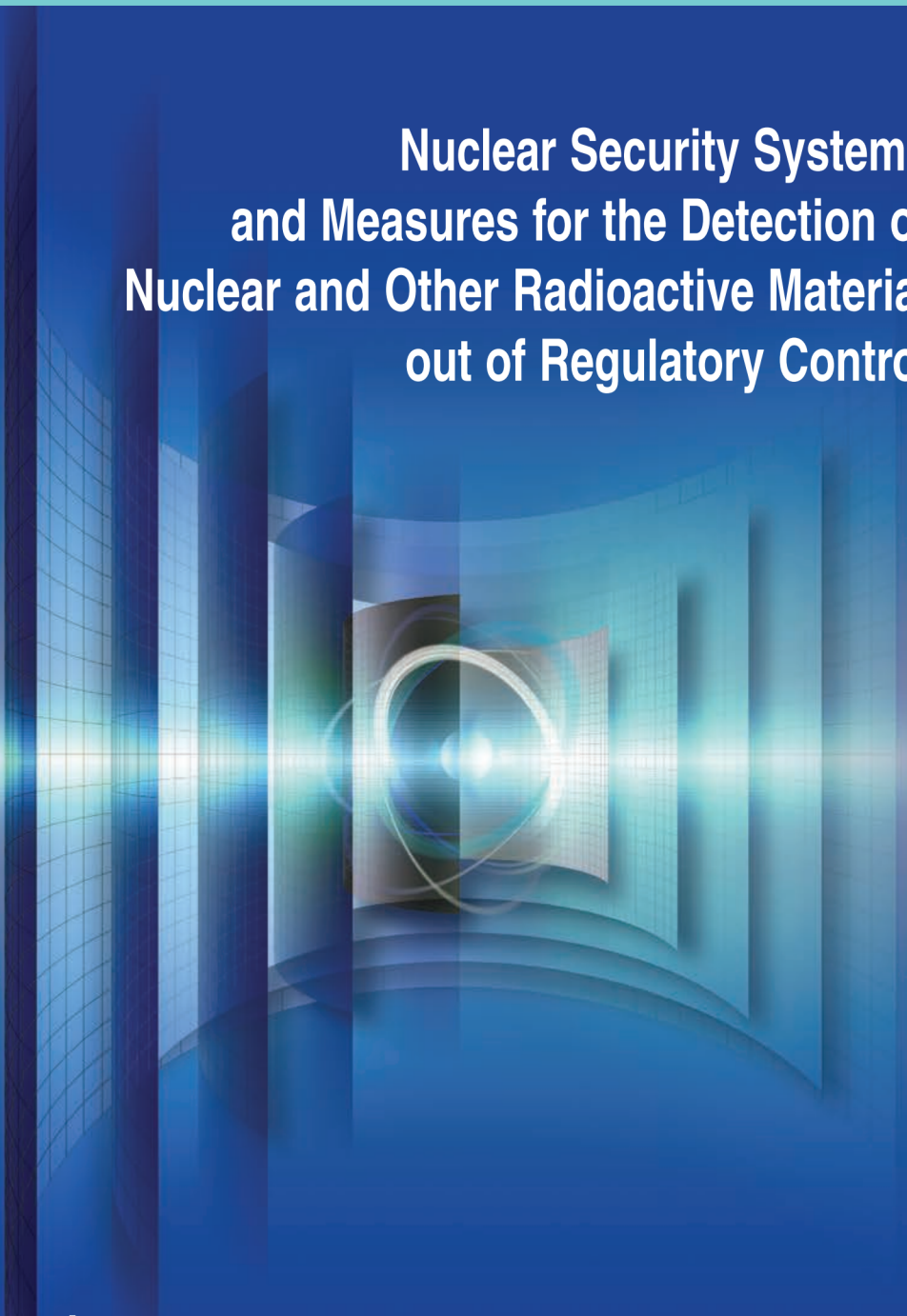
IAEA Nuclear Security Series No. 21

Implementing Guide

Nuclear Security Systems and Measures for the Detection of Nuclear and Other Radioactive Material out of Regulatory Control



IAEA
International Atomic Energy Agency

THE IAEA NUCLEAR SECURITY SERIES

Nuclear security issues relating to the prevention and detection of, and response to, theft, sabotage, unauthorized access and illegal transfer or other malicious acts involving nuclear material and other radioactive substances and their associated facilities are addressed in the **IAEA Nuclear Security Series** of publications. These publications are consistent with, and complement, international nuclear security instruments, such as the amended Convention on the Physical Protection of Nuclear Material, the Code of Conduct on the Safety and Security of Radioactive Sources, United Nations Security Council Resolutions 1373 and 1540, and the International Convention for the Suppression of Acts of Nuclear Terrorism.

CATEGORIES IN THE IAEA NUCLEAR SECURITY SERIES

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

- **Nuclear Security Fundamentals** contain objectives, concepts and principles of nuclear security and provide the basis for security recommendations.
- **Recommendations** present best practices that should be adopted by Member States in the application of the Nuclear Security Fundamentals.
- **Implementing Guides** provide further elaboration of the Recommendations in broad areas and suggest measures for their implementation.
- **Technical Guidance** publications include: **Reference Manuals**, with detailed measures and/or guidance on how to apply the Implementing Guides in specific fields or activities; **Training Guides**, covering the syllabus and/or manuals for IAEA training courses in the area of nuclear security; and **Service Guides**, which provide guidance on the conduct and scope of IAEA nuclear security advisory missions.

DRAFTING AND REVIEW

International experts assist the IAEA Secretariat in drafting these publications. For Nuclear Security Fundamentals, Recommendations and Implementing Guides, open-ended technical meeting(s) are held by the IAEA to provide interested Member States and relevant international organizations with an appropriate opportunity to review 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. This allows Member States an opportunity to fully express their views before the text is published.

Technical Guidance publications are developed in close consultation with international experts. Technical meetings are not required, but may be conducted, where it is considered necessary, to obtain a broad range of views.

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.

NUCLEAR SECURITY SYSTEMS AND MEASURES FOR THE DETECTION OF NUCLEAR AND OTHER RADIOACTIVE MATERIAL OUT OF REGULATORY CONTROL

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

AFGHANISTAN
ALBANIA
ALGERIA
ANGOLA
ARGENTINA
ARMENIA
AUSTRALIA
AUSTRIA
AZERBAIJAN
BAHRAIN
BANGLADESH
BELARUS
BELGIUM
BELIZE
BENIN
BOLIVIA
BOSNIA AND HERZEGOVINA
BOTSWANA
BRAZIL
BULGARIA
BURKINA FASO
BURUNDI
CAMBODIA
CAMEROON
CANADA
CENTRAL AFRICAN REPUBLIC
CHAD
CHILE
CHINA
COLOMBIA
CONGO
COSTA RICA
CÔTE D'IVOIRE
CROATIA
CUBA
CYPRUS
CZECH REPUBLIC
DEMOCRATIC REPUBLIC OF THE CONGO
DENMARK
DOMINICA
DOMINICAN REPUBLIC
ECUADOR
EGYPT
EL SALVADOR
ERITREA
ESTONIA
ETHIOPIA
FIJI
FINLAND
FRANCE
GABON
GEORGIA
GERMANY
GHANA
GREECE
GUATEMALA
HAITI
HOLY SEE
HONDURAS
HUNGARY
ICELAND
INDIA
INDONESIA
IRAN, ISLAMIC REPUBLIC OF
IRAQ
IRELAND
ISRAEL
ITALY
JAMAICA
JAPAN
JORDAN
KAZAKHSTAN
KENYA
KOREA, REPUBLIC OF
KUWAIT
KYRGYZSTAN
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
NORWAY
OMAN
PAKISTAN
PALAU
PANAMA
PAPUA NEW GUINEA
PARAGUAY
PERU
PHILIPPINES
POLAND
PORTUGAL
QATAR
REPUBLIC OF MOLDOVA
ROMANIA
RUSSIAN FEDERATION
RWANDA
SAUDI ARABIA
SENEGAL
SERBIA
SEYCHELLES
SIERRA LEONE
SINGAPORE
SLOVAKIA
SLOVENIA
SOUTH AFRICA
SPAIN
SRI LANKA
SUDAN
SWAZILAND
SWEDEN
SWITZERLAND
SYRIAN ARAB REPUBLIC
TAJIKISTAN
THAILAND
THE FORMER YUGOSLAV REPUBLIC OF MACEDONIA
TOGO
TRINIDAD AND TOBAGO
TUNISIA
TURKEY
UGANDA
UKRAINE
UNITED ARAB EMIRATES
UNITED KINGDOM OF GREAT BRITAIN AND NORTHERN IRELAND
UNITED REPUBLIC OF TANZANIA
UNITED STATES OF AMERICA
URUGUAY
UZBEKISTAN
VENEZUELA
VIETNAM
YEMEN
ZAMBIA
ZIMBABWE

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

IAEA NUCLEAR SECURITY SERIES No. 21

NUCLEAR SECURITY SYSTEMS AND MEASURES FOR THE DETECTION OF NUCLEAR AND OTHER RADIOACTIVE MATERIAL OUT OF REGULATORY CONTROL

IMPLEMENTING GUIDE

INTERNATIONAL ATOMIC ENERGY AGENCY
VIENNA, 2013

COPYRIGHT NOTICE

All IAEA scientific and technical publications are protected by the terms of the Universal Copyright Convention as adopted in 1952 (Berne) and as revised in 1972 (Paris). The copyright has since been extended by the World Intellectual Property Organization (Geneva) to include electronic and virtual intellectual property. Permission to use whole or parts of texts contained in IAEA publications in printed or electronic form must be obtained and is usually subject to royalty agreements. Proposals for non-commercial reproductions and translations are welcomed and considered on a case-by-case basis. Enquiries should be addressed to the IAEA Publishing Section at:

Marketing and Sales Unit, Publishing Section
International Atomic Energy Agency
Vienna International Centre
PO Box 100
1400 Vienna, Austria
fax: +43 1 2600 29302
tel.: +43 1 2600 22417
email: sales.publications@iaea.org
http://www.iaea.org/books

© IAEA, 2013

Printed by the IAEA in Austria
May 2013
STI/PUB/1613

IAEA Library Cataloguing in Publication Data

Nuclear security systems and measures for the detection of nuclear and other radioactive material out of regulatory control : implementing guide. — Vienna : International Atomic Energy Agency, 2013.
p. ; 24 cm. — (IAEA nuclear security series, ISSN 1816–9317 ; no. 21)
STI/PUB/1613
ISBN 978–92–0–142910–0
Includes bibliographical references.

1. Radioactive substances — Detection. 2. Radiation sources — Safety measures. 3. Nuclear Terrorism — Prevention. I. International Atomic Energy Agency. II. Series.

IAEAL 13–00813

FOREWORD

Nuclear terrorism and the illicit trafficking of nuclear and other radioactive material threaten the security of all States. There are large quantities of diverse radioactive material in existence, which are used in areas such as health, the environment, agriculture and industry. The possibility that nuclear and other radioactive material may be used for terrorist acts cannot be ruled out in the current global situation. States have responded to this risk by engaging in a collective commitment to strengthen the protection and control of such material, and to establish capabilities for detection and response to nuclear and other radioactive material out of regulatory control.

Through its nuclear security programme, the IAEA supports States to establish, maintain and sustain an effective nuclear security regime. The IAEA has adopted a comprehensive approach to nuclear security. This approach recognizes that an effective national nuclear security regime builds on: the implementation of relevant international legal instruments; information protection; physical protection; material accounting and control; detection of and response to trafficking in nuclear and other radioactive material; national response plans; and contingency measures. Within its nuclear security programme, the IAEA aims to assist States in implementing and sustaining such a regime in a coherent and integrated manner.

Each State carries the full responsibility for nuclear security, specifically: to provide for the security of nuclear and other radioactive material and associated facilities and activities; to ensure the security of such material in use, storage or in transport; to combat illicit trafficking; and to detect and respond to nuclear security events.

This is an Implementing Guide on nuclear security systems and measures for the detection of nuclear and other radioactive material out of regulatory control. The objective of the publication is to provide guidance to Member States for the development or improvement of nuclear security systems and measures for the detection of criminal or unauthorized acts with nuclear security implications involving nuclear and other radioactive material out of regulatory control. The preparation of this publication benefitted from the model guidelines document for nuclear detection architectures developed within the framework of the Global Initiative to Combat Nuclear Terrorism (GICNT). The work undertaken by the GICNT in this endeavour is gratefully acknowledged.

The preparation of this publication in the IAEA Nuclear Security Series has been made possible by the contribution of a large number of experts from IAEA Member States. An extensive consultation process with all Member States included an open-ended technical meeting in Vienna in October 2011. The draft was then circulated to all Member States for 120 days to solicit further comments and suggestions. The experts' contributions for developing and reviewing this publication are highly appreciated.

EDITORIAL NOTE

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.

The IAEA has no responsibility for the persistence or accuracy of URLs for external or third party Internet web sites referred to in this book and does not guarantee that any content on such web sites is, or will remain, accurate or appropriate.

