IAEA
International Atomic Energy Agency

IAEA NUCLEAR SECURITY SERIES

No. 47-T

Detection in a State's Interior of Nuclear and Other Radioactive Material out of Regulatory Control

Jointly sponsored by

EUROPOL, IAEA, ICPO-INTERPOL, UNICRI, UNOCT, UNODC

EUROPOL IAEA INTERPOL unicri

UNITED NATIONS OFFICE OF COUNTER-TERRORISM
UN Counter-Terrorism Centre (UNCCT)

UNODC
United Nations Office on Drugs and Crime

TECHNICAL GUIDANCE

IAEA NUCLEAR SECURITY SERIES

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

CATEGORIES IN THE IAEA NUCLEAR SECURITY SERIES

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

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

DRAFTING AND REVIEW

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

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

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

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

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

DETECTION IN A STATE'S INTERIOR 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
ANTIGUA AND BARBUDA
ARGENTINA
ARMENIA
AUSTRALIA
AUSTRIA
AZERBAIJAN
BAHAMAS
BAHRAIN
BANGLADESH
BARBADOS
BELARUS
BELGIUM
BELIZE
BENIN
BOLIVIA, PLURINATIONAL STATE OF
BOSNIA AND HERZEGOVINA
BOTSWANA
BRAZIL
BRUNEI DARUSSALAM
BULGARIA
BURKINA FASO
BURUNDI
CABO VERDE
CAMBODIA
CAMEROON
CANADA
CENTRAL AFRICAN REPUBLIC
CHAD
CHILE
CHINA
COLOMBIA
COMOROS
CONGO
COSTA RICA
CÔTE D'IVOIRE
CROATIA
CUBA
CYPRUS
CZECH REPUBLIC
DEMOCRATIC REPUBLIC OF THE CONGO
DENMARK
DJIBOUTI
DOMINICA
DOMINICAN REPUBLIC
ECUADOR
EGYPT
EL SALVADOR
ERITREA
ESTONIA
ESWATINI
ETHIOPIA
FIJI
FINLAND
FRANCE
GABON
GAMBIA
GEORGIA
GERMANY
GHANA
GREECE
GRENADA
GUATEMALA
GUINEA
GUYANA
HAITI
HOLY SEE
HONDURAS
HUNGARY
ICELAND
INDIA
INDONESIA
IRAN, ISLAMIC REPUBLIC OF
IRAQ
IRELAND
ISRAEL
ITALY
JAMAICA
JAPAN
JORDAN
KAZAKHSTAN
KENYA
KOREA, REPUBLIC OF
KUWAIT
KYRGYZSTAN
LAO PEOPLE'S DEMOCRATIC REPUBLIC
LATVIA
LEBANON
LESOTHO
LIBERIA
LIBYA
LIECHTENSTEIN
LITHUANIA
LUXEMBOURG
MADAGASCAR
MALAWI
MALAYSIA
MALI
MALTA
MARSHALL ISLANDS
MAURITANIA
MAURITIUS
MEXICO
MONACO
MONGOLIA
MONTENEGRO
MOROCCO
MOZAMBIQUE
MYANMAR
NAMIBIA
NEPAL
NETHERLANDS, KINGDOM OF THE
NEW ZEALAND
NICARAGUA
NIGER
NIGERIA
NORTH MACEDONIA
NORWAY
OMAN
PAKISTAN
PALAU
PANAMA
PAPUA NEW GUINEA
PARAGUAY
PERU
PHILIPPINES
POLAND
PORTUGAL
QATAR
REPUBLIC OF MOLDOVA
ROMANIA
RUSSIAN FEDERATION
RWANDA
SAINT KITTS AND NEVIS
SAINT LUCIA
SAINT VINCENT AND THE GRENADINES
SAMOA
SAN MARINO
SAUDI ARABIA
SENEGAL
SERBIA
SEYCHELLES
SIERRA LEONE
SINGAPORE
SLOVAKIA
SLOVENIA
SOUTH AFRICA
SPAIN
SRI LANKA
SUDAN
SWEDEN
SWITZERLAND
SYRIAN ARAB REPUBLIC
TAJIKISTAN
THAILAND
TOGO
TONGA
TRINIDAD AND TOBAGO
TUNISIA
TÜRKİYE
TURKMENISTAN
UGANDA
UKRAINE
UNITED ARAB EMIRATES
UNITED KINGDOM OF GREAT BRITAIN AND NORTHERN IRELAND
UNITED REPUBLIC OF TANZANIA
UNITED STATES OF AMERICA
URUGUAY
UZBEKISTAN
VANUATU
VENEZUELA, BOLIVARIAN REPUBLIC OF
VIET NAM
YEMEN
ZAMBIA
ZIMBABWE

