat* for *radioactive material*, *associated facilities* and *associated activities*. The State should periodically review its national *threat*, and evaluate the implications of any changes in the *threat* for the design or update of its *nuclear security regime*…. The *regulatory body* should use the results of the *threat assessment* as a common basis for determining security requirements for *radioactive material* and for periodically evaluating their adequacy."

2.4. The following subsections address in more detail several issues related to national nuclear security threat assessment using a risk informed approach; adversaries and their attributes and characteristics; and information security.

RISK INFORMED APPROACH AND THREAT STATEMENTS

2.5. Essential Element 9 of a nuclear security regime [1] is the use of risk informed approaches, including in the allocation of resources for nuclear security systems and nuclear security measures and in the conduct of nuclear security related activities that are based on a graded approach and defence in depth. Taking a risk informed approach to nuclear security should involve consideration of the threat, the attractiveness and vulnerability of potential targets, and the potential consequences resulting from malicious acts.

2.6. Paragraph 3.41 of Ref. [2] recommends that "The State should ensure that the State's *physical protection regime* is capable of establishing and maintaining the risk of *unauthorized removal* and *sabotage* at acceptable levels through risk management." Risk management should include a periodic re-evaluation of the threat and the potential consequences of malicious acts and should ensure that appropriate nuclear security systems and measures are put in place to prevent or reduce the likelihood of a successful malicious act.

2.7. A national nuclear security threat assessment is an evaluation of the existing nuclear security related threats, including both physical and computer security threats, to determine the attributes and characteristics of potential adversaries. This national nuclear security threat assessment process makes use of global, regional and national sources of information.

2.8. The results of the national nuclear security threat assessment process are recorded in the national nuclear security threat assessment documentation and can be used to develop threat statements. A threat statement sets out the attributes and characteristics of credible potential adversaries against whom activities and facilities associated with nuclear material and other radioactive material are to be protected.

2.9. An assessment of the current threat related to nuclear security, provided in threat statements such as design basis threats and representative threat statements, can be used to facilitate a risk informed approach to nuclear security and risk management at individual facilities and activities. Threat statements can assist the design and evaluation of nuclear security systems and measures that take account of the potential consequences of a successful malicious act.

2.10. States may choose to develop threat statements in the form of either design basis threats or representative threat statements, or may use both along

with a suitable regulatory approach[3] for different types of facility and activity. A representative threat statement could be used to develop regulatory requirements emphasizing prescriptive requirements for a particular subset of lower consequence materials or facilities to be protected, while a design basis threat could be defined for use in implementing regulatory requirements emphasizing a performance based approach to protect a specific higher consequence facility or activity. For example, a representative threat statement might be used by a competent authority to develop prescriptive regulatory requirements for the protection of Category 1 radioactive sources in use and storage, while a design basis threat might be used by an operator to design and evaluate a nuclear security system to satisfy performance based requirements to provide effective protection against attack scenarios for a specific Category 1 radioactive source.

2.11. On the basis of the results of the national nuclear security threat assessment, States may choose to define different representative threat statements for different categories of nuclear material and other radioactive material and for different types of facility and activity (e.g. Category 1 radioactive sources, irradiators, transport of radioactive material), for different adversary objectives (e.g. theft, sabotage) and for assets that might be particularly targeted by cyber-attacks (e.g. sensitive information or computer based systems for nuclear safety, nuclear security, nuclear material accounting and control or emergency response).

2.12. Similarly, States may choose to define different design basis threats based on the national nuclear security threat assessment that are applicable to materials in specific facilities or activities that represent higher risks (e.g. research reactors, transport of spent nuclear fuel). These design basis threats would take account of details of the facilities or activities (e.g. design, location), policy considerations (e.g. the degree of conservatism necessary to maintain public confidence), and the capabilities and resources of the State and the operator.

2.13. Some threats identified during the national nuclear security threat assessment process are likely to be excluded from design basis threats or representative threat statements, as they will be considered to be beyond the design basis. Protection against these threats, even if the operator's nuclear security system provides some inherent protection, needs to be considered in the State's contingency plan by coordinating a State response with the operator's contingency response plan. Although the State should develop measures to counter these threats, the operator

[3] More detailed information on prescriptive and performance based regulatory approaches can be found in Refs [2, 3, 8, 9].

might still have a role in assisting the State either to protect against these nuclear security threats or to mitigate their consequences.

2.14. Decisions regarding nuclear security risk are based on current threats of concern to a State, the possibility of new and emerging threats, and decisions regarding how to balance conservatism against costs and operational impact. Such decisions might also involve consideration of international and regional threats, political and financial factors, the public's perception of risk, and lessons identified from previous nuclear security threat assessments.

POTENTIAL ADVERSARIES AND THEIR ATTRIBUTES AND CHARACTERISTICS

2.15. Potential adversaries could include terrorists, other criminals and extremists who might seek to acquire and use nuclear material or other radioactive material to build nuclear explosive devices, radiological dispersal devices or radiation exposure devices. Such adversaries might also seek to sabotage facilities in which nuclear material or other radioactive material is used or stored or the transport of such material.

2.16. A potential adversary is characterized by motivation, intent and capabilities. For example, motivation could be financial, political or ideological, or could result from disgruntlement or coercion. Intent could include unauthorized possession of nuclear material or other radioactive material, acquisition of sensitive information or sensitive information assets, damage through sabotage, or the creation of public embarrassment for the operator of a facility or activity or for the State. The capabilities of an adversary depend on characteristics such as the number of individuals involved, the level of organization and coordination, and whether insiders are involved. Capabilities also include the individuals' and organization's abilities, assets and relevant skills, such as tactics, weapons, explosives, transport, physical and computer related tools, knowledge of software vulnerabilities, and level of access to a facility or its computer based systems.

2.17. Adversaries might include insiders [9]: individuals with authorized access to 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. Adversaries might seek to become insiders by acquiring authorized access to a

facility (e.g. to be employed or hired as contractors) to exploit this access later, or existing personnel might become insider threats by developing or acquiring an intention to commit or facilitate malicious acts.

2.18. The potential for collusion between insiders and external adversaries should also be considered. For example, an insider might carry out an unauthorized act, physically or using computer related means, to facilitate the commission of a malicious act by an external adversary.

2.19. States should consider not only potential malicious acts that involve physical access to the facility or activity but also those that use cyber-attack. Such attacks might be aimed at computer based systems used for nuclear safety (including instrumentation and control systems), nuclear material accounting and control, nuclear security or emergency response (including communication and alarm systems). Adversaries might also undertake a blended attack, where an attack on a computer based system is conducted in combination with a physical attack, such as an armed intrusion using electronically falsified access credentials with the intention of sabotage or theft of material.

2.20. The potential for both insiders and external adversaries to undertake acts resulting in a compromise of the confidentiality, integrity and availability of information in computer based systems should be considered. Such acts could be facilitated either by insiders or by external adversaries through a remote cyber-attack. The introduction of malware to computer based systems through the supply chain should also be considered.

2.21. The potential for stand-off attacks should also be considered. A stand-off attack could involve devices operated from a distance, such as drones, missiles or directed energy weapons.