CONTENTS

1. INTRODUCTION 1

Background (1.1–1.7) 1
Purpose (1.8) 3
Scope (1.9–1.10) 3
Structure (1.11) 4

2. BASIS FOR ESTABLISHING A NATIONAL NUCLEAR SECURITY DETECTION ARCHITECTURE (2.1–2.6) 5

National nuclear security detection strategy (2.7–2.14) 7
Legal and regulatory framework (2.15–2.17) 8
National capabilities (2.18–2.28). 9
International and regional cooperation (2.29) 12

3. DESIGN AND DEVELOPMENT OF THE NATIONAL NUCLEAR SECURITY DETECTION ARCHITECTURE (3.1–3.3) 14

Attributes of effective nuclear security detection (3.4) 15
Structural and organizational elements (3.5–3.18) 17
Role of information in effective nuclear security detection (3.19–3.30) 23
Trustworthiness of personnel (3.31) 27
Role of nuclear security culture (3.32–3.33) 27

4. DETECTION BY INSTRUMENTS (4.1). 28

Detection instruments (4.2–4.12) 28
Data network for detection instruments (4.13) 31
Detection technology investments and operational requirements (4.14–4.15) 31
Evaluating detection technologies (4.16–4.17) 31
Research and development in detection technology (4.18–4.19) 32

5. DETECTION BY INFORMATION ALERT (5.1) 34

Operational information (5.2–5.4). 34
Medical surveillance reports (5.5–5.6) 35

Reporting regulatory non-compliance (5.7–5.9) 35
Reporting loss of regulatory control (5.10–5.11). 36

6. INITIAL ASSESSMENT OF ALARMS/ALERTS (6.1) 37

Initial assessment of alarms (6.2–6.3) 37
Initial assessment of alerts (6.4–6.5) 38

7. IMPLEMENTATION FRAMEWORK (7.1). 40

Roles and responsibilities (7.2–7.3). 40
Instrument deployment plan (7.4–7.7). 41
Concept of operations (7.8–7.15) 43
Education, awareness, training and exercises (7.16–7.20) 44
Sustainability (7.21–7.24) 46

APPENDIX: NUCLEAR SECURITY DETECTION ARCHITECTURE 'CHECKLIST' 49

REFERENCES 55
GLOSSARY 57

1. INTRODUCTION

BACKGROUND

1.1. The risk that nuclear or other radioactive material could be used in terrorist acts is regarded as a serious threat to international peace and security. The IAEA maintains an Incident and Trafficking Database [1], which contains confirmed reports of detected nuclear and other radioactive material out of regulatory control. Material out of regulatory control could lead to criminal or terrorist acts including: (i) criminals or terrorists acquiring and using nuclear material to build an improvised nuclear device (IND); (ii) deliberate dispersal of radioactive material by the construction of a radiological dispersal device (RDD) or radiation exposure device (RED); or (iii) an act of sabotage at a facility that uses or stores nuclear and other radioactive material, or during transport of nuclear and other radioactive material.

1.2. There are a number of international legal instruments, both binding and non-binding, which are intended to combat nuclear terrorism. The IAEA has responded to requests from Member States for guidance on their obligations and best practices with respect to these international legal instruments. The guidance publications include:

— Nuclear Security Fundamentals [2];
— Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5) [3];
— Nuclear Security Recommendations on Radioactive Material and Associated Facilities [4];
— Nuclear Security Recommendations on Nuclear and Other Radioactive Material out of Regulatory Control [5];
— The International Legal Framework for Nuclear Security [6].

1.3. The Recommendations [3–5], the second tier guidance publications in the IAEA Nuclear Security Series, elaborate upon the essential elements of nuclear security set out in the Nuclear Security Fundamentals [2], and present international consensus recommendations on how States should apply these essential elements.

1.4. This publication falls within the third tier of guidance in the IAEA Nuclear Security Series, Implementing Guides, which are intended to provide more

detailed information on implementing the Recommendations using appropriate systems and measures.

1.5. A State's nuclear security regime comprises:

— The legislative and regulatory framework, and administrative systems and measures governing the nuclear security of nuclear material, other radioactive material, associated facilities and associated activities;
— The institutions and organizations within the State responsible for ensuring the implementation of the legislative and regulatory framework and administrative systems of nuclear security;
— Nuclear security systems and measures for the prevention of, detection of and response to nuclear security events [2].

1.6. One of the necessary elements supporting the establishment of an effective nuclear security regime is the development of a national detection strategy [5]. The implementation of the national detection strategy relies upon an effective nuclear security detection architecture[1] that contributes to the protection of persons, property, society and the environment from the harmful consequences of a nuclear security event by enhancing a State's capacity to monitor and control the movement of nuclear and other radioactive material.

1.7. An effective nuclear security detection architecture is based on the national detection strategy and the national legal and regulatory framework for nuclear security, and is supported by a well functioning system of law enforcement[2] [7]. The nuclear security detection architecture comprises:

— Established competent authorities[3] with responsibilities for the nuclear security systems and measures for detection as well as technical support organizations and arrangements for coordination and communication;

---

[1] Within the context of this publication, the term 'nuclear security detection architecture' means the integrated set of nuclear security systems and measures as defined in Ref. [5], and is based on an appropriate legal and regulatory framework needed to implement the national strategy for the detection of nuclear and other radioactive material out of regulatory control.

[2] As used here, the term 'law enforcement' is intended to cover a wide range of different functions and responsibilities concerned with enforcing laws, regulations and related requirements.

[3] Competent authorities are governmental organizations or institutions that have been designated by a State to carry out one or more nuclear security functions [5].

— Arrangements for international cooperation and assistance in relation to detection;
— Nuclear security systems and measures for detection of nuclear and other radioactive material out of regulatory control that provide adequate coverage of the State, its facilities and other strategic locations (e.g. borders), including:
  - A comprehensive set of detection instruments (fixed and/or mobile) with appropriate concepts of operations;
  - A system for the collection and promulgation of appropriate operational information, medical surveillance data (that indicates radiation exposure), and non-compliance reports from the regulatory authority and other competent authorities who may issue approval (e.g. transport, or import or export approvals) as part of information alerts.

PURPOSE

1.8. The purpose of this publication is to provide guidance on the development of, or improvement of an existing nuclear security detection architecture that establishes systems and measures for the detection of criminal acts or unauthorized acts with nuclear security implications involving nuclear and other radioactive material out of regulatory control.

SCOPE

1.9. This publication provides guidance to States for the development of an effective nuclear security detection architecture for detection of a criminal act or an unauthorized act with nuclear security implications involving nuclear and other radioactive material out of regulatory control.

1.10. This publication does not address in detail the legal or regulatory framework or the national nuclear security strategy that support the nuclear security detection architecture, nor does it address the preventive measures that may be implemented. It provides guidance on the interface with the response measures but does not deal with the response to nuclear security events. It is recognized that safety measures may be needed for the protection of people against radiation from detection instruments (particularly active ones) or from nuclear or other radioactive material being detected. This publication does not address such safety measures. Radiation protection requirements are set out in Ref. [8].

STRUCTURE

1.11. Following this introduction, Section 2 describes the basis for establishing an effective nuclear security detection architecture, including the relationship between its components. Section 3 sets out the elements of an effective nuclear security detection architecture. Sections 4 and 5 describe the basic concepts for detection by instruments and by information alerts, respectively. Section 6 presents guidelines on the initial assessment of alarms and alerts. Section 7 provides an overview of the implementation framework for establishing a nuclear security detection architecture. The Appendix provides a 'checklist' for establishing an effective nuclear security detection architecture.

2. BASIS FOR ESTABLISHING A NATIONAL NUCLEAR SECURITY DETECTION ARCHITECTURE

2.1. The Nuclear Security Recommendations on Nuclear and Other Radioactive Material out of Regulatory Control [5] recommend that for a State to have an effective nuclear security regime, it should ensure that there is:

— Comprehensive legislation that provides legal authority to the various competent authorities within the State to undertake their activities in an effective manner;
— Provision of sufficient and sustained resources to the various competent authorities to enable them to carry out their assigned functions, including establishing and maintaining systems and measures to detect, through an instrument alarm and/or an information alert, the actual or suspected commission of a criminal act or an unauthorized act with nuclear security implications involving nuclear or other radioactive material out of regulatory control.[4]

2.2. The nuclear security detection architecture should integrate the nuclear security systems and measures needed to implement a national strategy for the detection of nuclear and other radioactive material out of regulatory control. The systems and measures should be implemented within a concept of operations and be supported by communications, law enforcement, intelligence agencies, systems of regulatory compliance as well as human resources (e.g. enforcement officials, experts, local and national response teams, other authorities) to ensure their effectiveness.

---

[4] A 'criminal act' is normally covered by criminal or penal law in a State, whereas an 'unauthorized act' is typically the subject of administrative or civil law. In addition, criminal acts involving nuclear or other radioactive material may constitute offences related to acts of terrorism which, in some States, are subject to special legislation that may be of relevance in following the recommendations. Unauthorized acts with nuclear security implications could include both intentional and unintentional unauthorized acts as determined by the State. Examples of a criminal act or an unauthorized act with nuclear security implications could, if determined by the State, include: (i) the undertaking of an unauthorized activity involving radioactive material by an authorized person; (ii) the unauthorized possession of radioactive material by a person with the intent to commit a criminal or unauthorized act with such material, or to facilitate the commission of such acts; or (iii) the failure of an authorized person to maintain adequate control of radioactive material, thereby making it accessible to persons intending to commit a criminal or an unauthorized act, using such material.

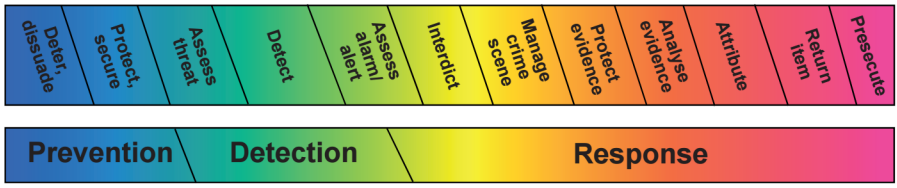


FIG. 1. Spectrum of nuclear security activities.

2.3. The remainder of Section 2 discusses a number of elements of a national nuclear security regime that provide the basis for an effective nuclear security detection architecture and that need to be taken into account in establishing such an architecture.

2.4. The nuclear security detection architecture addresses part of a spectrum of nuclear security activities shown in Fig. 1. While this publication relates to the detection part of the spectrum, the relationships between the different parts of the spectrum (prevention, detection and response) are important.[5]

2.5. Although details of the prevention and response parts of the spectrum are outside the scope of this publication, it is important to consider the entire spectrum in the design and development of a State's nuclear security detection architecture. The nuclear security detection architecture will include detection systems and measures established by the responsible competent authorities.

2.6. Detection includes the assessment of information indicating an encounter between a threat and a detection measure by:

— An instrument alarm;
— An information alert;
— A collection of qualitative and quantitative information concerning the alarm or alert;
— Information from other sources, such as radiography, that may not necessarily be readings from radiation detectors;
— Initial assessment of the alarm or alert.

[5] Reference [5] recommends that once there has been a conclusive initial assessment that a nuclear security event has occurred, the relevant competent authorities should commence with response activities. These are outside the scope of this publication.

NATIONAL NUCLEAR SECURITY DETECTION STRATEGY

2.7. An effective nuclear security detection architecture should be derived from a comprehensive, integrated detection strategy prepared by the State, through the coordinating body or mechanism[6] to ensure the necessary institutional support [5]. In some instances, implementation of a detection strategy at the national level may require new legislation, while in other instances existing legislation may provide a sufficient basis for the implementation of the strategy.

2.8. The national detection strategy should determine the scope of, and priority assigned to the nuclear security detection architecture. It should articulate objectives for the detection systems and measures, and provide the basis for assignment of functions, including cooperation and coordination between the competent authorities and allocation of resources.

2.9. The detection strategy should be based on a careful characterization and analysis of the threat posed by the potential use[7] or transport of nuclear and other radioactive material out of regulatory control. A national threat assessment is prepared by the responsible competent authority in coordination with all involved organizations and is updated periodically in light of new information and changing conditions. The detection strategy should be based on a risk-informed approach and be reviewed and updated in accordance with changes to the threat assessment. The detection strategy should be reviewed periodically and whenever the threat environment changes significantly.

2.10. Threats will differ depending on the circumstances in each State. Possibilities that should be considered include the following:

— Criminal or terrorist groups attempting to build or use an IND;
— Criminal or terrorist groups acquiring and/or using nuclear or other radioactive material, through theft or other means — for example, for the construction of an RED or RDD — or sabotage of facilities and activities[8]; or
— A range of other criminal or unauthorized activities, such as unauthorized transport through a State territory, unauthorized possession or use of

---

[6] A 'coordinating body' is a committee with representatives of all relevant competent authorities. If the State has a federal structure, the coordinating body could be established at the federal and at the State, regional or local level.

[7] In this context, 'use' includes trade, receipt, possession and storage.

[8] The detection of such acts at regulated facilities and activities is not covered in this publication. For details, see Refs [3, 4, 9, 10].

nuclear or other radioactive material and devices within the State, as well as conspiracies and hoaxes or scams where the material is not actually nuclear or other radioactive material.

2.11. Similarly, a range of threats may be considered, from relatively unsophisticated and opportunistic isolated attacks to highly sophisticated and determined campaigns. Furthermore, all States, including those that assess the likelihood of the use within, or transport of nuclear and other radioactive material out of regulatory control through their territory to be relatively low, should be aware that material, equipment and technology that may ultimately contribute to the construction of an IND, RED or RDD may either originate in their State or be shipped through their State.

2.12. The detection strategy should include a policy on sensitive information and assign responsibilities to the various competent authorities for information security related to systems for detection of criminal or unauthorized acts with nuclear security implications involving the use of nuclear or other radioactive material out of regulatory control.

2.13. Consistent with Ref. [5], the national detection strategy should include making use, as appropriate, of opportunities for international and regional cooperation.

2.14. Once approved, key elements of a national detection strategy should be communicated to relevant stakeholders in an appropriate manner, which may differ depending on national laws and practices.

LEGAL AND REGULATORY FRAMEWORK

2.15. In accordance with Ref. [5], the State should establish and maintain an effective legal and regulatory framework as the basis for the implementation of the national detection strategy.

2.16. The legal framework should define the conduct or actions that are considered to be a criminal act, or an unauthorized act(s), with nuclear security implications. Criminal acts should be defined to include threatening or attempting to commit such an act as well as actually committing the act. The legal framework should include provisions that result in the protection of nuclear and other radioactive material at the source (i.e. security of material in authorized production, use and storage) and during transport. The legal framework should also provide the basis for the implementation of national import and export controls as well as customs

and border operations for detection at designated and undesignated points of entry and/or exit (POEs), and at other strategic locations.