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

IAEA NUCLEAR SECURITY SERIES No. 47-T

DETECTION IN A STATE'S INTERIOR OF NUCLEAR AND OTHER RADIOACTIVE MATERIAL OUT OF REGULATORY CONTROL

TECHNICAL GUIDANCE

JOINTLY SPONSORED BY THE
EUROPEAN UNION AGENCY FOR
LAW ENFORCEMENT COOPERATION,
INTERNATIONAL ATOMIC ENERGY AGENCY,
INTERNATIONAL CRIMINAL POLICE ORGANIZATION-INTERPOL,
UNITED NATIONS INTERREGIONAL CRIME AND JUSTICE
RESEARCH INSTITUTE,
UNITED NATIONS OFFICE OF COUNTER-TERRORISM AND
UNITED NATIONS OFFICE ON DRUGS AND CRIME

INTERNATIONAL ATOMIC ENERGY AGENCY
VIENNA, 2024

COPYRIGHT NOTICE

Publishing Section
International Atomic Energy Agency
Vienna International Centre
PO Box 100
1400 Vienna, Austria
tel.: +43 1 2600 22529 or 22530
email: sales.publications@iaea.org
www.iaea.org/publications

Printed by the IAEA in Austria
June 2024
STI/PUB/2084
https://doi.org/10.61092/iaea.2nzd-8c4d

IAEA Library Cataloguing in Publication Data

Names: International Atomic Energy Agency.
Title: Detection in a State's interior of nuclear and other radioactive material out of regulatory control / International Atomic Energy Agency.
Description: Vienna : International Atomic Energy Agency, 2024. | Series: nuclear security series, ISSN 1816–9317 ; no. 47-T | Includes bibliographical references.
Identifiers: IAEAL 24-01678 | ISBN 978-92-0-109724-8 (paperback : alk. paper) | ISBN 978-92-0-109824-5 (pdf) | ISBN 978-92-0-109924-2 (epub)
Subjects: LCSH: Radioactive substances — Detection. | Radioactive substances — Security measures. | Radioactive substances — Safety measures. | Nuclear nonproliferation.
Classification: UDC 341.67 | STI/PUB/2084

FOREWORD

by Rafael Mariano Grossi
Director General

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

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

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

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

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

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

EDITORIAL NOTE

Guidance issued in the IAEA Nuclear Security Series is not binding on States, but States may use the guidance to assist them in meeting their obligations under international legal instruments and in discharging their responsibility for nuclear security within the State.

Guidance expressed as 'should' statements is intended to present international good practices and to indicate an international consensus that it is necessary for States to take the measures recommended or equivalent alternative measures.

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

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

PREFACE

The IAEA Nuclear Security Series provides recommendations and guidance that States can use in establishing, implementing and maintaining their national nuclear security regimes.

IAEA Nuclear Security Series No. 15, Nuclear Security Recommendations on Nuclear and Other Radioactive Material out of Regulatory Control, provides recommendations to a State for the nuclear security of nuclear or other radioactive material that has been reported as being out of regulatory control, as well as for material that is lost, missing or stolen but has not been reported as such, or has been otherwise discovered. IAEA Nuclear Security Series No. 15 is jointly sponsored by the European Police Office (EUROPOL), the IAEA, the International Civil Aviation Organization (ICAO), the International Criminal Police Organization-INTERPOL (ICPO-INTERPOL), the United Nations Interregional Crime and Justice Research Institute (UNICRI), the United Nations Office on Drugs and Crime (UNODC) and the World Customs Organization (WCO).

The present publication provides more detailed guidance on meeting the recommendations set out in IAEA Nuclear Security Series No. 15. It addresses nuclear security detection systems and measures in a State's interior, with special consideration of planning detection operations, equipment deployment and human resources development.

This publication is jointly sponsored by the European Union Agency for Law Enforcement Cooperation (EUROPOL), the IAEA, the International Criminal Police Organization-INTERPOL (ICPO-INTERPOL), the United Nations Interregional Crime and Justice Research Institute (UNICRI), the United Nations Office of Counter-Terrorism (UNOCT) and the United Nations Office on Drugs and Crime (UNODC).

CONTENTS

1. INTRODUCTION

BACKGROUND

1.1. Paragraph 3.10 of IAEA Nuclear Security Series No. 20, Objective and Essential Elements of a State's Nuclear Security Regime [1], states:

> "A *nuclear security regime* ensures that *nuclear security systems* and *nuclear security measures* are in place at all appropriate organizational levels to detect and assess *nuclear security events* and to notify the relevant *competent authorities* so that appropriate response actions can be initiated, including:
>
> …….
>
> (c) At *major public events* or *strategic locations*, including locations of critical infrastructure, as designated by the State;
> (d) In searches for, recoveries of, or discoveries of *nuclear material* or *other radioactive material* that is missing or lost or otherwise out of *regulatory control*;
> (e) Within the State's territory or on board its ships or aircraft, and at its international borders."

The interior of a State covers the area within the State's national borders and includes urban and rural locations, transport hubs and arteries, national airports and internal waters.

1.2. IAEA Nuclear Security Series No. 15, Nuclear Security Recommendations on Nuclear and Other Radioactive Material out of Regulatory Control [2], provides recommendations to States on establishing or improving prevention, detection and response measures for nuclear and other radioactive material out of regulatory control. Reference [2] provides recommendations for the detection and assessment of instrument alarms and information alerts related to nuclear or other radioactive material out of regulatory control.