INFORMATION SECURITY CONSIDERATIONS

2.22. All credible information related to threats, including national intelligence and other sensitive information, should be considered in the development and maintenance of threat statements. Some of this information and many of its sources need to be protected. A design basis threat or a representative threat statement that is used in the design and evaluation of nuclear security systems should be protected as sensitive information, namely information, in whatever form, including software, the unauthorized disclosure, modification, alteration, destruction or denial of use of which could compromise nuclear security.

2.23. Detailed guidance on protecting sensitive nuclear security information can be found in IAEA Nuclear Security Series No. 23-G, Security of Nuclear Information [10].

3. OVERVIEW OF THE PROCESS OF DEVELOPMENT, USE AND MAINTENANCE OF THE VALIDITY OF THE NATIONAL NUCLEAR SECURITY THREAT ASSESSMENT AND ITS DOCUMENTATION, DESIGN BASIS THREATS, AND REPRESENTATIVE THREAT STATEMENTS

3.1. The process of development, use and maintenance of the validity of the national nuclear security threat assessment and its documentation as well as design basis threats and representative threat statements is shown in Fig. 1 and consists of five steps:

(1) Definition of roles and responsibilities;
(2) Conduct and documentation of the national nuclear security threat assessment;
(3) Development of design basis threats and/or representative threat statements;
(4) Use of the design basis threats and/or representative threat statements in the regulatory framework;
(5) Maintenance of the validity of the national nuclear security threat assessment, design basis threats and/or representative threat statements.

3.2. During step 1, the roles and responsibilities in this process should be defined by the State for the regulatory body and other competent authorities, as well as for operators, in accordance with the legal and regulatory framework of the State.

3.3. During step 2 — the conduct of the national nuclear security threat assessment — the competent authority responsible for performing that assessment, together with other relevant competent authorities, should collect intelligence and other threat information, including information from open sources, past nuclear security events and security events non-nuclear-related activities. The competent authorities should analyse the collected information and evaluate its potential relevance to nuclear security. The competent authorities should also evaluate the credibility of the threat information and screen out information that is not credible.

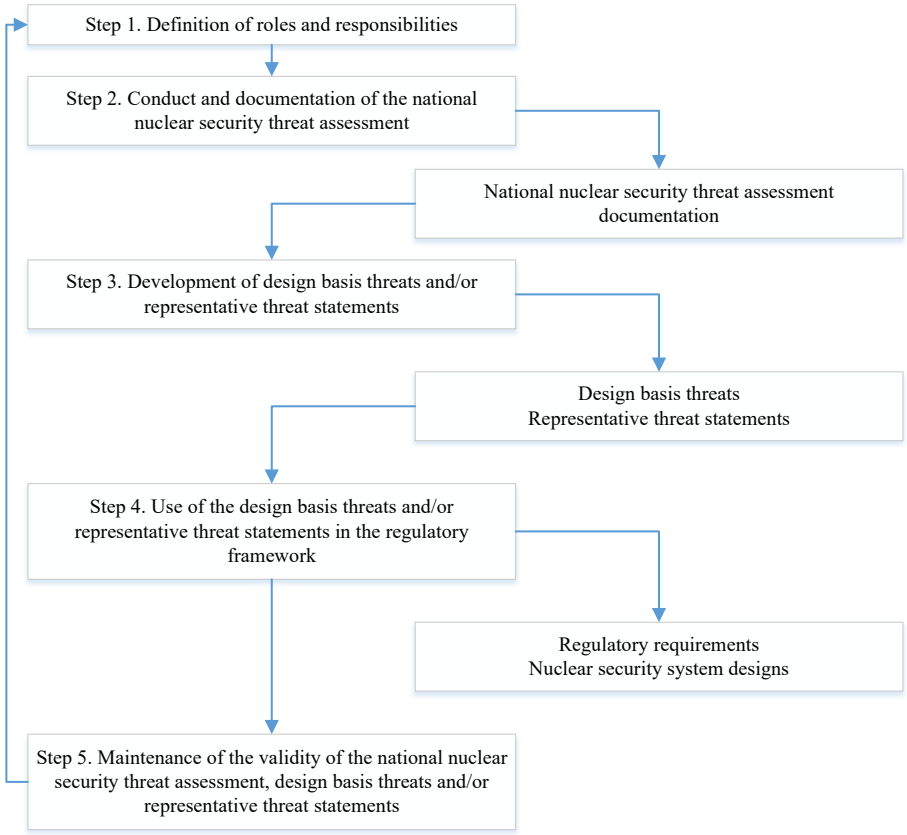


FIG. 1. Process for development, use and maintenance of the validity of the national nuclear security threat assessment and its documentation as well as design basis threats and representative threat statements.

On the basis of the remaining information, the competent authorities should identify potential adversaries and characterize the likelihood of possible adversary actions and the attributes and characteristics of the potential adversaries. Finally, the competent authorities should evaluate whether specific adversary capabilities are relevant to potential targets. The results of this process should be recorded in the national nuclear security threat assessment documentation.

3.4. In step 3, using the results of the national nuclear security threat assessment, the competent authority responsible for developing the threat statements, in agreement with other competent authorities, as appropriate, should develop material, facility or activity specific design basis threats and/or develop representative threat statements applicable to different types and categories

of nuclear material, other radioactive material, associated facilities and associated activities.

3.5. In step 4, the regulatory body's actions will depend on the regulatory approach followed:

(a) For a performance based approach, the regulatory body should disseminate design basis threats to relevant operators, who should then develop facility specific attack scenarios and use these scenarios to design nuclear security systems to counter the design basis threats and to meet the nuclear security objectives established in the State's legal framework.
(b) For a prescriptive approach, the regulatory body should develop regulatory requirements based on the representative threat statements and the nuclear security objectives established in the State's legal framework, and should ensure that operators implement nuclear security systems and measures in compliance with these requirements.
(c) For a combined approach, the regulatory body should include elements drawn from both the performance based and the prescriptive approaches.

3.6. In step 5, the competent authorities should review and, if appropriate, revise the national nuclear security threat assessment and its documentation, the design basis threats and/or the representative threat statements. Determinations of whether to revise these documents may be made according to a defined review cycle, in the event of a change in the threat environment and/or to incorporate lessons identified following a nuclear security event. In the case of new or emerging threats needing immediate consideration, the competent authorities, together with the operators, should take the necessary actions to manage these threats, if necessary separately from the existing design basis threats or representative threat statements, pending their revision. This process should be integrated into the State's nuclear security regime.

3.7. In Sections 4–8, each of these steps is addressed in more detail, including more specific guidance for States, competent authorities and operators in putting these steps into practice.

4. ROLES AND RESPONSIBILITIES

4.1. The State, relevant competent authorities (including the regulatory body) and operators have roles and responsibilities related to the national nuclear security threat assessment and the development of design basis threats and/or representative threat statements. These roles and responsibilities should be clearly defined before beginning work on the national nuclear security threat assessment.