2.17. The legal framework should define the roles and responsibilities of, and assign authority to the relevant competent authorities. Related functions of competent authorities in the development of a detection architecture should include:

— Contributing to the development of the national detection strategy;
— Developing, operating and maintaining the detection systems and alarm assessment procedures, and providing the resources necessary for implementing and testing the associated activities;
— Providing adequate training and information to all personnel involved in carrying out nuclear security detection measures;
— Sustaining the detection capabilities and ensuring operational preparedness through sound management practices, performance testing, detection instrument maintenance, personnel training, exercises and process improvements;
— Cooperating with the coordinating body (if established), other competent authorities and bilateral and multilateral counterparts as applicable, in part to ensure the effectiveness of their procedures and allocation of responsibilities;
— Developing sustainable communication between designated staff and other designated organizations for assessment of instrument alarms and information alerts.

NATIONAL CAPABILITIES

2.18. States may draw on a wide range of ongoing activities in the design, development and implementation of an effective nuclear security detection architecture. The national capabilities to support establishing and implementing an effective nuclear security detection architecture can be summarized as follows [7].

Security of nuclear and other radioactive material

2.19. The implementation of nuclear security systems and measures for nuclear and other radioactive material in authorized use or storage and during transport can prevent potential adversaries from obtaining material that could be used for a criminal act or an unauthorized act with nuclear security implications and provide a level of assurance that materials are secure and under control [3, 4, 9, 10].

Regulatory controls

2.20. Regulatory controls including enforcement measures contribute to detection of nuclear and other radioactive material. An effective nuclear security detection architecture necessarily relies upon regulatory authorities and other competent authorities that have a role in regulating and controlling the secure use, storage and transport of radioactive material.

2.21. Provision for inspecting vehicles, transport routes, facilities and other locations that have the potential to be targets for nuclear security threats should be made, in compliance with licensing and safety regulations within the State. Inspection methods may include weigh stations, highway checkpoints or random screening, and other inspection activities which provide an opportunity for nuclear security detection using shared instrumentation, information and cooperative planning.

Technical expertise

2.22. In addition to the expertise that should be available within competent authorities, technical experts, able to provide scientific and engineering expertise on the design of the detection systems and measures, operational concepts and procedures, analysis of data from detection systems and on interdicted material, may be found in academia and national research institutions. These resources may be integrated into the nuclear security detection architecture, provided that the methods of engaging such experts are formalized.

2.23. Technical experts can also assist in the assessment of instrument alarms or information alerts and analysis of trends in the performance of the systems. They can provide this support remotely and/or at the detection site, depending on the national nuclear security detection systems and measures. A State may have specialized tools for data analysis and collection, and may consider allocating resources to further develop these tools to enhance their utility as part of the nuclear security detection architecture.

Customs and border controls

2.24. Effective border controls are critical in preventing and/or detecting the unauthorized transport of nuclear and other radioactive material. In general, nuclear security detection systems and measures should be compatible with existing systems for controlling entry and exit of people and goods at designated land, water and air POEs. Organizations involved in border control enforcement

should be involved (where appropriate) in the development of the detection systems and measures to ensure effective and compatible screening, detection and interdiction. Local knowledge of authorities conducting counter-smuggling or drug enforcement operations focused on undesignated POEs (land, air and water) will be important for the detection of a criminal act or an unauthorized act involving nuclear and other radioactive material out of regulatory control, and should be factored into the planning of the nuclear security detection architecture.

Law enforcement

2.25. Law enforcement organizations at the national, sub-national and local levels should support the nuclear security detection architecture. Even if they do not use detection instruments themselves (and they may in some cases), law enforcement agencies have institutional knowledge and experience in security systems for the protection of targets that will be essential for implementing an effective nuclear security detection architecture. Mechanisms such as communication and coordination, joint training and exercises, and development of integrated operational protocols and procedures may be used to keep law enforcement authorities prepared to detect nuclear and other radioactive material out of regulatory control and aware of the existence of nuclear and other radioactive material in use, storage or transport within their jurisdictions.

Information gathering, processing and sharing

2.26. As the nuclear security detection architecture is developed and implemented, information and analysis regarding alarms and alerts, and knowledge of potential threats should be shared and used to enhance overall performance. A State may have existing mechanisms for the collection, analysis and sharing of operational information among law enforcement, border control and other competent authorities that can serve as a model and may be applied in the development of the nuclear security detection architecture. Information sharing may be formalized through appropriate protocols and agreements, so that essential information is shared among competent authorities such as law enforcement, customs and other competent authorities.

Private and public sectors

2.27. As the private and public sectors both have vital roles in an effective nuclear security detection architecture, there should be an appropriate partnership between the State and private industry. This interaction is illustrated by the private sector involvement as:

— Participants in the worldwide supply chain for internationally traded goods;
— Shippers and common carriers of vessels, aircraft, rail carriages and shipping containers used in normal commerce, which are routinely screened;
— Retailers, shippers and consumers of goods containing naturally occurring radioactive material (NORM), which can cause innocent alarms (see para. 6.2);
— Participants in the recycling industry;
— Operators of private port facilities, airports, railway stations and private security arrangements at major public events;
— Medical institutions using radioactive material;
— Suppliers and users of detection instruments and industrial devices that incorporate radioactive material;
— Suppliers of radiochemistry products for medical and research applications;
— Suppliers and shippers of dual use commodities.

2.28. The responsible competent authorities should develop outreach efforts to inform the private and public sectors of detection objectives and policies, as well as potential impacts and unintended consequences. Detection instruments and procedures for detection should be designed to avoid undue cost and inconvenience to business and not to unduly impede the flow of legitimate commerce.

INTERNATIONAL AND REGIONAL COOPERATION

2.29. While responsibility for the design of an effective nuclear security detection architecture rests with the State, international and regional cooperation may offer a number of benefits, such as:

— Opportunities to obtain information, advice or technical assistance to help improve detection capabilities.
— Development of regional technical support centres that can combine high level technical and scientific expertise to assess alarms and alerts.

— Advancement of research and development into new technical solutions, thereby accelerating progress and reducing the resource burden on any one State.
— Voluntary nuclear security event reporting to neighbouring States.
— Voluntary reporting to the IAEA Incident and Trafficking Database [1], and sharing of information on alarms, trends and detector performance.
— Conduct of vulnerability and threat assessments. While specific vulnerability information may be sensitive and unlikely to be shared, except under carefully controlled circumstances, cooperation in the methodologies for assessing vulnerabilities, risks and threats is possible and could be helpful for States as they seek to strengthen their capabilities and practices in this area.
— In situations where States are required to cooperate for the free movement of people and goods among neighbouring countries, States could cooperate and adopt a regional approach to nuclear security detection systems and measures.

3. DESIGN AND DEVELOPMENT OF THE NATIONAL NUCLEAR SECURITY DETECTION ARCHITECTURE

3.1. The design and development of an effective nuclear security detection architecture should include:

— Assignment and coordination of responsibilities for the implementation of the nuclear security detection architecture;
— Determination of:
  - The nature and amount of nuclear and other radioactive material present within a State;
  - The nature of the criminal and unauthorized acts with nuclear security implications involving nuclear and other radioactive material out of regulatory control that have been defined in relevant legislation;
  - The routes[9] along which nuclear and other radioactive material might be transported;
  - Individuals' and groups' capabilities and intentions to engage in criminal or unauthorized acts with nuclear security implications involving nuclear and other radioactive material out of regulatory control;
  - The tactics and capabilities that could be employed in acquiring, transporting and using nuclear and other radioactive material for criminal or unauthorized acts;[10]
  - The targets and strategic locations that might be attacked;
  - The conditions under which attacks might take place.
— Specification of a baseline, i.e. a set of initial capabilities and criteria upon which basis the detection systems and measures will be established;
— Determination, through a comparison of threat assumptions and baseline capabilities, of the gaps and vulnerabilities in nuclear security provisions;
— Consideration of a range of options, including detection systems and measures, technologies and non-technological solutions that could potentially reduce or eliminate the vulnerabilities;

---

[9] At the most generic level, such routes include designated and undesignated land, air and water POEs, with subdivisions under each of these broad categories. For example, land routes include rail, road and pedestrian crossings; aviation routes include commercial and private aviation; maritime routes include small vessels (e.g. less than 300 t) and larger vessels.

[10] Tactics and capabilities may include the use of various forms of shielding and masking to obscure the signatures of radioactive material; falsification of documents or other forms of deception to conceal illicit actions; the capability to use threats, coercion or violence; technical, financial, logistical and human resources; and possible insider information or assistance.

— Evaluation of the potential risk reduction benefits, costs and other impacts of the identified options;
— Prioritization of the available options according to risk reduction, costs and other impacts;
— Identification of short term risk reduction options for inclusion in the short term deployment of detection systems and measures;
— Identification of longer term options, such as research and development on improved technologies, methods and procedures;
— Evaluation of the effectiveness of the implemented systems and measures and identification of additional options and recommendations as appropriate.

3.2. In designing a nuclear security detection architecture, undue focus should not be placed on current or past threats. This can be avoided by a design that is forward looking and protects against threats that may exist in the future. This can be done through the performance of threat assessments to anticipate potential threats before they arise and careful consideration of vulnerabilities and consequences, including routes that might be exploited and targeted in the future. Therefore, it is important to revisit the analysis and adapt to changes in threat and risk.

3.3. Significant time may be needed to fully implement the technical and operational solutions. While the system is being developed, immediate steps, such as those listed below, may be needed to reduce risks and vulnerabilities:

— Ensuring timely and reliable technical support from sources of expertise away from the scene of detection to allow front line officers at the scene to consult with experts who can advise on all aspects of detection and assessment;
— Developing, exercising and evaluating concepts of operation.

ATTRIBUTES OF EFFECTIVE NUCLEAR SECURITY DETECTION

3.4. The policy and strategy attributes of an effective nuclear security detection architecture should [7]:

— Be risk-informed: The nuclear security detection architecture should be effective in limiting the risk associated with nuclear security threats, make efficient use of resources, be compatible with existing measures to prevent

the unauthorized movement of hazardous cargo and be based on a balance between risk reduction, cost effectiveness and other pertinent factors.

— Apply the defence in depth principle: Individual measures or defences can be circumvented or defeated, given sufficient time. No single layer can be sufficiently effective or reliable to ensure effective defence. Defence in depth is a key design principle for increasing the effectiveness of complex systems. For further guidance on defence in depth, see paras 3.5–3.18.
— Be graded and balanced: Vulnerabilities across lightly or undefended routes may be easily exploited. Effective defence needs to be balanced and avoid undue emphasis on a small number of easily defended routes while leaving other routes essentially unprotected. Furthermore, not all routes are equally attractive or feasible. A graded approach that recognizes the different risks associated with various routes will provide the best level of protection.
— Be designed to adapt and evolve over time: Threats change, sometimes quickly, and new threats can emerge with little warning. Technologies also evolve, enabling new or modified capabilities that can reduce risks, save money, improve timeliness or increase information availability and quality. Furthermore, the conditions in which detection systems operate may change as economic and commercial systems evolve. The detection systems and measures should, therefore, be able to be adapted accordingly.
— Have an element of unpredictability: Elements of unpredictability within the detection architecture can provide a strategic advantage. Random schedules for additional screening at varying locations, carefully guarded by operational security, will improve the effectiveness of the system. Mobile and re-locatable detection instruments can contribute significantly to unpredictability and deterrence.
— Not rely solely on radiation detection instruments: Radiation detection instruments are only one means of detection, and the overall effectiveness of a detection system can be enhanced by complementary methods. For example, operational or other qualitative information can contribute to detection.
— Emphasize operational flexibility: Mobile detection instruments can enable the detector to be brought nearer to the threat. Mobile detection instruments provide such advantages as flexibility to adjust to evolving threats and the ability to respond to information alerts or other information specific to particular threats or situations (such as major public events or heightened security alerts). However, fixed detectors can still play an important role, particularly at POEs and entrances to strategic locations.
— Be tailored to specific conditions and circumstances: The design principles outlined above have broad applicability to detection of nuclear and other radioactive material out of regulatory control. However, there is no ‘one

size fits all' approach that will be effective in all circumstances. Nuclear security detection architecture design should take into account specific differences among:

- States, including their legal systems, threat environments and resources.
- Competent authorities, including operating routines, technical bases, cultures, traditions and resources.
- Operational environments: These may differ greatly depending on whether they are at a seaport, airport, land crossing, rail crossing, post office, harbour, shoreline, mountainous open border, or in a desert or other harsh climate[11]. Some POEs tend to have somewhat regular, predictable traffic patterns but others may exhibit great variability.

— Exploit opportunities to integrate at the national, regional and international levels: Detection systems and measures may beneficially be integrated within the State using common data formats and protocols, and such integration is also to be encouraged at regional and international levels, to the extent consistent with national security. At the same time, sensitive information about design, vulnerabilities and operations needs to be protected. When appropriate, the benefits of sharing knowledge, research, best practices, information, intelligence and resources can lead to enhanced performance of national and international detection systems.

STRUCTURAL AND ORGANIZATIONAL ELEMENTS

3.5. The nuclear security detection architecture and its systems and measures should be based on the principles of defence in depth, e.g. including measures at and between POEs into the State, within the State and in other cooperating States. In addition, there are key foundations and cross-cutting elements that tie the layers together and provide important synergies among the layers.

Multi-layered approach

3.6. When designing the nuclear security detection architecture, the design of the detection systems within the State may depend, at least in part, upon the design of detection systems in other States. Figure 2 is intended to give a comprehensive view of a detection system structure and components for a possible global nuclear security detection architecture (which could be a long term vision). A national

[11] One important effort in this regard is establishing detection instrument settings appropriate to the unique physical and operating environment.