STATE

4.2. The State is responsible for assigning, coordinating and supervising the competent authorities leading and participating in the following:

(a) Conducting a national nuclear security threat assessment and maintaining the validity of the assessment and its documentation;
(b) Developing and maintaining the validity of design basis threats and/or representative threat statements;
(c) Using the design basis threats and/or representative threat statements.[4]

4.3. A nuclear security event might give rise to a nuclear or radiological emergency. Paragraph 4.22 of IAEA Safety Standards Series No. GSR Part 7, Preparedness and Response for a Nuclear or Radiological Emergency [11], states that "The government shall ensure that the hazard assessment includes consideration of the results of threat assessments made for nuclear security purposes".

COMPETENT AUTHORITIES

4.4. All relevant competent authorities should be involved in the national nuclear security threat assessment process to enable as full a range of credible threats as possible to be identified and considered in the assessment.

4.5. Relevant expertise for identifying and assessing credible threats might exist in several organizations of a State, such as intelligence organizations (including security agencies), ministries of the interior and foreign affairs, computer security

[4] The State may assign different competent authorities to lead the different processes; however, the roles and responsibilities have to be clearly defined and the coordination mechanism among competent authorities has to be well established and exercised.

centres, law enforcement agencies, military services, the regulatory body for nuclear security and other relevant organizations. Such organizations will have staff who are familiar with the processes of collecting and analysing information and skilled in making the necessary judgements. In addition, such organizations may have access to particular sources of information, including information from contacts with other States or regional or international organizations.

4.6. The responsibilities of competent authorities might include the following:

(a) Collecting and collating information on potential threats;
(b) Analysing available threat information to ensure its credibility;
(c) Sharing relevant threat information with other competent authorities;
(d) Coordinating with other competent authorities to determine the subset of credible threats that are relevant to nuclear security;
(e) Cooperating in the threat assessment process, identifying potential adversaries and documenting the national nuclear security threat assessment;
(f) Developing design basis threats and/or representative threat statements on the basis of the results of the national nuclear security threat assessment;
(g) Maintaining the validity of the national nuclear security threat assessment and its documentation and of the design basis threats and representative threat statements;
(h) Sharing the national nuclear security threat assessment documentation, as appropriate, with relevant emergency response organizations[5];
(i) Considering the national nuclear security threat assessment when performing hazard assessment [12];
(j) Implementing information security considerations.

4.7. Some competent authorities (e.g. national and local police authorities, armed forces, border control authorities, customs authorities) have much broader areas of responsibility within a State, which may include playing a role in protecting against threats related to nuclear security, either on their own or in conjunction with others. Some competent authorities might also have responsibilities for providing support to the operator during a nuclear security event. Such competent authorities should be involved or consulted in the process to develop design basis threats and/or representative threat statements as well as regulatory requirements.

[5] As response in the area of nuclear security refers to response to a nuclear security event, the term ‘emergency response organization’ is used in this publication to avoid misinterpretation. ‘Emergency response organization’ is used in line with the definition established in GSR Part 7 [11] for ‘response organization’.

4.8. The regulatory body for nuclear security, in coordination with other competent authorities as appropriate, is responsible for the following tasks:

(a) Developing prescriptive requirements for operators on the basis of representative threat statements and/or providing the design basis threats and performance based requirements to operators to be used for developing attack scenarios and designing nuclear security systems and measures;
(b) Ensuring that operators review appropriately, and revise as necessary, security and emergency arrangements, taking account of the developed attack scenarios and the results of threat assessments.

OPERATORS

4.9. Operators should implement nuclear security systems and measures that achieve one or both of the following:

(a) Meet the regulatory requirements, including relevant prescriptive requirements developed on the basis of the representative threat statement;
(b) Protect against a range of facility or activity specific attack scenarios developed on the basis of the design basis threat.

4.10. In some cases, operators' knowledge of the financial, operational and safety impact of specific nuclear security measures might influence the division of responsibility between operators and competent authorities for nuclear security measures. Operators' input, either formal or informal, should be taken into consideration in developing design basis threats, representative threat statements and regulatory requirements. Specifically, operators should provide the following:

(a) Input on facility and activity specific threats related to nuclear security that should be considered for inclusion in design basis threats and/or representative threat statements;
(b) Feedback to the regulatory body, if considered necessary and requested within the legal and regulatory framework, concerning the financial, operational, security and safety impact of potential decisions regarding design basis threats, representative threat statements and/or regulatory requirements;
(c) Supporting information, if considered necessary and requested within the legal and regulatory framework, regarding attack scenarios and adversary attributes and characteristics derived from physical attacks, cyber-attacks and blended attacks that might have occurred.

5. CONDUCT OF A NATIONAL NUCLEAR SECURITY THREAT ASSESSMENT

5.1. The aim of the national nuclear security threat assessment is to provide an assessment of credible threats, describing the motivations, intentions and capabilities of potential adversaries. It is not intended to describe specific attack scenarios.

5.2. A sufficiently detailed and specific description of potential threats can be used to determine the level of protection that is appropriate and sufficient for nuclear material and other radioactive material, as well as associated facilities and associated activities, and provides a basis on which a nuclear security system can be effectively designed.

5.3. During the national nuclear security threat assessment process, information on existing threats and credible potential threats is collected and analysed, and information on the attributes and characteristics of potential adversaries is compiled and aggregated. The output of the national nuclear security threat assessment is a detailed description of the threats related to nuclear security and is referred to as the national nuclear security threat assessment documentation. All relevant organizations with different areas of expertise and responsibility should work closely together to collect and analyse this information. Close working relationships between all relevant organizations are needed for the national nuclear security threat assessment to be effective. Records should be kept of the conduct of the national nuclear security threat assessment to support the periodic review and revision process for maintaining the assessment's validity.

5.4. The roles and responsibilities for performing the actions described in detail in the following subsections, or ensuring that they are completed, are described in Section 4.

INPUT: COLLECTION OF RELEVANT THREAT INFORMATION

5.5. The first task in the national nuclear security threat assessment process is to collect and collate comprehensive information concerning all potential adversaries, their motivations, intentions and capabilities. This information might include both sensitive and non-sensitive information and should address both physical and computer related capabilities and both potential insider and external adversaries.

5.6. Potential sources of information should be identified, and the relevant information should be collected. Consideration should be given to the sensitivity of the information to ensure that the appropriate security is applied both to the information and to its sources. If not already in place, a mechanism to share threat information between all relevant organizations in the threat assessment process should be established and should provide for the security of sensitive information. Written agreements may be needed to establish arrangements for sharing threat information.

5.7. Intelligence and other sources of information relating to threats might provide sufficient information to design a nuclear security system. However, owing to the limitations of intelligence and the dynamic nature of threats, nuclear security systems designed only for currently known threats might not be effective against future threats.

5.8. The national nuclear security threat assessment should not rely on a single source. The use of intelligence and threat information from multiple sources combined into a single coherent assessment will result in the most comprehensive, reliable and robust national nuclear security threat assessment. All credible and relevant national and international sources of intelligence and threat information should be considered in the collection of data.

5.9. Sources of information and intelligence should include, as appropriate, intelligence organizations (including security agencies), computer and information security organizations, law enforcement agencies, the International Criminal Police Organization, the regulatory body for nuclear security and other competent authorities, customs and border agencies, the military services, shippers and carriers, official government reporting, incident reporting by operators, databases maintained by international organizations, and other open sources.

5.10. Technical and scientific support organizations, commercial entities and open databases could be used as sources of additional information about potential threats, especially threats to computer security. Operators might also have information on such threats and their attributes and characteristics.

5.11. Relevant information on the attributes and characteristics of potential threats to other types of critical infrastructure should be considered as possible analogues for nuclear security threats.

5.12. Information should be collected on recent and historical nuclear security events (including those involving computer security), if applicable.

5.13. The information collection task should aim to identify all relevant types of threat, including the following:

(a) Global, national and local threats;
(b) Physical attacks, cyber-attacks and blended attacks;
(c) Insider threats, external adversaries and threats resulting from the collusion of insider and external adversaries.

5.14. Credible adversary capabilities should also be considered, even if they have not been demonstrated. Consideration should also be given to potential persistent adversaries who plan multistage attacks over extended periods of time, possible technological developments, the potential frequency of attacks and the possibility of attacks on the supply chain (e.g. hardware and/or modified software being compromised before delivery).

ANALYSIS OF RELEVANT THREAT INFORMATION

5.15. Once the collection of relevant threat information is complete, this information should be collated using information management tools to index and sort it before beginning the analysis. Effectively organizing all intelligence and other available information ensures that all necessary information is available to be analysed. The organized information should then be analysed to identify and document the credible motivations, intentions and capabilities of potential adversaries related to nuclear security.

5.16. The comprehensiveness of the information collected and the accuracy of the analysis will affect the confidence that can be placed in the design basis threats and/or representative threat statements resulting from the process.

5.17. Information collection and analysis are likely to be iterative. Analysis will often demonstrate the need for more information or identify previously unknown or emerging threats on which information is needed. Analysis of the threat information involves evaluating what is known on the basis of that information and making a judgement about how the attributes and characteristics of adversaries might change in the future.

5.18. During the analysis process, the credibility of the information used in the national nuclear security threat assessment should be evaluated. In general, when assessing the credibility of threat information, it is important to consider both the trustworthiness and the technical expertise of the source of the information.

Law enforcement and intelligence agencies, including security agencies, should indicate how much confidence can, in their judgement, be attached to the information they provide. Open source information (e.g. from public media or social networks) that is easily available might be useful, but its accuracy should be carefully considered. The degree of confidence in any information should be taken into account when deciding how that information will be used later. During evaluation of the credibility of information, some information might also be excluded as not being relevant to the analysis and additional information gaps might be identified (e.g. if information that appeared to fill a gap is judged not to be sufficiently credible).

5.19. The national nuclear security threat assessment process should include consideration of at least the following attributes and characteristics of adversaries for each identified threat (although there might not be data available for all the listed attributes and characteristics for all threats):

(a) Motivations of the adversary, which might be, for example, political, financial, ideological and/or personal (e.g. as a result of disgruntlement or coercion);
(b) Persistence of the adversary;
(c) Dedication of the adversary, including level of risk aversion and willingness to put their own life at risk;
(d) Demonstrated capabilities of the adversary, including characterization of past nuclear security events that have occurred;
(e) Intentions of the adversary, such as sabotage of material or of a facility, unauthorized removal of nuclear or other radioactive material, theft of sensitive information;
(f) Number of adversaries in a group, including the attack force, coordination personnel and support personnel;
(g) Types and numbers of weapons available to the adversary;
(h) Types and quantities of explosives available to the adversary, whether acquired in the form of devices or improvised, and the sophistication of trigger mechanisms;
(i) Tools available to the adversary, such as mechanical, thermal or electromagnetic equipment, manual powered or electronic equipment, or communications equipment;
(j) Transport available to the adversary, including type (public, private), mode (land, sea, air), and vehicle types and numbers;
(k) Likely modes of access to targets, both physical and computer related;
(l) Influence over operations and/or personnel;

(m) Potential adversary tactics, such as stealth, deception, force, reconnaissance activities or social engineering;
(n) Planning skills of the adversary, such as the ability to plan a diversion or coordinate simultaneous attacks by smaller groups;
(o) Practical skills, knowledge and experience available to the adversary, including skills in engineering, use of explosives, chemicals and communications, and military or paramilitary experience;
(p) Access to computer and computer security skills, such as knowledge of control systems, computer security measures, reverse engineering and vulnerability testing, communication protocol engineering, social engineering, source obfuscation, redirection of attribution, network surveillance, and traffic manipulation;
(q) Knowledge of or access to information about targets, such as target characteristics, facility layout, site plans and procedures, security plans, security measures, safety and radiation protection measures, facility and transport operations, possible entry points for cyber-attacks, vendor support procedures and plans, and supply chain and procurement procedures;
(r) Sources and amounts of funding, and how they are accessed;
(s) Potential for exploitation of insiders (including by collusion, coercion or deception), possible number of insiders and whether they are passive or active, violent or non-violent;
(t) Adversaries' support structures, such as the presence or absence of local sympathizers, support organizations or logistical support.

OUTPUT: NATIONAL NUCLEAR SECURITY THREAT ASSESSMENT DOCUMENTATION

5.20. The output of the national nuclear security threat assessment process is recorded in the national nuclear security threat assessment documentation, which describes the overall threat environment for nuclear security and all known credible threats that should be taken into consideration. The supporting analytical narrative should provide as much detail as possible about these threats and the credibility of the information.

5.21. Both the national nuclear security threat assessment documentation and the details of intelligence sources are typically protected as sensitive information.

6. DEVELOPMENT OF DESIGN BASIS THREATS AND REPRESENTATIVE THREAT STATEMENTS

6.1. As described in Section 5, the national nuclear security threat assessment process results in the production of the national nuclear security threat assessment documentation. Using the national nuclear security threat assessment as a basis, threat statements, in the form of design basis threats and/or representative threat statements, can be developed. These statements describe credible adversaries against whom facilities and activities using or storing nuclear or other radioactive material are to be protected, as well as the attributes and characteristics of these adversaries.

REGULATORY APPROACHES AND THREAT STATEMENTS

6.2. Three regulatory approaches are possible when regulating the operation of a facility or activity: the performance based approach, the prescriptive approach and the combined approach. In the performance based approach, the operator needs to design and implement a nuclear security system to meet the nuclear security objectives defined by the State, taking account of the design basis threat disseminated by the regulatory body, the level of effectiveness specified for protecting against malicious acts and the provision of contingency responses. In the prescriptive approach, the regulatory body, without sharing threat information with the operators, establishes specific nuclear security measures it has determined are necessary to meet the defined nuclear security objectives for each category of nuclear material or other radioactive material and each level of potential radiological consequences. These provide a set of ‘baseline’ measures for the operator to implement. The combined approach includes elements from both the prescriptive and performance based approaches. Further detailed information on each of these regulatory approaches can be found in Refs [13, 14].