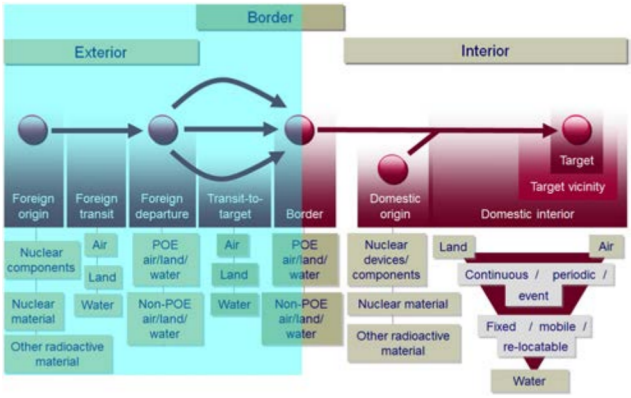


FIG. 2. Detection system structure and components.[12]

nuclear security detection architecture is on a smaller scale, focused at and within national borders. Figure 2 illustrates a wider context that should be considered in the implementation of a State's national nuclear security detection architecture.

3.7. Cooperation on the bilateral, regional and international levels is important for improving global nuclear security detection efforts. Such cooperation, as suggested by this comprehensive concept, requires agreement of all involved States.

Primary layers: exterior, trans-border and interior

3.8. This overarching concept has three layers:

— Exterior: The exterior layer encompasses the nuclear security detection architecture in other States, but should nevertheless be considered when designing the national nuclear security detection architecture.
— Trans-border: The trans-border layer encompasses the domestic border (both at and between the POEs) of the State, as well as transit corridors between the State and other States.
— Interior: The interior layer, within the target State, represents the final opportunity to detect and interdict nuclear and other radioactive material out of regulatory control before it could be used in a criminal act or unauthorized act. The national nuclear security detection architecture is within this layer and at the domestic border.

[12] While Fig. 2 depicts a linear path, it is important to recognize that threats may originate in any layer.

3.9. These three layers can be further broken down into a total of nine sub-layers, each of which is discussed briefly below. In the following discussion, it is assumed (unless otherwise indicated) that the target State is the State to whose nuclear security detection architecture these guidelines are being applied.

Exterior sub-layers: point of origin, transit and point of exit

3.10. Detection can focus on three sub-layers of the exterior layer:

— Foreign origin: The foreign origin sub-layer of nuclear security detection architecture focuses on locations in other States where nuclear and other radioactive material are stored, used or produced. The security and detection capabilities around these potential points of origin should be taken into account in the design of the national nuclear security detection architecture.
— Foreign transit: The transport of nuclear and other radioactive material within and between States provides opportunities for detection. The foreign transit sub-layer encompasses transport of material within or between States from their point of origin to their last POE before reaching the border of the target State. Within this element, material could be transported across multiple borders, by different modes of transport, and could encounter various elements of the nuclear security detection architecture operated by one or more States (or none at all, depending on the scenario). The types of detection opportunity are many and varied, and could include border crossings (at designated POEs or otherwise), checkpoints, law enforcement encounters, and maritime and air transport security procedures. This element includes the air, land and maritime domains, and can be further divided into designated and undesignated POEs.
— Foreign POEs: Foreign POEs from other States to the target State are natural screening points, since they form a possible common point through which traffic normally passes en route to the target State. The number of airports, seaports and land crossings through which cargo or people pass to the target State may be large. Nonetheless, even a large number of ports is much more manageable than the vast spaces between ports. For land crossings between adjacent nations, the foreign point of exit is generally physically adjacent to (and, hence, the same) as the domestic point of entry and will be described later under the border element of the nuclear security detection architecture.

Trans-border sub-layers: transit-to-target and border

3.11. The trans-border layer may be considered as two sub-layers:

— Transit-to-target: The transit-to-target sub-layer encompasses the actual passage of material from the point of exit from one State to the point of entry into another. The portion of the detection architecture designed to detect and interdict in the transit-to-target sub-layer represents the last opportunity to detect material before the material reaches the target State. As with the other parts of the architecture, this part can be divided into air, land and maritime modes of transport.
— Border: The border sub-layer comprises detection instruments at (or near) all geographical boundaries of the target State, including the land borders with adjacent States, the coastal and inland waterway borders, and airspace. Border areas are typically segmented by mode of transport (land, maritime, air) and whether the entry is through a designated or undesignated POE.

Interior sub-layers: domestic origin, domestic sub-element, target vicinity and target

3.12. A State developing a national detection strategy may consider several sub-layers:

— Domestic origin: As the material may originate from within the State itself, a major focus of the detection architecture in this sub-layer is locations within the State where nuclear and other radioactive material are stored, used or produced, or are out of regulatory control. Similar to those of the foreign origin sub-layer, countermeasures in this interior sub-layer are designed to protect nuclear and other radioactive material from being stolen or lost from these locations and to detect whether protection has failed.
— Domestic: The domestic sub-layer of the detection architecture includes capabilities to detect nuclear and other radioactive material between entry into the State (or the domestic point of origin) and the ultimate target. The purpose of this layer is to detect the device or material before it reaches its target or exits the country on the way to a foreign target.
— Target vicinity: The target vicinity sub-layer encompasses those detectors located near targets but at a sufficient distance that the targets can still be protected. It also includes search capabilities within the target vicinity. For example, the target vicinity may be around the perimeter of a base or campus or to the boundaries of a metropolitan area (boundaries that may themselves require definition), or at a security perimeter set up specifically for a major public event. An IND or RDD could be assembled near the

target itself or assembled elsewhere and moved to the target just prior to detonation. Therefore, States should consider methods of addressing such a threat when developing a national detection strategy. These methods may include performing inspection prior to major public events, tightly coupled with information gathering or increased perimeter inspections.

— Target: This sub-layer should be flexible, incorporating mobile detection instruments that can be deployed around high value targets and that are suitable for major public events, and means for handling information alerts on the possible use of material. It should be noted that POEs can in themselves be targets and should be included in the national threat assessment.

Cross-cutting elements

3.13. Cutting across all the layers are elements that integrate and support the layers. Key cross-cutting elements include the following.

Operations and analysis centre

3.14. This is the focal point for information about and from the detection systems. A national operations centre (or set of regional operation centres), if established, should be responsible for maintaining situational awareness of nuclear security capabilities and for facilitating the coordination of responses to the detection of nuclear and other radioactive material. An operations centre may also play a key role in informing and coordinating resources to mitigate consequences after an event. States should consider designating an operations centre or centres with responsibility for coordination and information dissemination between local, national and international entities. To be most effective, an operations centre should have access to relevant information on both threats and capabilities to counter or interdict threats. The responsible authority should have the ability to coordinate and communicate decisions to direct those capabilities. The State may have one or more such centres, depending on the organization of responsibilities for nuclear and other radioactive material within the State. States with multiple centres need to establish a mechanism for coordination among the centres.

Technical support[13] for detection

3.15. This is the (often remote) capability to assist those at the detection site in the assessment of radiation alarms or information alerts or on the discovery of suspicious or unauthorized material that could be used to manufacture an IND, RED or RDD. Technical support relies heavily on radiation analysts and subject matter experts who can identify specific isotopes and potential threats based on data collected from the detection site, either remotely or in person. International technical support capabilities may be available on request (e.g. through organizations such as the IAEA and other incident reporting channels).

Performance testing, evaluation and verification

3.16. This should involve planned and systematic efforts to evaluate the performance of the overall system and its ability to adjust to different radiological and cargo environments, provide quality control for sensors and systems, perform trend analysis and maintain longer term environmental knowledge.

Human resource development, training, exercises and operational readiness

3.17. Personnel skills and performance should be maintained by providing regular exercises and training at all levels (national, regional and international). Specialized training for the operation of management procedures and protocols for use of technology for the detection of nuclear and other radioactive material is vital. Overall system training should also include testing of the readiness of all relevant national authorities (including public health response, rescue, environmental protection and law enforcement authorities) [11].

Data exchange protocol

3.18. Deployed assets, such as detectors, technical support and analysis centres, should have the ability to exchange accurate and timely data. An effective data exchange infrastructure should have a combination of effective connectivity (robust, redundant and of sufficient bandwidth) and appropriate data standards or protocols to allow the recipient to understand the transmitted information. Effective data exchange also enables necessary situational awareness.

---

[13] The term 'technical support' refers to mechanisms for engaging subject matter experts, including researchers, scientists and analysts, to assist with technical expertise in investigating and resolving alarms and alerts.

Implementation difficulties typically arise because of the need to cross jurisdictional boundaries or the lack of interoperability of legacy systems.

ROLE OF INFORMATION IN EFFECTIVE NUCLEAR SECURITY DETECTION

3.19. Information is vital for the implementation of an effective nuclear security detection architecture. This information comes from many sources, takes many forms and plays a number of critical roles. Relevant information can come from radiation detectors, other sensors (e.g. cameras), detector operators, technical experts and analysts, emergency responders, law enforcement, intelligence analysts and international partners. Information may be captured as alarms, alerts, data, pictures, status, text, alerts and trends, or via more formal and specific mechanisms particular to each national organization. The information generated by the nuclear security detection architecture may be used to detect, identify or interdict material and to identify suspicious activities, or to evaluate the effectiveness of the architecture itself. The information could also be sensitive and should be protected at the national level.

3.20. Independent operation of individual, localized detection systems and measures limits the overall effectiveness of the detection architecture. In contrast, the effective flow and use of relevant information allows for optimal functioning of nuclear security detection systems. For the nuclear security detection architecture, information can be categorized into the following three main types.

Threat and alarm/alert information

3.21. This includes information about nuclear security threats, detections and relevant criminal or unauthorized activities such as smuggling, as well as technical assessments or collections of data related to possible nuclear security events. Such information also includes information related to detection alarms or alerts. This information should be transmitted to relevant competent authorities as soon as possible, especially when an actual threat is indicated. Protocols should be established in advance to ensure that appropriate officials of competent authorities are notified rapidly of nuclear security events.

3.22. The amount and type of data that may need to be transferred will vary. A technical support analyst may want to see detailed detector data and corroborative data about the circumstances of a detection. A customs officer or border guard may want information related to shipment manifests to aid in targeting or

inspecting cargo containers. Information provided to law enforcement officers may be critical in identifying and interdicting threats; not all interdictions of threats will necessarily be directly triggered by detecting alarms. Given the variety of information needs, national centres, such as the operations and analysis centre, designed to integrate data from all sources will improve the effectiveness of the nuclear security detection architecture.

Configuration information

3.23. This includes information about the set-up and organization of the detection systems. As this information is sensitive, it should be protected at the national level. This information includes specific data related to:

— Location of detection instruments;
— Types of detection instrument, including hardware and software configurations;
— Technical capability of instruments and their false alarm rates;
— Agencies and operators responsible for detection instruments;
— Authorities responsible for conducting inspections;
— Degree of training and expertise of operators;
— Operational information, such as the time periods when operations occur and the number of operators per detector;
— Supporting technical systems;
— Failure rates and maintenance schedules.

Status information

3.24. This includes information about the current (or historical) state of the detection instruments, operators, processes and systems. This information can be considered sensitive and should, therefore, be protected at the national level.

3.25. Information related to the location and status of deployed equipment and operators enables a more rapid and effective response to nuclear security events. Over time, aggregate data collected by nuclear security detection systems support important longer term trend analyses. These analyses can improve overall awareness related to the authorized transport of nuclear and other radioactive material, as well as potential threats. In addition, analysis of such information can provide national decision makers with the information required to allocate additional resources for maintenance and improvements to the detection systems.

Delivering information to users

3.26. Providing correct data to the correct users at the correct time is vital to ensuring that information effectively supports the detection of a nuclear security event. Detection systems can produce large amounts of data that should be collected and managed appropriately to ensure its effective use.

3.27. An important challenge for information management systems for a nuclear security detection architecture is the interoperability of detection instruments at different locations and with multiple users. This challenge increases as additional detectors, sensors or data collectors are included within a given information system. The development of common data formats and testing protocols may help ensure effective communications, even across multiple operators or jurisdictions. The design of the information system should be considered when designing the nuclear security detection architecture to ensure all information needs are addressed, including in relation to content, presentation and information sharing.

3.28. The various users of data from detection systems have different needs in terms of content, presentation and timeliness. These needs are highly dependent on the responsibilities of the user within the national nuclear security detection architecture. A tiered structure for information flow, including clear guidelines about what information is passed from tier to tier and in what circumstances, should be defined. Typically, States may have three broad levels of user, as follows:

— National decision makers, the highest level of data users, should receive timely information about the detection of nuclear security events. These decision makers also need an understanding of current capabilities and gaps to inform decisions about future investments. Without this information, investments may result in inefficient allocation of resources.
— The second level of information users comprises national and sub-national operations managers, including leaders of operational agencies and technical experts who support nuclear security detection systems. These data users are often geographically separated from the detection instruments for which they have responsibility. To effectively manage their real time operations, these national and sub-national managers should have rapid and secure access to data from detection instruments.
— Local operators of detection instruments, the third level of information users, are most often the first and direct recipients of data from detection instruments. Successful interdiction relies upon these operators making rapid decisions based on sometimes ambiguous detector data. Information

should, therefore, be transferred to these users rapidly and in forms that are easy to interpret, to allow them to work at an effective pace and respond properly.[14] Where relevant, operators should be provided with information that originates at higher level sub-national or national authorities, such as operational information and adjustments to operational or response protocols. Means to consistently supply such information should be established during the initial phases of implementing a detection architecture.

Information management

3.29. The nuclear security detection architecture should ensure that information cannot be retrieved by those seeking to circumvent or exploit the operation of detection systems. The detection strategy will include a policy on sensitive information related to detection architecture and define responsibilities of various competent authorities for information management. Each competent authority could establish an information management policy including the rules for protecting the confidentiality and integrity of sensitive information and for the dissemination of such information to other competent authorities within and outside the State on a need to know basis. In particular, the following information should be classified as sensitive and appropriately protected:

— Perceived national threats and vulnerabilities, and the results of the national threat assessment;
— Locations and configurations of detection systems as well as the performance, maintenance and calibration records of the detection instruments;
— Preparedness and response plans and procedures;
— Communication, authentication and encryption codes for transfer of sensitive information.

3.30. The policy should require appropriate training of the relevant personnel in procedures for information management.

[14] Accordingly, operational testing and evaluation should be conducted on data formats as they are displayed to operators to avoid inaccurate data interpretation.

TRUSTWORTHINESS OF PERSONNEL

3.31. States should establish systems for assessing the trustworthiness of personnel who work on elements of the national nuclear security detection architecture. Each competent authority should establish policy and procedures consistent with national laws requiring all personnel having responsibilities under the nuclear security detection architecture to be subject to:

— An appropriate trustworthiness check;
— A condition of employment requiring that a positive trustworthiness check be obtained and maintained;
— A requirement that such trustworthiness checks be revalidated on a regular basis, in accordance with national policy or regulations.

ROLE OF NUCLEAR SECURITY CULTURE

3.32. Three major components should be combined to promote an effective nuclear security culture within a State. The first is the nuclear security policy of the State that is put into practice in relation to a particular aspect of nuclear security, in this case the national nuclear security detection strategy. The second is individual organizations' roles in implementing aspects of nuclear security detection. The third is the management and individuals within organizations that put the nuclear security detection systems and measures into effect.

3.33. All personnel should be encouraged to be accountable for their attitude and behaviour and motivated to contribute to effect nuclear security. Effective nuclear security culture [11] is characterized by:

— Clear policy and legislation that emphasizes the importance of nuclear security;
— Institutions with clear mandates, roles and responsibilities in relation to nuclear security;
— Leaders and managers who model behaviour that emphasizes nuclear security;
— Recruitment and training of personnel that requires individuals to have attitudes and behaviour that support nuclear security;
— Training programmes and frequent exercises that reinforce attitudes and behaviours that support nuclear security.

4. DETECTION BY INSTRUMENTS

4.1. Detection of criminal acts or unauthorized acts involving nuclear or other radioactive material out of regulatory control may be achieved by detecting such material itself by technical means and/or by other means of detection. This section focuses on measures to detect nuclear and other radioactive material by radiation detection instruments, both passive and active, and by other technical means.

DETECTION INSTRUMENTS

4.2. Passive and active detection technologies use fundamentally different approaches. Passive detection instruments directly measure normal emissions of radiation from nuclear or other radioactive material. For example, personal radiation detectors, which are passive detectors, continuously monitor for the presence of radiation and signal elevated levels of gamma or neutron emissions to an operator. Active detection systems aim to detect nuclear or other radioactive material indirectly by detecting something else that may indicate the presence of nuclear or other radioactive material. For example, radiography, a simple active system, is used to detect dense material, which might be the shielding for the radioactive material. Active systems complement but do not replace passive systems.

4.3. Compared to active detection instruments, passive detection instruments are generally less expensive, and present no additional health risks to personnel. Passive detection instruments may also allow faster throughput than active detection instruments. However, passive detection instruments are inherently limited because they rely upon material emitting a radiation signal detectable above ambient background radiation. Therefore, passive detection instruments may not detect the presence of nuclear or other radioactive material, particularly if it is shielded. Owing to their comparatively low costs and distinct capability, passive detection instruments are common tools for the detection of nuclear or other radioactive material.

Passive detection instruments

4.4. Passive detection instruments generally provide the primary means to detect and, in some cases, identify a wide range of materials that could be used in criminal acts or unauthorized acts with nuclear security implications [12, 13]. Many of the currently available radiation detection instruments, often called

gross counting systems, rely upon algorithms that compare the instantaneous ambient level of radiation against a known background. While often effective in detecting sources of radiation, these detection instruments are susceptible to innocent alarm rates due to the presence of radioactive material that is not out of regulatory control, such as NORM. Spectroscopic detection instruments, which identify radionuclides through automated analysis of measured radiation energy spectra, may be integrated with gross counting detection instruments. Spectroscopy relies on the fact that every radionuclide emits radiation at specific energy levels, creating a unique emission energy signature or fingerprint for each isotope. These detection instruments can recognize and dismiss NORM.

4.5. Passive detection instruments are available in several types to meet a wide array of operational needs. They range in size from personal radiation devices or hand-held detectors [14] to portal monitors [13].

4.6. Personal radiation detectors have traditionally been intended for personnel protection but are now being considered for other applications. These detectors are generally small (approximately the size of a mobile telephone) and may be worn by operators on their belts or on their persons for an extended period of time. Personal radiation detectors continuously monitor the local gamma and/or neutron radiation. By integrating these measurements over specific time intervals, these detectors measure total radiation background and generally provide an alarm when radiation levels exceed a pre-established threshold. Personal radiation detectors can serve as a valuable tool for detecting the presence of radiation sources (especially those with particularly high activity levels). Some commercially available personal radiation detectors also provide radiation dose measurements and a limited capability to identify the isotopic constituents of a source by analysing the detected radiation.

4.7. Compared to smaller radiation detection instruments, portal monitors can rapidly scan much larger items, such as shipping containers and vehicles, and potentially detect much smaller amounts of radioactive material. The comparatively large volume of detector material provides the relatively high sensitivity of the portal monitor. A variety of mobile and re-locatable instruments can offer similar detection capability to that of a fixed portal monitor. These mobile or re-locatable instruments are designed for specific applications, such as:

— Land and water borders between designated POEs;
— Temporary detection locations established for major public events or in response to information alerts;
— Transit cargo at seaports and airports.

4.8. Mobile detection instruments may be installed in vehicles (such as vans), on cargo handling equipment (e.g. straddle carriers) or in manned or unmanned aircraft.

4.9. Recently developed hand-held and other portable or wearable passive detection instruments provide increased capability compared to earlier versions of the technology; many provide some degree of spectroscopic radiation identification capability. By employing advanced detectors and electronics with increased energy resolution and associated analysis tools, portable spectroscopic systems can measure the energy spectrum of emitted radiation and provide additional information to an operator on the presence of specific radionuclides [15, 16].

4.10. However, hand-held detectors, as personal radiation detectors, suffer from the relatively small size of their sensors. As sensitivity is directly related to the volume of the detector, these devices have limited detection ranges and may need a longer time to scan larger areas or items, such as shipping containers to obtain a sufficiently low limit of detection.

Active detection instruments

4.11. Active detection instruments provide different capabilities to passive detection instruments, but also introduce challenges. For example, active detection instruments could provide the ability to indirectly detect shielded radioactive material that might not be detectable by passive detection instruments. However, because active detection instruments operate by penetrating the object with radiation such as X rays, gamma radiation or neutrons, they often generate a safety concern, as people could be exposed to radiation. Thus, a balance between safety and security should be sought when deploying active detection instruments.

4.12. Two types of active detection instrument currently in operation or development are radiography and interrogation technologies. For the first type, X ray or gamma radiography is used to discriminate between low and high density material, which enables the detection of shielding. These detection instruments usually produce images that are analysed for anomalies by operators. The second type of active detection instrument, interrogation technologies, can directly detect nuclear material, whether shielded or unshielded, by generating a measurable radiation signature from the material in response to radiation from the interrogation instrument.

DATA NETWORK FOR DETECTION INSTRUMENTS

4.13. Integrating data from detection instruments into information networks is also an important element of developing an effective overall detection system. States may significantly improve operational effectiveness by integrating detection systems into local, sub-national and national data sharing networks. Networked detection systems and information sharing offer the benefit of helping to reduce operational burdens associated with innocent alarms. By sharing information between locations, operators can reduce duplicate inspections of individual targets and rapidly clear innocent alarms associated with many passive detection systems.

DETECTION TECHNOLOGY INVESTMENTS AND OPERATIONAL REQUIREMENTS

4.14. Investment in detection technologies should be directly informed by the national detection strategy for creating the nuclear security detection architecture, and in particular by operational requirements and constraints. This will reduce the likelihood of unnecessary costs, poorly performing technologies, ineffective use of scarce resources leading to a false sense of security, and other undesirable effects such as a negative impact on the flow of people and goods among States.

4.15. No single technology will meet all operational requirements. A highly effective system is one that is multi-layered and can cover a wide range of potential types of threat. Knowledge sharing among the international community will assist in meeting these challenges when designing the nuclear security detection architecture.

EVALUATING DETECTION TECHNOLOGIES

4.16. Evaluation of detection technologies should address a defined set of common performance characteristics. Evaluations should include objective laboratory testing of technology that is currently available to verify performance, and also technologies under development for possible operational enhancements that newer technologies may provide. Evaluation should also consider whether new technologies are compatible with existing operations. If appropriate, regional and international collaboration and sharing of evaluation results can provide a significant benefit to States by avoiding duplication of testing and data collection.

4.17. The following performance characteristics should be considered by a State when assessing detection technologies:

— Detection capability requirements, which are based on information derived from the threat assessment;
— Detection instrument performance in the context of the concept of operations: Radiation detection instruments may perform differently in different operational environments, so evaluations of specific detection instruments should be made in an operational context to the extent possible;
— Detection instrument performance for identification of the type of detected radiation: This can be achieved by a multi-layered approach where an initial technology is used to detect radiation, and additional technical capabilities are applied in secondary inspections to identify the source of the radiation [16];
— Detection instrument range, sensitivity and efficiency: While smaller detectors generally exhibit shorter detection ranges, detector range is not only a function of detector size. The range is inversely related to the probabilities of detection and identification. Depending on the application (e.g. wide area searches as compared to the scanning of passenger luggage), there will usually be a trade-off between detection range and the probability of detecting specific material;
— Detection instrument mobility or ability to be re-located: The potential for mobility encompasses a number of factors, including size, weight, durability, power requirements and data connectivity;
— Other factors influencing the choice of detection instrument technology, including initial cost, life cycle cost, temperature or shock resistance, other operating requirements (energy consumption, weight, cooling requirements) and physical dimensions.

RESEARCH AND DEVELOPMENT IN DETECTION TECHNOLOGY

4.18. Ongoing research and development to develop new capabilities should be considered vital to support detection technologies. Individual States may adopt different approaches to development depending on their research and development framework. International collaboration is an important means of sharing improvements in technology that will benefit all States. Such collaboration will be dependent on whether certain information may be shared or is classified as sensitive by a State.

4.19. Research in detection technology may focus on the technical attributes such as probability of detection, identification capability, detection range and mobility. These improvements may be sought at a systems level, through the development of improved instruments, and for integrating detector hardware and software.

5. DETECTION BY INFORMATION ALERT

5.1. Detection of criminal acts or unauthorized acts with nuclear security implications can also be achieved by information alert. An information alert, possibly indicating a nuclear security event, may come from a variety of sources, including operational information, medical surveillance and border monitoring, and with a follow-up assessment may lead to detection. This section outlines the need for establishing systems and measures for collecting and analysing information alerts.

OPERATIONAL INFORMATION

5.2. Within the framework of a national nuclear security detection architecture, the competent authorities concerned with detection systems should gather operational information in order to gain a better understanding of the threats within the State. Gathering and analysing information on the following should be considered:

— Activities of sub-national groups.
— Information obtained through other national or international sources, including the IAEA Incident and Trafficking Database [1].
— Non-compliance with regulatory requirements, particularly relating to transport of nuclear and other radioactive material.
— Abnormal activities in international trade.
— Trading of nuclear and other radioactive material (who is buying the radioactive sources and for what purpose). Counterterrorism capabilities may need to be used to investigate such activities.
— Discrepancies in the inventory of nuclear and other radioactive material.
— Other information suggesting unauthorized activities involving nuclear and other radioactive material.

5.3. Effective information gathering should involve the full cooperation of competent authorities and other relevant organizations, including the regulatory authority, law enforcement, intelligence and customs officers, border guards and port authorities.

5.4. The State should implement a policy encouraging persons to report to the competent authorities any suspicious or unusual activity potentially involving nuclear and other radioactive material.

MEDICAL SURVEILLANCE REPORTS

5.5. Most radiation injuries to members of the public caused by radioactive material have been accidental in nature. Nevertheless, the appearance of radiation injuries[15] may indicate involvement in a criminal or an unauthorized act with nuclear security implications or the preparation for such acts.

5.6. While respecting the principle of confidentiality between doctor and patient, health professionals should report the occurrence of any suspicious or unexplained radiation injury to the relevant competent authorities. Those authorities should ensure that all such reports are followed up to determine the cause of the injuries.

REPORTING REGULATORY NON-COMPLIANCE

5.7. In accordance with Ref. [5], authorized persons should promptly report non-compliances related to nuclear and other radioactive material to the relevant regulatory authority. Such reporting arrangements should provide an early alert of the possible loss of regulatory control over nuclear and other radioactive material, and should, therefore, be regarded as part of the arrangements for the detection of nuclear or other radioactive material out of regulatory control by information alert.

5.8. The regulatory authority should develop procedures and protocols to assist authorized persons to report regulatory non-compliances having nuclear security implications to other relevant competent authorities.

5.9. Competent authorities, including law enforcement bodies as appropriate, should make effective use of such reporting arrangements. An effective reporting process, under which all law enforcement bodies and regulatory authorities are informed immediately of regulatory non-compliances relating to nuclear or other radioactive material, allows these agencies to maintain an appropriate alert status and to analyse trends and patterns relating to possible threats.

---

[15] Recognition of radiation injuries could, therefore, be part of the syllabus for the training of health professionals. In addition, information on such injuries could be provided to those health professionals that are already practising their profession. Such information could be provided through short training courses or through the provision of information leaflets.