6.3. As indicated in para. 2.10, representative threat statements are often used to develop prescriptive regulatory requirements for a specified subset of materials, activities and/or facilities to be protected, while design basis threats are often defined for specific facilities or activities. The regulatory body should adopt the regulatory approach and accompanying choice of representative threat statements and/or design basis threats that best suit the State’s needs, consistent with its legal and regulatory framework. The regulatory body’s chosen approach should be approved by the State, since the choice will likely have resource implications for the regulatory body and operators.

6.4. The use of a design basis threat in a performance based regulatory approach as the basis for designing nuclear security systems and measures can lead to an efficient allocation of resources by allowing the development of requirements for protection and nuclear security systems and measures against specific relevant threats rather than generic ones. The use of a performance based approach and a design basis threat allows for customization of the design of the nuclear security system to address unique features of the material, activities or facilities (including their instrumentation and control systems) but also sets a baseline against which nuclear security systems and measures can be evaluated (and modifications made if necessary) and provides a clear basis for defining the nuclear security responsibilities of the operator. The use of a design basis threat also provides a more detailed and precise technical basis for design and evaluation criteria and can provide greater assurance that the protection is sufficient.

6.5. The use of a design basis threat in a performance based approach means that greater resources and competence will be needed on the part of the regulatory body and the operator. The decision to pursue a design basis threat might therefore be influenced by the availability of the necessary resources and competence in the regulatory body for defining a design basis threat and in the operator for effectively using the design basis threat to design nuclear security systems and measures. However, if the State determines that the level of assurance associated with a design basis threat is needed, the State should make the necessary resources and competence available.

6.6. States should consider basing their physical protection requirements for nuclear material and nuclear facilities on a design basis threat specifically for unauthorized removal of Category 1 nuclear material and for sabotage of nuclear material and nuclear facilities with the potential to cause high radiological consequences if the State has such material or facilities [2]. States should also consider the development of a design basis threat for other cases where they determine that the potential consequences of a malicious act would be severe.

6.7. Development of a design basis threat should be considered for the protection of nuclear material or other radioactive material, an associated activity, or an associated facility for which potential consequences are lower in any of the following cases:

(a) The national nuclear security threat assessment indicates the existence of a threat with a known intention to commit a malicious act.
(b) The national nuclear security threat assessment indicates a highly capable threat for which the intention is unknown.

(c) Too much uncertainty is considered in the national nuclear security threat assessment due to insufficient data or insufficient confidence in the sources of the data.

6.8. For new facilities, a State may consider the possible long term advantages of designing protection against more conservative threat attributes and characteristics than those indicated by the current national nuclear security threat assessment in order to reduce the potential cost implications of upgrades added after the facility is in operation.

DEVELOPING A DESIGN BASIS THREAT

6.9. A design basis threat should be developed from the national nuclear security threat assessment using the following five tasks:

(1) Screening the national nuclear security threat assessment documentation to identify relevant threats with the motivation, intention and/or capability to commit a malicious act;
(2) Collating adversary attributes and characteristics;
(3) Adjusting collated adversary attributes and characteristics to take account of policy factors;
(4) Tailoring adversary attributes and characteristics to specific facilities and activities;
(5) Finalizing and establishing the design basis threat.

Screening the national nuclear security threat assessment documentation

6.10. Targets for which malicious acts could lead to unacceptable radiological consequences, as defined by the State, should be identified. These targets should then be considered in conjunction with the attributes and characteristics of the potential adversaries described in the national nuclear security threat assessment documentation in order to identify threats that are relevant to these targets and that might therefore cause unacceptable radiological consequences. This consideration should include a review of the motivations, intentions and capabilities of the adversaries with respect to these targets.

6.11. The descriptions of adversaries in the national nuclear security threat assessment documentation should be reviewed to determine which of them possess the capabilities necessary to commit a malicious act that could lead to unacceptable radiological consequences. If the capabilities of a given adversary

are not sufficient to commit such an act, then that adversary may be excluded from further consideration. However, caution should be exercised when making such a decision. In particular, a threat should not be excluded from further consideration on the basis that the existing nuclear security system in place to protect a facility or activity is sufficient to defeat the adversary. Existing nuclear security measures should not be considered when judging adversaries' capabilities during the development of a design basis threat.[6]

6.12. Each adversary considered to have sufficient capabilities to commit a malicious act potentially leading to unacceptable radiological consequences should then be reviewed to determine whether that adversary is also believed to have sufficient motivation or intention to commit such an act. If neither sufficient motivation nor intention is determined to be present, the adversary may be excluded from further consideration. However, caution should be exercised when considering excluding a highly capable adversary solely on the basis of perceived lack of motivation or intention. The decision on whether to exclude the adversary should take into account consideration of whether the adversary's perceived motivation is consistent with the potential consequences of such a malicious act and whether the degree of confidence in the data used to assess their motivation and intention is sufficient.

6.13. The reasons for the exclusion of any adversary described in the national nuclear security threat assessment documentation from further consideration for the design basis threat should be well documented. Any adversary excluded from consideration should be considered again if new information that would affect the reasons for the exclusion is acquired at a later time.

6.14. At the end of the screening process, a list should be produced of all credible adversaries that are capable of and might have the motivation and the intention to commit a malicious act potentially leading to unacceptable radiological consequences.

Collating adversary attributes and characteristics

6.15. Each of the relevant adversaries identified from the national nuclear security threat assessment documentation should be assigned to an appropriate

[6] This is a deliberately conservative assumption. For example, these nuclear security measures might later be removed by an operator if the design basis threat does not include adversary attributes and characteristics against which the measures would be necessary and effective.

adversary type, and credible descriptions of each adversary type should be developed. Adversary types may be given illustrative labels for ease of reference (e.g. 'terrorists', 'criminals', 'extremists'), but they should be defined by their specific attributes and characteristics. The threat posed by an adversary type should reflect the range of attributes and characteristics of the various adversaries assigned to the adversary type.

6.16. The relevant attributes and characteristics associated with a given adversary type should be collated. The collated attributes and characteristics should not simply represent a combination of the most extreme attributes and characteristics of different adversaries but should be a credible combination that could realistically occur together in an adversary.

Adjusting collated adversary attributes and characteristics to take account of policy factors

6.17. The collated adversary attributes and characteristics should be assessed in the light of any relevant policy factors identified. This may result in adjustments to the collated attributes and characteristics of adversary types to enable a sustainable level of security, and may result in a change in the level of adversary capabilities assumed.

6.18. For example, the collated adversary attributes and characteristics may be adjusted to accommodate the degree of conservatism desired in the national nuclear security threat assessment. Such adjustment may aim to compensate for uncertainty and different interpretations in the data used in the national nuclear security threat assessment; to ensure the continued effectiveness of operators' nuclear security systems and measures as the threat evolves with time; or to include attributes and characteristics of threats about which there is little or no current intelligence, as a prudent approach.