REPORTING LOSS OF REGULATORY CONTROL

5.10. As soon as an authorized person detects the loss of nuclear or other radioactive material, they should promptly report the loss of regulatory control to the relevant regulatory authority. Such reports should be treated as an alert of the loss of control over nuclear or other radioactive material and should, therefore, be regarded as part of detection through an information alert.

5.11. The regulatory authority that receives such a report should promptly inform other relevant competent authorities. Such competent authorities, including law enforcement bodies as appropriate, should make effective use of such reports. An effective reporting process, under which all law enforcement bodies and other competent authorities are informed of the loss of control of radioactive material, is an important element of detection through an information alert.

6. INITIAL ASSESSMENT OF ALARMS/ALERTS

6.1. An instrument alarm or an information alert should trigger an initial assessment. Procedures and protocols should be in place for the prompt initial assessment of an instrument alarm and an information alert by designated staff from relevant organizations. A generic alarm/alert assessment and response process is shown in Fig. 3.

INITIAL ASSESSMENT OF ALARMS

6.2. An instrument alarm will normally correspond to one of three conditions[16]:

— False alarm: This occurs when there is an alarm but the subsequent assessment reveals no presence of nuclear or other radioactive material.
— Innocent alarm: This occurs when there is an alarm but the subsequent assessment reveals the presence of radioactive material that is not out of regulatory control. Examples include cases where regulatory control is not applicable, such as items containing NORM or people recently subjected to medical procedures involving radioactive material, and those where the material is under the control prescribed by regulation, such as industrial devices incorporating radioactive material. Such industrial devices should have formal transport documents and appropriate package labelling.
— Confirmed non-innocent alarm: Nuclear or other radioactive material is present and is out of regulatory control. In this case, appropriate response measures should be initiated in accordance with the national response plan [5].

6.3. Technical support should be available for assessing alarms and assisting in the initial assessment activities. Technical support in the form of expert support teams should include persons equipped and trained to use basic radiation monitoring instruments for categorization of radioactive material and to perform radiation

[16] State of the art technology can automatically recognize:
— NORM;
— Common medical isotopes;
— Common industrial isotopes;
— Nuclear material.

Detection instruments cannot usually determine uranium isotope ratios but they are able to distinguish uranium ore from human-made processed material [17].

protection tasks. Technical support organizations may provide the necessary expertise and coordinate the support needed for the initial assessment of alarms.

INITIAL ASSESSMENT OF ALERTS

6.4. In the case of an information alert, the initial assessment should include:

— Assessing the quality and credibility of the information;
— Considering verifying the national inventory of nuclear and other radioactive material;
— Identifying a possible location of the nuclear and other radioactive material, and arranging a search;
— Searching for the nuclear or other radioactive material;
— Initiating response measures[17].

6.5. Decisions on whether to institute a specific search for the nuclear or other radioactive material and the priority to be given to the search should be determined by factors such as:

— The hazard associated with the material, in particular, whether it is nuclear material or other radioactive material such as categories 1–3 of the categorization of radioactive sources [18].
— The estimated time elapsed between the loss or theft of nuclear or other radioactive material and the alert: Reporting should be prompt, but there may, for example, have been some delay between the loss or theft taking place and recognition that the material was missing.
— The amount of information available that might be used to direct the search.
— The resources, in terms of personnel, instrumentation and costs, needed to undertake the search.

[17] Response measures could include heightened border control activities (e.g. if an information alert indicates proximity to the border) or targeted law enforcement operation (e.g. if in a State's interior).

FIG. 3. Generic functional flow for initial assessment of alarms and alerts.

7. IMPLEMENTATION FRAMEWORK

7.1. This section describes the initial steps towards implementing an effective nuclear security detection architecture to support the implementation of the systems and measures, and sustain and improve the effectiveness of those systems and measures over time, as well as providing immediate improvements to national capabilities.

ROLES AND RESPONSIBILITIES

7.2. The establishment of a nuclear security detection architecture should include establishing roles and responsibilities for its management, operation and maintenance. It may also call for the development of new and additional capabilities. Many levels and agencies of government, as well as private entities, may be involved.

7.3. The establishment of a nuclear security detection architecture within the national nuclear security regime should involve the following actions:

— Development of a national nuclear security detection strategy;
— Design of the national nuclear security detection architecture;
— Design of national policy and programmes to implement the nuclear security detection architecture;
— Ensuring the coordinating body or mechanism and relevant competent authorities have, or can obtain, legal authority to meet their responsibilities;
— Identification of the physical, human and financial resources needed and provision of these to the competent authorities to enable them to effectively meet their responsibilities;
— Assignment of responsibility for implementing detection systems;
— Development of detection systems including instrument deployment plans;
— Establishment of a process for evaluating and assessing the management of the nuclear security detection architecture, including the relevant elements at the national, regional and local levels;
— Establishment of a process for refining the implementation of the nuclear security detection architecture based on changes in threat and the results of performance evaluation over time;
— Consideration of the addition of an operations' centre and/or a technical support centre as part of the framework to play a key coordination and cooperation function.

INSTRUMENT DEPLOYMENT PLAN

7.4. Based on the detection strategy and within the framework of the national nuclear security detection architecture, the competent authorities could prepare an instrument deployment plan(s) based upon the assessed threat of criminal or unauthorized acts involving nuclear or other radioactive material out of regulatory control. Consideration should be given to the following:

— Monitoring for radiation at POEs at land borders, seaports and airports;
— Monitoring for radiation inside the country and searching for nuclear and other radioactive material out of regulatory control;
— Monitoring for radiation at venues for major public events and any other strategic locations that are considered to be vulnerable to attack using an IND, RDD or RED.

7.5. Criteria for the use of detection instruments should be based on appropriate considerations, including the following:

— The national threat assessment;
— The concept of operations;
— The type and quantity of nuclear or other radioactive material to be detected;
— The capability of customs, border control and other law enforcement personnel to operate radiation detection instruments and to respond to alarms at borders and in the domestic interior;
— The number of border crossing locations, seaports and airports to be screened;
— The volume of traffic and goods entering and leaving the country;
— The volume of domestic traffic between installations that produce, store, use or dispose of radioactive material;
— The number of events involving criminal or unauthorized acts within the country and immediate neighbouring countries;
— The financial implications of the various policy options.

7.6. Taking into account the above and the prioritization of available resources, the competent authorities should develop an appropriate detection instrument deployment plan, considering the following:

— Structural and organizational elements of the detection systems based on the principle of defence in depth. These could include locating detection systems on transport routes within the State, locations where the probability of detection is estimated to be maximized, or near to locations where nuclear or other radioactive material is produced, used, stored or disposed of. The

locations for monitoring at any particular border crossing should be the control or nodal points (such as customs checkpoints and weigh-bridges) where the flow of traffic is at its most dense. Consideration should also be given as to whether to monitor the transit points for the public or those for commercial vehicles or both. In all cases, consideration should be given to the degree of disruption caused by the monitoring.

— The operational and performance specifications of the detection instruments, in accordance with national and international standards and technical guidelines.
— The capabilities of, and constraints and limitations on detection instruments at both designated and undesignated air, land and water border crossing points.
— The potential for mobile and re-locatable detection systems to provide flexibility and adjustments to evolving threats.
— Detection requirements in support of law enforcement operations associated with information alerts.
— Additional measures for events of national significance, such as major public events, strategic locations and critical infrastructure.

7.7. The detection instrument deployment plan should include:

— Specifications, initial installation, calibration and acceptance testing of equipment, the setting up of a maintenance procedure, training and qualification of users and technical support staff, and systems and procedures for conducting a radiation survey or a radiation search for nuclear and other radioactive material out of regulatory control;
— Defining threshold levels of an instrument alarm;
— Establishing the concept of operations and procedures for performing initial alarm assessment and other secondary inspection actions such as location, identification, categorization and characterization of nuclear and other radioactive material, including obtaining technical support from experts to assist in the assessment of an alarm that cannot be resolved on site;
— Provision of sustainable supporting measures to ensure effective detection, including personnel training, equipment calibration, testing and maintenance, safe and secure disposition of discovered material, and documented response procedures.

CONCEPT OF OPERATIONS

7.8. The concept of operations for the nuclear security detection architecture should include procedures for routine operations, for responding to instrument alarms and information alerts in relation to detection of nuclear and other radioactive material and for assessing the threat and determining what, if any, actions are necessary.

7.9. The concept of operations should describe the functions and capabilities necessary to implement the nuclear security detection architecture. It should include a complete set of procedures and protocols to address the full range of possible cases related to the unauthorized movement of nuclear and other radioactive material [12].

7.10. Whether initiated by an instrument alarm or information alert, the concept of operations should apply a graded approach such that the response is commensurate with the severity of the situation as determined by a progression of assessment steps. In some cases, technical support may need to be provided from a location remote from that to which the alarm or alert relates. In other cases, experts may travel to the location in the form of a mobile expert support team to provide the necessary assistance.

7.11. The concept of operations should include consideration of appropriate radiation protection measures during the initial assessment of the alarm/alert and other response actions.

Technical specifications of detection instruments

7.12. Technical specifications for instruments should take account of the detection capability needed to resolve the types of alarm expected based on the national threat assessment. Specifications should be guided by the concepts of operations and adherence to international [13] or national standards, the type(s) of radiation expected to be detected, and functional considerations such as the sensitivity required, susceptibility to false and innocent alarms, ability to withstand exposure to environmental factors, installation and/or deployment considerations, ease of training of staff, ease of maintenance and sustainability of the instruments.

7.13. In addition, investigation levels and alarm setting levels should be established for the detection equipment that is to be used. These should be established taking account of:

— Background radiation levels;
— The nature of the vehicles, objects or persons to be screened;
— Transit times through the monitoring zone;
— The nature of any cargo;
— The density of any material which would affect self-shielding;
— The type of detector that has been installed.

Installation, acceptance testing, calibration and maintenance

7.14. Detection instruments should be calibrated prior to use for the first time and subject to an acceptance test to confirm the required performance specifications. In addition, calibration, performance testing and preventive maintenance should be carried out periodically by qualified experts, based on international or national standards and advice from the manufacturer of the equipment. Daily checks to verify that the equipment can detect appropriate increases in radiation intensity can confirm the availability and proper operation of the detection instruments. Records should be kept of all calibrations, evaluations and daily checks.

7.15. A maintenance plan for the equipment should be established at the time of installation and be based on the international standards and advice from the manufacturer of the equipment.

EDUCATION, AWARENESS, TRAINING AND EXERCISES

7.16. Comprehensive education, awareness and training programmes should be put in place for personnel with responsibility for operations, detection, assessment and maintenance. Training for, and raising awareness of, the nuclear security detection architecture involves many types of personnel. The curriculum design should account for the disparate backgrounds of the personnel and provide them with the appropriate level of competence or awareness for their job duties [19].

7.17. The existing nuclear security detection architecture and the individual's role therein will often determine whether an education, awareness or training programme is the best way to develop and sustain a capability. A needs assessment should be conducted to define the training, human and financial

resources necessary to support the nuclear security detection architecture. The needs assessment and subsequent actions should include the following steps:

— Determine training goals based on the national threat assessment and the associated concept of operations developed to counter those threats, and identify the related training objectives and factors that could affect the nuclear security detection architecture;
— Perform a job task analysis to determine the specific skills, qualification and certification requirements for all personnel with a role in the development, implementation and operation of the various elements of the nuclear security detection architecture;
— Evaluate existing training programmes to determine elements that could be used for training in detection instruments, techniques and procedures;
— Determine what international assistance programmes may be available to raise awareness and aid the implementation of education and training programmes;
— Establish a training schedule that accounts for staff rotation, staff attrition and periodic performance evaluations;
— Implement the training programme, applying adult learning principles and progressive training methodologies that include subject matter expert instructors, as well as customized and realistic training props and job aids;
— Establish a process for ongoing evaluation of training activities, courses and providers.

7.18. Well planned exercises and performance evaluations are useful in assessing local and national nuclear security detection capabilities to identify and correct deficiencies in equipment, concept of operations and training. An exercise programme should be designed to continually improve these capabilities in a manner that complements other performance measurement tools, such as drills and inspections. Exercise programmes should be appropriate to the size of the national nuclear security detection effort, its level of maturity and its integration with other security, border control and counter-smuggling activities. The results of exercises should be carefully recorded and assessed by programme officials. A wide variety of training exercises can be used, including table-top exercises, simulations, functional exercises and announced or unannounced field exercises.

7.19. Depending on their scope and objective, exercises could involve the participation of multiple local and national agencies, ministries, law enforcement and public safety officials, private partners and other key stakeholders, as well as regional and international participants. Exercise rules, roles and responsibilities

should be established in advance, along with the methodology for evaluating results.

7.20. In addition to conducting evaluation exercises, formal inspections or assessments should be undertaken to ensure compliance with existing processes and activities defined by the nuclear security detection architecture.

SUSTAINABILITY

7.21. Sustainability is a key consideration for the nuclear security detection architecture. Significant planning and commitment of resources, both financial and human, are needed to ensure the long term operational effectiveness of national capabilities for detection of nuclear and other radioactive material out of regulatory control. Achieving effective operations over time will require a focus on maintaining the appropriate level of detection capabilities, commensurate with the national threat assessment. Attention should also be given to day to day operations, maintenance, quality control and continuous system improvements, as well as to flexibility to adapt to evolving threats.

7.22. Consideration of the sustainability of human resources should take into account personnel rotation and attrition within different authorities, as well as the training requirements for existing and new personnel. Plans should also ensure that there will be sufficient numbers of qualified personnel to operate and maintain equipment and assess instrument alarms and information alerts.

7.23. To sustain performance of technical equipment, resource estimation and planning should cover the associated platform and full life cycle requirements, including recapitalization and essential product improvements. Comprehensive maintenance plans should be established that include preventive and corrective maintenance and an inventory of spare parts.

7.24. The sustainability of instrument performance affects the system's overall reliability, availability, downtime and cost of operation. Competent authorities should consider:

— Establishing a plan for monitoring the usage, configuration control and inventory of instrumentation;
— Establishing appropriate performance monitoring, calibration and periodic testing;

— Identifying critical components[18] (hardware, firmware and data collection and evaluation software) for each detection instrument and their expected lifetimes;
— Investigating possible suppliers for the critical components and determining their availability;
— Preparing a long term plan and identifying measures to ensure supply and flexibility to accommodate possible modifications, adaptations and upgrades.

[18] Within the context of this publication, 'critical components' are hardware and software components of an instrument with limited availability in time or obsolescence and need to be considered for sustaining the nuclear security detection system.

Appendix

NUCLEAR SECURITY DETECTION ARCHITECTURE 'CHECKLIST'

Item	Task	Paragraphs	Status
	National detection strategy		
1	Articulate national detection strategic goals and objectives.	2.7–2.14	
2	Conduct a national threat assessment to inform detection strategy.	2.9–2.11	
3	Determine scope and priority of the nuclear security detection architecture.	2.7–2.14	
4	Endorse the detection strategy by the coordinating body or mechanism with responsibility for the overall coordination of the national nuclear security architecture.	2.7, 7.2–7.3	
5	Define overall roles and responsibilities.	2.7, 2.17, 7.2–7.3	
6	Establish risk informed approach to evaluate, prioritize investments and resource allocations, and inform strategic decision making.	2.7–2.14	
7	Communicate various elements of the national detection strategy to all relevant stakeholders in an appropriate manner.	2.14	
	Assessment and evaluation of national capabilities		
8	Perform an initial capabilities and resource assessment (i.e. 'baseline' assessment), including financial capabilities, technological capabilities and resources, operational information capabilities, trained personnel, technical experts and general resources.	2.18–2.28, 3.1–3.3	
9	Perform a needs assessment (i.e. identify gaps and vulnerabilities), through a comparison of threat assumptions and targets with initial capabilities and resource assessment.	3.1–3.3	
10	Postulate a range of options, including detection systems and measures as well as solutions, to address identified gaps and vulnerabilities.	3.1–3.3	
11	Evaluate and prioritize the risk reduction benefits, costs and other impacts of the identified options.	3.1–3.3	
12	Determine necessary detection technologies, legal/regulatory framework, and authorities to execute country-specific nuclear security detection architecture functions.	2.15–2.17, 4.14–4.19, 7.2–7.7	

Item	Task	Paragraphs	Status
13	Subsequent to implementation, evaluate the effectiveness of the solution measures and identify additional options and recommendations as appropriate.	3.1–3.18	
	Planning and organization		
14	Ensure that the coordinating mechanism and relevant competent authorities have or obtain the legal authority to carry out their roles and responsibilities.	7.2–7.3	
15	Establish a legal and regulatory framework built upon pre-existing laws (to the extent feasible) covering all elements of the nuclear security detection architecture.	2.15–2.17	
16	Establish operational priorities, policies and requirements.	2.7–2.14, 4.14–4.15, 7.2–7.3	
17	Define roles and responsibilities at the agency or organizational level, and describe the conduct of day to day operations.	7.2–7.3	
18	Identify the physical, human and financial resources required, and provide them to the relevant competent authorities to implement the relevant parts of the nuclear security detection architecture.	3.17, 7.2–7.3	
19	Pursue and become party to international and regional treaties or agreements of cooperation, as appropriate.	2.29	
20	Identify need for regional and/or international cooperation/support (e.g. detection instruments, technical support) where appropriate.	2.29	
21	Identify and document what acts are authorized and not authorized.	2.7–2.17	
22	Provide adequate criminal and/or civil penalties for illicit trafficking or misuse of such materials.	2.15–2.17	
23	Identify relevant stakeholders, other agencies and authorities needed to inform and liaise with the relevant authorities responsible for the various elements of the nuclear security detection architecture and define the mechanisms of coordination between these elements of the overall strategy.	2.18–2.25, 2.27–2.28, 7.2–7.3	
24	Ensure sufficient numbers of qualified personnel to operate and maintain the detection instruments.	7.16–7.24	
25	Establish sustainable funding for implementation of the nuclear security detection architecture.	3.1–3.4, 7.2–7.7, 7.21–7.24	

Item	Task	Paragraphs	Status
26	Establish a process for evaluating and assessing the management of nuclear security detection architecture activities at national, sub-national and local levels.	7.2–7.3	
27	Verify assumptions made in planning and organization of the nuclear security detection architecture, including what the detection architecture should do as well as what it cannot do.	2.7–2.14, 3.1–3.3	
28	Ensure sustainability of human resources, taking into account personnel rotations and attrition as well as training requirements.	7.21–7.24	
29	Consider the addition of an operations and analysis centre or centres as part of the information coordination mechanism of the nuclear security detection architecture.	3.13–3.18, 5.2–5.4, 7.2–7.3	
Design of detection architecture			
30	State and prioritize the high level implementation concepts for the nuclear security detection architecture.	2.7–2.14	
31	Utilize existing national activities, capabilities and systems in the nuclear security detection architecture (e.g. existing licensing, inspection, customs and border control, law enforcement, analysis and operational information capabilities).	2.15–2.28	
32	Utilize identified and necessary public and private sector capabilities and resources in the nuclear security detection architecture.	2.18–2.28	
33	Develop an operational concept that translates the strategic goals and objectives (from the national level nuclear security detection strategy) into authorized, pre-established procedures across all relevant pathways for responding to instrument alarms and information alerts.	3.2–3.3, 7.2–7.3, 7.8–7.15	
34	Set technical investment policies and priorities.	4.14–4.15	
35	Taking into account the exterior layers, establish and utilize a layered approach to security that utilizes detection systems and measures at strategic locations at the border and domestic interior.	3.6–3.12	
36	Establish mechanisms for collection of operational information, analysis and sharing capabilities.	3.1–3.3, 5.2–5.11, 6.4–6.5	
37	Establish cooperative monitoring practices for reporting and information sharing with neighbouring States and the IAEA on a voluntary basis.	2.29	

Item	Task	Paragraphs	Status
38	Establish a process for refining the implementation of the nuclear security detection architecture based on evolutions in the threat, including scalability, and the results of measured performance during periodic inspections and exercises.	7.2–7.3	
	Information management		
39	Categorize nuclear security sensitive information (threat information, detections, technical assessments, etc.).	3.19–3.30	
40	Establish an information management policy, including the rules for protecting the confidentiality and integrity of sensitive information, and for dissemination of such information.	3.19–3.30	
41	Develop information sharing standards and common data formats and protocols for timely exchange of information.	3.13–3.18, 3.26–3.28	
42	Create a tiered structure of information flow.	3.26–3.28	
43	Create an information delivery system to national, sub-national and local decision makers, relevant managers and operators.	3.26–3.28	
44	Ensure data integrity, information and network security.	3.29–3.30	
45	Integrate information from detection instruments and information alerts.	3.19–3.30, 5.2–5.11	
46	Develop or identify necessary technical support capability for detection under country specific nuclear security detection architecture and/or establish access to international expert technical and support capabilities, as appropriate.	3.1–3.3, 3.13–3.18, 6.2–6.5	
	Detection by instruments		
47	Set technology requirements and standards consistent with the national level deployment plan.	4.2–4.15	
48	Ensure detection technology investments are consistent with the national level detection strategy.	4.14–4.15, 7.4–7.7	
49	Based on established criteria, develop a detection instrument deployment plan at designated POEs, strategic locations at borders and inside the country and at major public venues, ports, etc.	7.4–7.7	
50	As part of the detection instrument deployment plan, ensure a suite of complementary fixed, mobile and re-locatable passive and active detection systems appropriate to specific applications (e.g. POEs, and temporary locations in support of major public events).	4.2–4.12, 7.4–7.7	

Item	Task	Paragraphs	Status
51	Based on a graded approach, evaluate performance requirements in the acquisition/deployment of detection systems for detection, localization and identification.	3.5–3.18, 4.16–4.17, 6.2–6.3	
52	Evaluate detectors that provide different capabilities depending on operational requirements, including portable, vehicle based and stationary (e.g. radiation portal monitors).	4.16–4.17	
53	Evaluate deployment of detection instruments of varying sensitivity and performance.	4.16–4.17	
54	Conduct laboratory testing and evaluation of equipment for technical feasibility as appropriate (e.g. probability of detection, identification accuracy and precision) or have access to international recommendations.	3.13–3.18, 4.16–4.17, 7.14–7.15	
55	Field test equipment for operational suitability (e.g. range, re-location/mobility, environmental factors).	4.16–4.17	
56	Establish appropriate alarm threshold levels and ensure periodic calibration, performance testing and maintenance.	7.12–7.15	
57	Understand the technical attributes and limitations of detection instruments — such as probability of detection, identification capability, performance and mobility.	4.18–4.19	
58	As appropriate, develop research agendas that respond to enduring technical challenges and that promise improvements in deployed technical capabilities.	4.18–4.19	
59	Pursue international and other partnerships for research and development as appropriate.	4.18–4.19	
60	Develop a sustainability plan for detection instruments.	7.21–7.24	
	Concept of operations		
61	Establish procedures for prompt reporting of regulatory non-compliance of nuclear and other radioactive material, loss of regulatory control and (as appropriate) suspicious radiation injuries.	5.5–5.11	
62	Describe the processes for employing instruments, operators and competent authorities for meeting the objectives of the nuclear security detection strategy.	7.8–7.15	
63	Establish procedures for the assessment of alarms, notification and technical support.	6.2–6.5	
64	Establish requirements, procedures and protocols for reporting instrument alarms and information alerts to relevant competent authorities.	5.2–5.11, 6.2–6.5, 7.8–7.15	

Item	Task	Paragraphs	Status
65	Ensure consistency with the response procedures, protocols and scenarios for effective nuclear security detection and response systems and measures.	7.8–7.15	
66	As part of ongoing threat assessment, collect and analyse relevant operational information.	5.2–5.4	
	Awareness, training and exercises		
67	Determine training goals based on the national threat assessment and the associated concept of operations.	3.17, 7.16–7.20	
68	Perform a job/task analysis to determine the specific skill, qualification and certification requirements for all personnel with a role in the nuclear security detection architecture.	7.16–7.20	
69	Account for training requirements for both existing and new personnel.	7.21–7.24	
70	Evaluate existing training programmes to determine elements that could be leveraged for training in detection instruments, techniques and procedures.	3.13–3.18, 7.16–7.20	
71	Determine what international assistance programmes may be available.	2.29	
72	Establish a training schedule that accounts for staff rotation, staff attrition and periodic performance evaluations.	7.16–7.20	
73	Implement the training programme, applying appropriate learning principles and methodologies for all disciplines and expertise levels.	7.16–7.20	
74	Establish a process for ongoing evaluation of training activities, courses and providers.	7.16–7.20	
75	Identify appropriate stakeholders for exercises based on scope and objective.	7.16–7.20	
76	Establish exercise roles, rules, responsibilities and evaluation methodology.	7.16–7.20	
77	Conduct formal internal and external inspections or assessment to ensure compliance with existing processes and activities.	7.16–7.20	
	Nuclear security culture and trustworthiness		
78	Promote culture of security awareness across all competent authorities and relevant stakeholders.	3.32–3.33	
79	Establish policies and procedures requiring all personnel having responsibilities to be subject to an appropriate trustworthiness check.	3.31	
80	Regularly assess the trustworthiness of the responsible personnel.	3.31	

REFERENCES

[1] INTERNATIONAL ATOMIC ENERGY AGENCY, Incident and Trafficking Database, Fact Sheet, IAEA, http://www-ns.iaea.org/downloads/security/itdb-fact-sheet.pdf

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

[3] 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).

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

[5] 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).

[6] INTERNATIONAL ATOMIC ENERGY AGENCY, The International Legal Framework for Nuclear Security, IAEA International Law Series No. 4, IAEA, Vienna (2011).

[7] GLOBAL INITIATIVE TO COMBAT NUCLEAR TERRORISM, Model Guidelines Document for Nuclear Detection Architectures, United States Department of Homeland Security, Domestic Nuclear Detection Office, U.S. Government Printing Office: 2010-634-986 (2009).

[8] INTERNATIONAL ATOMIC ENERGY AGENCY, Radiation Protection and Safety of Radiation Sources: International Basic Safety Standards — Interim Edition, IAEA Safety Standards Series No. GSR Part 3 (Interim), IAEA, Vienna (2011).

[9] INTERNATIONAL ATOMIC ENERGY AGENCY, Security in the Transport of Radioactive Material, IAEA Nuclear Security Series No. 9, IAEA, Vienna (2008).

[10] INTERNATIONAL ATOMIC ENERGY AGENCY, Security of Radioactive Sources, IAEA Nuclear Security Series No. 11, IAEA, Vienna (2009).

[11] INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Culture, IAEA Nuclear Security Series No. 7, IAEA, Vienna (2008).

[12] INTERNATIONAL ATOMIC ENERGY AGENCY, Combating Illicit Trafficking in Nuclear and Other Radioactive Material, IAEA Nuclear Security Series No. 6, IAEA, Vienna (2008).

[13] INTERNATIONAL ATOMIC ENERGY AGENCY, Technical and Functional Specifications for Border Monitoring Equipment, IAEA Nuclear Security Series No. 1, IAEA, Vienna (2006).