6.19. Cost–benefit considerations may also lead to adjustments to the collated adversary attributes and characteristics. This may include balancing the benefit to society associated with potential targets, the consequences for society of successful malicious acts against those targets, and the costs to society of reducing the risks of such acts by implementing appropriate nuclear security measures, compared with those for protecting other assets with the potential to cause consequences of similar severity (e.g. explosives, chemicals, biological agents) or other critical infrastructure.

6.20. Other policy factors may also need to be taken into account, such as the division of nuclear security responsibilities between the State and operators, the impact of decisions regarding risk acceptance on public confidence, the contribution to public welfare of the potential targets (e.g. the applications for which nuclear material or radioactive material are being used), the confidence of neighbouring States in a State's nuclear security and threats in neighbouring States.

6.21. Conservatism and the other policy factors noted here are likely to result in an increase in the assumed capability levels of collated adversary attributes and characteristics in the design basis threat, whereas cost–benefit considerations might decrease them.

Tailoring adversary attributes and characteristics to specific facilities and activities

6.22. The broadly representative adversary attributes and characteristics, adjusted for policy factors, should be tailored to take account of the characteristics of specific facilities and activities. For facilities, such considerations may include the location and accessibility of the site, specific design features of the facility, operating practices at the facility and any specific local threats. For activities, they may include operating procedures, modes and routes of transport, and any threats specific to particular locations or routes.

Finalizing and establishing the design basis threat

6.23. Before using a design basis threat in the regulatory framework, comments from other competent authorities and affected parties should be considered. The final decision on the content of a design basis threat, and the overall responsibility for this content, should rest with the competent authority assigned by the State to lead the development process.

6.24. A model design basis threat is provided in the Appendix.

DEVELOPING A REPRESENTATIVE THREAT STATEMENT

6.25. As with a design basis threat, a representative threat statement should be developed on the basis of the national nuclear security threat assessment. The development process for a representative threat statement follows the approach described in paras 6.9–6.24 for a design basis threat, but it is typically less rigorous

at each step and might involve fewer organizations. Moreover, the adversary attributes and characteristics are not tailored to a specific facility or activity.

6.26. The process for developing a representative threat statement should include the following four tasks:

(1) Screening the national nuclear security threat assessment documentation to identify relevant threats with the motivation, intention and/or capability to commit a malicious act;
(2) Collating adversary attributes and characteristics into sets representative of the range of attributes and characteristics;
(3) Adjusting representative adversary attributes and characteristics on the basis of relevant policy considerations;
(4) Finalizing and establishing the representative threat statement.

THREATS WITHIN AND BEYOND THE DESIGN BASIS THREAT

6.27. During the national nuclear security threat assessment process, a broad range of adversary capabilities are likely to be identified. Taking account of known, actual and prevailing threats, the State will need to determine a level of threat or adversary capability above which the responsibility for response would lie with the State rather than the operator, whose capabilities and/or resources for protection and response might be insufficient for such high capabilities and potential consequences. However, the operator may still have a role in assisting the State either to protect against these nuclear security threats or to mitigate their consequences.

6.28. Design basis threats should therefore be based on adversaries with capabilities that fall below this threshold, with the implication that the operator does not have prime responsibility for protection against and response to adversaries with higher capabilities. Responsibility for countering adversaries with capabilities above this threshold will rest primarily with the State. The State's determination of this threshold will need to balance cost, operational impact and other considerations.

7. USE OF DESIGN BASIS THREATS AND REPRESENTATIVE THREAT STATEMENTS

7.1. As described in paras 6.2–6.8, a State may choose to use a performance based regulatory approach, a prescriptive regulatory approach or a combined approach. The use of design basis threats and representative threat statements in each of these regulatory approaches is discussed in this section.

PERFORMANCE BASED REGULATORY APPROACH

7.2. In a performance based regulatory approach, design basis threats and the State's nuclear security objectives provide the basis for designing, implementing and evaluating nuclear security systems and measures.

7.3. A process for using design basis threats in a performance based regulatory approach includes the following tasks:

(a) The regulatory body should disseminate the design basis threats to the operators.
(b) Each operator, in cooperation with the regulatory body, should define credible attack scenarios on the basis of the design basis threats provided.
(c) Each operator should design nuclear security systems and measures that are effective against the defined attack scenarios for its facility or activity.
(d) Each operator should describe its nuclear security system design in its security plan and should submit this plan to the regulatory body for approval, if required.
(e) The regulatory body should evaluate the effectiveness of each operator's nuclear security system design on the basis of the submitted security plan.
(f) When the security plan is approved, the operator can operate its facility or activity.

7.4. Relevant emergency response organizations, including the regulatory body and the operator, should use the results of the national nuclear security threat assessment in the hazard assessment to establish adequate emergency arrangements for preparedness and response for a nuclear or radiological emergency triggered by a nuclear security event, and for coordinated and integrated contingency response.

PRESCRIPTIVE REGULATORY APPROACH

7.5. In a prescriptive regulatory approach, the representative threat statements appropriate to each category of material and type of facility or activity should be used by the regulatory body to develop prescriptive regulatory requirements, taking account of nuclear security objectives defined by the State. The prescriptive regulatory requirements should specify nuclear security systems and measures that are to be implemented to ensure sufficient protection to meet the objectives of the State's nuclear security regime. Guidance that could assist States in developing such prescriptive regulatory requirements can be found in Refs [13–16].

7.6. A process for using representative threat statements as part of a prescriptive regulatory approach includes the following tasks:

(a) The regulatory body should define credible attack scenarios based on each representative threat statement and design nuclear security measures for different categories of material and types of facility and activity.
(b) The regulatory body should consider the measures recommended or suggested in relevant IAEA publications, such as Refs [2, 3, 9, 13–16], as appropriate, and determine whether these measures are sufficient to meet nuclear security objectives or whether additional measures need to be added to provide the level of protection required for the relevant representative threat statement.
(c) The regulatory body should develop prescriptive regulatory requirements for applying the designed nuclear security measures.
(d) Operators should implement the nuclear security measures as prescribed by the relevant regulatory requirements.

COMBINED APPROACH

7.7. As noted in para. 6.2 and in Refs [13, 14], elements of both prescriptive and performance based approaches are used in a combined regulatory approach.

7.8. The State may apply a performance based approach for facilities and activities where the benefit outweighs the cost, for example where greater assurance is appropriate owing to the potential consequences that could result from a nuclear security event. A prescriptive approach might be applied to material, associated facilities and associated activities where a nuclear security event would result in less severe potential consequences. The State may also decide that some

threats should be addressed with a performance based approach and others should be addressed with a prescriptive approach.

DEVELOPING ATTACK SCENARIOS

7.9. The development of attack scenarios relies on an understanding of how adversaries' attributes and characteristics might be used to carry out a malicious act, as well as whether and how different adversaries might cooperate to carry out such an act.

7.10. An attack scenario is a postulated or assumed set of conditions and events, commonly used in analysis or assessment to represent possible future conditions and events to be modelled, such as a possible nuclear security event. An attack scenario might represent the conditions at a single point in time or a single event, or a history of conditions or events (including processes) over time leading to or following from a nuclear security event, including potential delayed impacts.