[14] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Radiation Protection Instrumentation — Alarming Personal Radiation Devices (PRD) for detection of Illicit Trafficking of Radioactive Material, IEC 62401, Geneva (2001).
[15] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Radiation Protection Instrumentation — Spectroscopy-based Alarming Personal Radiation Devices (SPRD) for Detection of Illicit Trafficking of Radioactive Material, IEC 62618, Geneva (2011).
[16] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Radiation Protection Instrumentation — Hand-held Instruments for the Detection and Identification of Radionuclides and Additionally for the Indication of Ambient Dose-equivalent Rate from Photon Radiation, IEC 62327, Geneva (2006).
[17] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Radiation Protection Instrumentation — Spectroscopy-based Portal Monitors Used for the Detection and Identification of Illicit Trafficking of Radioactive Material, IEC 62484, Geneva (2010).
[18] INTERNATIONAL ATOMIC ENERGY AGENCY, Categorization of Radioactive Sources, IAEA Safety Standards Series No. RS-G-1.9, IAEA, Vienna (2005).
[19] INTERNATIONAL ATOMIC ENERGY AGENCY, Educational Programme in Nuclear Security, IAEA Nuclear Security Series No. 12, IAEA, Vienna (2010).

GLOSSARY

detection. Awareness of criminal act(s) or unauthorized act(s) with nuclear security implications, or measurement(s) indicating the unauthorized presence of nuclear material or other radioactive material at an associated facility or associated activity or a strategic location.

detection instrument. A complete functional system, being a combination of hardware and software (or firmware) supported by procedures for installation, calibration, maintenance and operation, used for detecting nuclear material or other radioactive material.

detection measure. Measures intended to detect a criminal or an unauthorized act with nuclear security implications.

detection system. An integrated set of detection measures including capabilities and resources necessary for detection of a criminal act or an unauthorized act with nuclear security implications.

false alarm. An alarm found by subsequent assessment not to have been caused by the presence of nuclear or radioactive material.

improvised nuclear device. A device incorporating radioactive materials designed to result in the formation of a nuclear-yield reaction. Such devices may be fabricated in a completely improvised manner or may be an improvised modification to a nuclear weapon.

information alert. Time sensitive reporting that could indicate a nuclear security event requiring assessment, and may come from a variety of sources, including operational information, medical surveillance, accounting and consigner/consignee discrepancies, border monitoring, etc.

innocent alarm. An alarm found by subsequent assessment to have been caused by nuclear or other radioactive material under regulatory control or exempt or excluded from regulatory control.

instrument alarm. A signal from a detection instrument or set of such instruments that could indicate a nuclear security event requiring assessment. An instrument alarm may come from devices that are portable or deployed at fixed locations and operated to augment normal commerce protocols and/or in a law enforcement operation.

major public event. A high profile event that a State has determined to be a potential target.

nuclear material. Nuclear material is defined to be any material that is either special fissionable material or source material as defined in Article XX of the IAEA Statute.

nuclear security event. An event that has the potential or actual implications for nuclear security that must be addressed.

nuclear security measure. A measure intended to prevent a nuclear security threat from completing criminal or intentional unauthorized acts involving or directed at nuclear material, other radioactive material, associated facilities, or associated activities or to detect or respond to nuclear security events.

nuclear security system. An integrated set of nuclear security measures.

point of entry and/or exit (POE). An officially designated place on the land border between two States, seaport, international airport or other point where travellers, means of transport and/or goods are inspected. Often, customs and immigration facilities are provided at these POEs. An undesignated POE is any air, land or water crossing point that is not officially designated for travellers and/or goods by the State, such as green borders, sea-shores and local airports.

radiation exposure device. A device with radioactive material designed to intentionally expose members of the public to radiation.

radiation search. The set of activities to detect and identify suspicious nuclear or other radioactive material out of regulatory control and to determine its location.

radiation survey. Activities to map the radiation background of natural and human-made radioactive material in an area or to facilitate later search activities.

radioactive material. Any material designated in national law, regulation or by a regulatory body as being subject to regulatory control because of its radioactivity.

radiological dispersal device. A device to spread radioactive material using conventional explosives or other means.

regulatory control. Any form of institutional control applied to nuclear material or other radioactive material, associated facilities or associated activities by any competent authority as required by the legislative and regulatory provisions related to safety, security and safeguards.

— *Explanation:* The phrase 'out of regulatory control' is used to describe a situation where nuclear material or other radioactive material is present in sufficient quantity that it should be under regulatory control, but control is absent, either because controls have failed for some reason or they never existed.

response. All of the activities by a State that involve assessing and responding to a nuclear security event.

response measure. A measure intended to assess an alarm/alert and to respond to a nuclear security event.

response system. An integrated set of response measures including capabilities and resources for assessing the alarms/alerts and response to a nuclear security event.

sensitive information. Information, in whatever form, including software, the unauthorized disclosure, modification, alteration, destruction or denial of use of which could compromise nuclear security.

strategic location. A location of high security interest in the State which is a potential target for terrorist attacks using nuclear material or other radioactive material, or a location at which nuclear material or other radioactive material that is out of regulatory control is located.

target. Nuclear material, other radioactive material, associated facilities, associated activities, or other locations or objects of potential exploitation by a nuclear security threat, including major public events, strategic locations, sensitive information and sensitive information assets.

IAEA
International Atomic Energy Agency

Where to order IAEA publications

In the following countries IAEA publications may be purchased from the sources listed below, or from major local booksellers. Payment may be made in local currency or with UNESCO coupons.

AUSTRALIA
DA Information Services, 648 Whitehorse Road, MITCHAM 3132
Telephone: +61 3 9210 7777 • Fax: +61 3 9210 7788
Email: service@dadirect.com.au • Web site: http://www.dadirect.com.au

BELGIUM
Jean de Lannoy, avenue du Roi 202, B-1190 Brussels
Telephone: +32 2 538 43 08 • Fax: +32 2 538 08 41
Email: jean.de.lannoy@infoboard.be • Web site: http://www.jean-de-lannoy.be

CANADA
Bernan Associates, 4501 Forbes Blvd, Suite 200, Lanham, MD 20706-4346, USA
Telephone: 1-800-865-3457 • Fax: 1-800-865-3450
Email: customercare@bernan.com • Web site: http://www.bernan.com

Renouf Publishing Company Ltd., 1-5369 Canotek Rd., Ottawa, Ontario, K1J 9J3
Telephone: +613 745 2665 • Fax: +613 745 7660
Email: order.dept@renoufbooks.com • Web site: http://www.renoufbooks.com

CHINA
IAEA Publications in Chinese: China Nuclear Energy Industry Corporation, Translation Section, P.O. Box 2103, Beijing

CZECH REPUBLIC
Suweco CZ, S.R.O., Klecakova 347, 180 21 Praha 9
Telephone: +420 26603 5364 • Fax: +420 28482 1646
Email: nakup@suweco.cz • Web site: http://www.suweco.cz

FINLAND
Akateeminen Kirjakauppa, PO BOX 128 (Keskuskatu 1), FIN-00101 Helsinki
Telephone: +358 9 121 41 • Fax: +358 9 121 4450
Email: akatilaus@akateeminen.com • Web site: http://www.akateeminen.com

FRANCE
Form-Edit, 5, rue Janssen, P.O. Box 25, F-75921 Paris Cedex 19
Telephone: +33 1 42 01 49 49 • Fax: +33 1 42 01 90 90
Email: formedit@formedit.fr • Web site: http://www. formedit.fr

Lavoisier SAS, 145 rue de Provigny, 94236 Cachan Cedex
Telephone: + 33 1 47 40 67 02 • Fax +33 1 47 40 67 02
Email: romuald.verrier@lavoisier.fr • Web site: http://www.lavoisier.fr

GERMANY
UNO-Verlag, Vertriebs- und Verlags GmbH, Am Hofgarten 10, D-53113 Bonn
Telephone: + 49 228 94 90 20 • Fax: +49 228 94 90 20 or +49 228 94 90 222
Email: bestellung@uno-verlag.de • Web site: http://www.uno-verlag.de

HUNGARY
Librotrade Ltd., Book Import, P.O. Box 126, H-1656 Budapest
Telephone: +36 1 257 7777 • Fax: +36 1 257 7472 • Email: books@librotrade.hu

INDIA
Allied Publishers Group, 1st Floor, Dubash House, 15, J. N. Heredia Marg, Ballard Estate, Mumbai 400 001,
Telephone: +91 22 22617926/27 • Fax: +91 22 22617928
Email: alliedpl@vsnl.com • Web site: http://www.alliedpublishers.com

Bookwell, 2/72, Nirankari Colony, Delhi 110009
Telephone: +91 11 23268786, +91 11 23257264 • Fax: +91 11 23281315
Email: bookwell@vsnl.net

ITALY
Libreria Scientifica Dott. Lucio di Biasio “AEIOU”, Via Coronelli 6, I-20146 Milan
Telephone: +39 02 48 95 45 52 or 48 95 45 62 • Fax: +39 02 48 95 45 48
Email: info@libreriaaeiou.eu • Website: www.libreriaaeiou.eu

JAPAN
Maruzen Company Ltd, 1-9-18, Kaigan, Minato-ku, Tokyo, 105-0022
Telephone: +81 3 6367 6079 • Fax: +81 3 6367 6207
Email: journal@maruzen.co.jp • Web site: http://www.maruzen.co.jp

REPUBLIC OF KOREA
KINS Inc., Information Business Dept. Samho Bldg. 2nd Floor, 275-1 Yang Jae-dong SeoCho-G, Seoul 137-130
Telephone: +02 589 1740 • Fax: +02 589 1746 • Web site: http://www.kins.re.kr

NETHERLANDS
De Lindeboom Internationale Publicaties B.V., M.A. de Ruyterstraat 20A, NL-7482 BZ Haaksbergen
Telephone: +31 (0) 53 5740004 • Fax: +31 (0) 53 5729296
Email: books@delindeboom.com • Web site: http://www.delindeboom.com

Martinus Nijhoff International, Koraalrood 50, P.O. Box 1853, 2700 CZ Zoetermeer
Telephone: +31 793 684 400 • Fax: +31 793 615 698
Email: info@nijhoff.nl • Web site: http://www.nijhoff.nl

Swets and Zeitlinger b.v., P.O. Box 830, 2160 SZ Lisse
Telephone: +31 252 435 111 • Fax: +31 252 415 888
Email: infoho@swets.nl • Web site: http://www.swets.nl

NEW ZEALAND
DA Information Services, 648 Whitehorse Road, MITCHAM 3132, Australia
Telephone: +61 3 9210 7777 • Fax: +61 3 9210 7788
Email: service@dadirect.com.au • Web site: http://www.dadirect.com.au

SLOVENIA
Cankarjeva Zalozba d.d., Kopitarjeva 2, SI-1512 Ljubljana
Telephone: +386 1 432 31 44 • Fax: +386 1 230 14 35
Email: import.books@cankarjeva-z.si • Web site: http://www.cankarjeva-z.si/uvoz

SPAIN
Díaz de Santos, S.A., c/ Juan Bravo, 3A, E-28006 Madrid
Telephone: +34 91 781 94 80 • Fax: +34 91 575 55 63
Email: compras@diazdesantos.es, carmela@diazdesantos.es, barcelona@diazdesantos.es, julio@diazdesantos.es
Web site: http://www.diazdesantos.es

UNITED KINGDOM
The Stationery Office Ltd, International Sales Agency, PO Box 29, Norwich, NR3 1 GN
Telephone (orders): +44 870 600 5552 • (enquiries): +44 207 873 8372 • Fax: +44 207 873 8203
Email (orders): book.orders@tso.co.uk • (enquiries): book.enquiries@tso.co.uk • Web site: http://www.tso.co.uk

On-line orders
DELTA Int. Book Wholesalers Ltd., 39 Alexandra Road, Addlestone, Surrey, KT15 2PQ
Email: info@profbooks.com • Web site: http://www.profbooks.com

Books on the Environment
Earthprint Ltd., P.O. Box 119, Stevenage SG1 4TP
Telephone: +44 1438748111 • Fax: +44 1438748844
Email: orders@earthprint.com • Web site: http://www.earthprint.com

UNITED NATIONS
Dept. I004, Room DC2-0853, First Avenue at 46th Street, New York, N.Y. 10017, USA
(UN) Telephone: +800 253-9646 or +212 963-8302 • Fax: +212 963-3489
Email: publications@un.org • Web site: http://www.un.org

UNITED STATES OF AMERICA
Bernan Associates, 4501 Forbes Blvd., Suite 200, Lanham, MD 20706-4346
Telephone: 1-800-865-3457 • Fax: 1-800-865-3450
Email: customercare@bernan.com · Web site: http://www.bernan.com

Renouf Publishing Company Ltd., 812 Proctor Ave., Ogdensburg, NY, 13669
Telephone: +888 551 7470 (toll-free) • Fax: +888 568 8546 (toll-free)
Email: order.dept@renoufbooks.com • Web site: http://www.renoufbooks.com

Orders and requests for information may also 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 2600 29302
Email: sales.publications@iaea.org • Web site: http://www.iaea.org/books

13-00813

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

NUCLEAR SECURITY RECOMMENDATIONS ON 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

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

NUCLEAR SECURITY SYSTEMS AND MEASURES FOR MAJOR PUBLIC EVENTS
IAEA Nuclear Security Series No. 18
STI/PUB/1546 (56 pp.; 2012)
ISBN 978–92–0–127010–8 Price: €30.00

The objective of this publication is to provide guidance to Member States for the development of, or improvement of nuclear security systems and measures for the detection of criminal or unauthorized acts with nuclear security implications involving nuclear and other radioactive material out of regulatory control. It describes the elements of an effective nuclear security detection architecture which is comprised of an integrated set of nuclear security systems and measures, and is based on an appropriate legal and regulatory framework for the implementation of the national detection strategy. The publication is an implementing guide within the IAEA Nuclear Security Series publications and is intended for use by national policy makers, legislative bodies, competent authorities, institutions, and individuals involved in the establishment, implementation, maintenance or sustainability of nuclear security systems and measures for the detection of nuclear and other radioactive material out of regulatory control.

INTERNATIONAL ATOMIC ENERGY AGENCY
VIENNA
ISBN 978–92–0–142910–0
ISSN 1816–9317