7.11. Attack scenarios should be defined to include all credible combinations of adversary attributes and characteristics defined in a representative threat statement or a design basis threat, including collusion between insider and external adversaries and combinations of physical attack and cyber-attack. The scenarios should define (a) likely adversary pathways, (b) penetration times based on assumed attack tactics and delay times for physical and computer security measures, and (c) detection probabilities based on sensors and monitoring measures and assumed tactics for evading or defeating them.

7.12. In particular, attack scenarios involving cyber-attack should be considered. While a cyber-attack alone is very unlikely to be sufficient for unauthorized removal of material, a cyber-attack could compromise nuclear security measures that deter, detect, delay or respond to an attempted act of unauthorized removal or sabotage. A cyber-attack might also result in degradation of safety, security, nuclear material accounting and control, or emergency preparedness and response functions in support of such an attack.

7.13. The factors affecting the feasibility of an attack may include its complexity; the amount and sophistication of tools and other resources needed; the skills and capabilities of the adversaries; their knowledge of the facility and access points (including knowledge of hiding places for adversaries or tools, and knowledge of weak points in the systems that can be exploited); the total number of external adversaries; the capabilities of response forces; the number and nature of insiders

involved and the extent of their collusion; and the effectiveness of physical barriers, computer security measures, and detection and monitoring technology.

8. MAINTENANCE OF THE VALIDITY AND REVIEW OF THE NATIONAL NUCLEAR SECURITY THREAT ASSESSMENT AND ITS DOCUMENTATION AND OF THREAT STATEMENTS

8.1. The national nuclear security threat assessment documentation should be periodically reviewed to assess whether the assessment still represents a comprehensive and balanced view of the credible threats to nuclear security in the State, and the assessment should be revised if necessary.

8.2. Design basis threats and representative threat statements may need to be reviewed (and revised if necessary) if the national nuclear security threat assessment documentation is revised, or to reflect changes in policy factors, or to take account of experience gained from the design and evaluation of nuclear security systems and measures or from a nuclear security event.

8.3. Periodic review of the national nuclear security threat assessment, design basis threats and representative threat statements might be initiated, for example, every 12–18 months. The periodic review should follow the same process used to perform the national nuclear security threat assessment.

8.4. Consideration of new and evolving threats and capabilities not known to be directly related to nuclear security could be incorporated into the review of the national nuclear security threat assessment to identify any possible relevance of these threats for nuclear material, other radioactive material, associated facilities and associated activities.

8.5. A number of other situations may lead to a need for a review of the national nuclear security threat assessment, design basis threats and representative threat statements outside the periodic review process. The conditions or events that might trigger such a review include the following:

(a) Any event or act, within the State or elsewhere, whether or not directly relating to nuclear material, other radioactive material, associated facilities

or associated activities, that significantly changes the perception of or actual level of the threat to nuclear security.

(b) Significant changes in government policy, law or international arrangements that affect the responsibility of the competent authorities or the operator, for example changes to response arrangements or organizational responsibilities.

(c) Changes in facilities or activities associated with nuclear material and other radioactive material that could change or introduce new potential consequences. Such changes could include, for example, construction of a different type of facility, use of material of higher enrichment, use of material in a new practice, repatriation of high enriched uranium, changing operation to use lower category material or nuclear safety improvements.

(d) A proposal for review by a competent authority, a technical or scientific support organization, or an operator.

8.6. A review will not necessarily result in revision of the national nuclear security threat assessment, the design basis threats or the representative threat statements. However, if the review shows that the national nuclear security threat assessment does not adequately address all credible threats, including new and emerging threats, the national nuclear security threat assessment and its documentation should be revised with the involvement of all relevant organizations. If there are substantial and fundamental changes in the national nuclear security threat assessment, the design basis threats and the representative threat statements should also be revised.

RESPONDING TO NEW AND EMERGING THREATS

8.7. Situations might arise outside the regular review process in which it is demonstrated or suspected that adversaries possess new or unexpected physical or computer related capabilities that are threatening enough to need immediate action on the part of the State. Intelligence and threat information may become available on these matters through both official and informal channels.

8.8. In addition to the process of developing design basis threats and representative threat statements, and maintaining their validity, the regulatory body and other competent authorities should put a process in place for sharing threat information among the competent authorities and with relevant operators. This is especially necessary when the threat level changes rapidly and there is not sufficient time for a full reappraisal of the national nuclear security threat assessment.

8.9. If an operator receives information on such a change in the threat through informal channels, the operator should inform the regulatory body and other competent authorities, as appropriate, to allow them to assess the credibility, relevance and severity of the potential impact of this change in the threat and to determine how, and how urgently, the State and/or the operator needs to respond.

8.10. Establishing a system of predetermined elevated threat levels, and corresponding predetermined sets of additional nuclear security measures to be implemented by operators at each level of elevated threat, can provide additional protection in such situations.

Appendix

A MODEL DESIGN BASIS THREAT

A.1. Table 1 is an example of how adversary attributes and characteristics could be reflected in a design basis threat.

A.2. A similar format could be used for representative threat statements, typically with less detail, or a less formal format could be used.

TABLE 1. EXAMPLE LISTING OF ADVERSARY ATTRIBUTES AND CHARACTERISTICS FOR A DESIGN BASIS THREAT

	Armed	Unarmed
Action		
Theft[a]	Insert *yes* or *no*	Insert *yes* or *no*
Sabotage[b]	Insert *yes* or *no*	Insert *yes* or *no*
Common attributes and characteristics		
Number	Insert a number	Insert a number
Level of funding	Insert *low* or *high*	Insert *low* or *high*
Insider support	Insert *active* or *passive*, and *violent* or *non-violent*	Insert *active* or *passive*, and *violent* or *non-violent*
Tactics	Insert *stealth* and/or *force*	Insert *stealth* and/or *force*
Planning skills	Insert *ability to plan a diversion*, and/or *adversaries attacking simultaneously in smaller groups,* and/or *knowledge of the facility layout* and/or *ability to plan a blended attack*	Insert *ability to plan a diversion*, and/or *adversaries attacking simultaneously in smaller groups,* and/or *knowledge of the facility layout* and/or *ability to plan a blended attack*

TABLE 1. EXAMPLE LISTING OF ADVERSARY ATTRIBUTES AND CHARACTERISTICS FOR A DESIGN BASIS THREAT (cont.)

	Armed	Unarmed
Physical attributes and characteristics		
Willingness to kill	Insert *yes* or *no*	Insert *yes* or *no*
Willingness to die	Insert *yes* or *no*	Insert *yes* or *no*
Pathway	Insert *air*, *road*, *rail*, *water* and/or *underground*	Insert *air*, *road*, *rail*, *water* and/or *underground*
Type of weapons	Insert *automatic weapons*, *semiautomatic weapons*, *side arms* and/or *knives*	Not applicable
Explosive	Insert the type and quantity of explosives	Not applicable
Tools	Insert *power tools*, *hand tools* and/or *tools available on-site*	Insert *power tools*, *hand tools* and/or *tools available on-site*
Technical skills	Insert *sophisticated explosive breaching*, *disabling communications lines* and/or *operating facility equipment*	Insert *sophisticated explosive breaching*, *disabling communications lines* and/or *operating facility equipment*
Contributing insider	Insert *access authorization*, *security guard*, *technical maintenance of equipment* and/or *material handler*	Insert *access authorization*, *security guard*, *technical maintenance of equipment* and/or *material handler*
Cyber attributes and characteristics		
Software tools	Insert *standard software tools*, *malware tools* and/or *own developed tools*	Insert *standard software tools*, *malware tools* and/or *own developed tools*

TABLE 1. EXAMPLE LISTING OF ADVERSARY ATTRIBUTES AND CHARACTERISTICS FOR A DESIGN BASIS THREAT (cont.)

	Armed	Unarmed
Expertise	Insert *social engineering*, *using commercial tools*, *developing new software tools, office domain*, *process control domain* and/or *knowledge about the applied IT system*	Insert *social engineering*, *using commercial tools*, *developing new software tools*, *office domain*, *process control domain* and/or *knowledge about the applied IT system*
Hardware tools	Insert *computer*, *mobile phone*, *connection to cables* and/or *routers*	Insert *computer*, *mobile phone*, *connection to cables* and/or *routers*
Ability to influence the supply chain	Insert *yes* or *no*	Insert *yes* or *no*
Persistence of the adversary	Insert *long term* and/or *repeated attacking capability*	Insert *long term* and/or *repeated attacking capability*
Contributing insider	Insert *access authorization*, *control the processes in I&C systems by normal user, administrator* and/or *third party vendor*	Insert *access authorization*, *control the processes in I&C systems by normal user*, *administrator* and/or *third party vendor*

Note: I&C — instrumentation and control; IT — information technology.

[a] May add criteria for the amount of material removed and/or one-time or protracted theft.

[b] May add criteria for radiological consequences.

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, Computer Security for Nuclear Security, IAEA Nuclear Security Series No. 42-G, IAEA, Vienna (in preparation).

[6] 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).

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

[8] Amendment to the Convention on the Physical Protection of Nuclear Material, INFCIRC/274/Rev.1/Mod.1, IAEA, Vienna (2016).

[9] INTERNATIONAL ATOMIC ENERGY AGENCY, Preventive and Protective Measures against Insider Threats, IAEA Nuclear Security Series No. 8-G (Rev. 1), IAEA, Vienna (2020).

[10] INTERNATIONAL ATOMIC ENERGY AGENCY, Security of Nuclear Information, IAEA Nuclear Security Series No. 23-G, IAEA, Vienna (2015).

[11] FOOD AND AGRICULTURE ORGANIZATION OF THE UNITED NATIONS, INTERNATIONAL ATOMIC ENERGY AGENCY, INTERNATIONAL CIVIL AVIATION ORGANIZATION, INTERNATIONAL LABOUR ORGANIZATION, INTERNATIONAL MARITIME ORGANIZATION, INTERPOL, OECD NUCLEAR ENERGY AGENCY, PAN AMERICAN HEALTH ORGANIZATION, PREPARATORY COMMISSION FOR THE COMPREHENSIVE NUCLEAR-TEST-BAN TREATY ORGANIZATION, UNITED NATIONS ENVIRONMENT PROGRAMME, UNITED NATIONS OFFICE FOR THE COORDINATION OF HUMANITARIAN AFFAIRS, WORLD HEALTH ORGANIZATION, WORLD METEOROLOGICAL ORGANIZATION, Preparedness and Response for a Nuclear or Radiological Emergency, IAEA Safety Standards Series No. GSR Part 7, IAEA, Vienna (2015).

[12] FOOD AND AGRICULTURE ORGANIZATION OF THE UNITED NATIONS, INTERNATIONAL ATOMIC ENERGY AGENCY, INTERNATIONAL LABOUR OFFICE, PAN AMERICAN HEALTH ORGANIZATION, UNITED NATIONS OFFICE FOR THE COORDINATION OF HUMANITARIAN AFFAIRS, WORLD HEALTH ORGANIZATION, Arrangements for Preparedness for a Nuclear or Radiological Emergency, IAEA Safety Standards Series No. GS-G-2.1, IAEA, Vienna (2007).

[13] 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).

[14] INTERNATIONAL ATOMIC ENERGY AGENCY, Security of Radioactive Material in Use and Storage and of Associated Facilities, IAEA Nuclear Security Series No. 11-G (Rev. 1), IAEA, Vienna (2019).

[15] INTERNATIONAL ATOMIC ENERGY AGENCY, Security of Radioactive Material in Transport, IAEA Nuclear Security Series No. 9-G (Rev. 1), IAEA, Vienna (2020).

[16] INTERNATIONAL ATOMIC ENERGY AGENCY, Security of Nuclear Material in Transport, IAEA Nuclear Security Series No. 26-G, IAEA, Vienna (2015).

GLOSSARY

design basis threat. 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.

representative threat statement. The attributes and characteristics of potential insider and/or external adversaries who might attempt unauthorized removal or sabotage, intended to be used to develop prescriptive requirements for the protection of defined materials and/or facilities.

threat assessment. An evaluation of the threats — based on available intelligence, law enforcement and open source information — that describes the motivations, intentions and capabilities of these threats.

threat statement. A description of credible adversaries (including attributes and characteristics) in the form of a design basis threat or a representative threat statement, developed on the basis of the national nuclear security threat assessment.

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

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

NUCLEAR SECURITY RECOMMENDATIONS ON RADIOACTIVE MATERIAL AND ASSOCIATED FACILITIES

IAEA Nuclear Security Series No. 14
STI/PUB/1487 (27 pp.; 2011)
ISBN 978-92-0-112110-3 Price: €22.00

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

PREVENTIVE AND PROTECTIVE MEASURES AGAINST INSIDER THREATS

IAEA Nuclear Security Series No. 8-G (Rev. 1)
STI/PUB/1858 (37 pp.; 2020)
ISBN 978-92-0-103419-9 Price: €24.00

SECURITY OF RADIOACTIVE MATERIAL IN TRANSPORT,

IAEA Nuclear Security Series No. 9-G (Rev. 1)
STI/PUB/1872 (102 pp.; 2020)
ISBN 978-92-0-105119-6 Price: €42.00

SECURITY OF RADIOACTIVE MATERIAL IN USE AND STORAGE AND OF ASSOCIATED FACILITIES

IAEA Nuclear Security Series No. 11-G (Rev. 1)
STI/PUB/1840 (105 pp.; 2019)
ISBN 978-92-0-110018-4 Price: €50.00

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 978-92-0-112210-0 Price: €46.00

This publication provides a step by step methodology for conducting a national nuclear security threat assessment, including both physical and computer security aspects, and for developing, using and maintaining design basis threats and representative threat statements. It is intended for use by States, competent authorities (including the regulatory body), relevant technical and scientific support organizations, and the operators of facilities and activities associated with nuclear material and other radioactive material, including shippers and carriers.

INTERNATIONAL ATOMIC ENERGY AGENCY
VIENNA