1.3. Building upon these recommendations, IAEA Nuclear Security Series No. 21, Nuclear Security Systems and Measures for the Detection of Nuclear and Other Radioactive Material out of Regulatory Control [3], describes how States can develop or improve systems and measures in order to detect criminal or intentional unauthorized acts with nuclear security implications involving nuclear and other radioactive material out of regulatory control.

1.4. IAEA Nuclear Security Series Nos 24-G, Risk Informed Approach for Nuclear Security Measures for Nuclear and Other Radioactive Material out of Regulatory Control [4], 34-T, Planning and Organizing Nuclear Security Systems and Measures for Nuclear and Other Radioactive Material out of Regulatory Control [5], and 18, Nuclear Security Systems and Measures for Major Public Events [6], provide guidance for systems and measures related to nuclear and other radioactive material out of regulatory control.

OBJECTIVE

1.5. The objective of this publication is to provide detailed guidance for developing and implementing systems and measures for the detection in a State's interior of nuclear and other radioactive material out of regulatory control.

1.6. The publication is intended to be used by competent authorities that have a role in designing, implementing and sustaining nuclear security systems and measures in a State's interior. These competent authorities may include law enforcement, national security organizations and defence forces, as well as medical services, emergency services, regulatory bodies, and technical and scientific expert support organizations.

SCOPE

1.7. This publication provides guidance on planning, implementing and evaluating systems and measures in a State in order to detect nuclear and other radioactive material out of regulatory control in the State's interior by means of instrument alarms and information alerts. The guidance covers the planning of detection operations, equipment deployment and human resource development.

1.8. This publication does not address nuclear security detection systems and measures at a State's borders. This is covered in IAEA Nuclear Security Series No. 44-T, Detection at State Borders of Nuclear and Other Radioactive Material out of Regulatory Control [7], with special consideration given to designated points of entry and/or exit, as well as to border areas.

1.9. This publication does not cover systems and measures for nuclear and other radioactive material under regulatory control, which is addressed in IAEA Nuclear Security Series Nos 13, Nuclear Security Recommendations on Physical

Protection of Nuclear Material and Nuclear Facilities [8], and 14, Nuclear Security Recommendations on Radioactive Material and Associated Facilities [9].

1.10. Detailed discussion of response activities, concerning situations in which nuclear or other radioactive material has been detected and a nuclear security event has been declared, is generally outside the scope of this publication. Relevant connections between activities undertaken during detection and response operations, as well as key preparatory actions during detection that could impact response activities, are covered herein. Further guidance on nuclear security related response activities is provided in IAEA Nuclear Security Series No. 37-G, Developing a National Framework for Managing the Response to Nuclear Security Events [10].

1.11. Recommendations on the identification and notification of a radiological emergency during detection activities and on the relevant activation of emergency response plans are provided in IAEA Safety Standards Series No. GSR Part 7, Preparedness and Response for a Nuclear or Radiological Emergency [11].

STRUCTURE

1.12. Section 2 provides information on detection in a State's interior as part of the national nuclear security detection architecture and presents the challenges and opportunities specific to a State's interior, as well as training considerations. Section 3 provides guidance on the design and implementation of detection operations in the interior of a State. Sections 4 and 5 describe the roles of information and equipment in the conduct of detection operations in the interior of a State. Annex I presents a list of radiation detection equipment that can be used for detection operations. Annex II provides an example of a template for developing a joint detection operations plan for nuclear and other radioactive material out of regulatory control. Annex III contains information on how to manage information alerts obtained from medical surveillance for the purpose of detecting criminal or intentional unauthorized acts involving material out of regulatory control.

2. DETECTION IN A STATE'S INTERIOR AS A COMPONENT OF THE NUCLEAR SECURITY DETECTION ARCHITECTURE

2.1. Paragraph 3.2 of Ref. [2] states:

> "As part of an overall framework, the State should establish and maintain effective executive, judicial, legislative and regulatory frameworks to govern the *detection* of and *response* to a criminal act, or an unauthorized act, with nuclear security implications involving any nuclear or other *radioactive material* that is out of *regulatory control*. Responsibilities should be clearly defined for implementing various elements of nuclear security and assigned to the relevant *competent authorities*".

2.2. A State should define in its detection strategy how the State plans to accomplish its detection mission in both the interior and at the borders. An integrated planning process for nuclear security systems and measures is described in Ref. [5], and additional information can be found in IAEA Nuclear Security Series No. 29-G, Developing Regulations and Associated Administrative Measures for Nuclear Security [12].

2.3. When a State designs and develops its national nuclear security detection architecture, it should apply the defence in depth principle and follow a multilayered approach "including measures at and between POEs [points of entry and/or exit] into the State, within the State and in other cooperating States" [3]. Defence in depth should consider incorporating not only a variety of locations for detection equipment (e.g. at border points, in the State's interior, in transregional locations), but also a mix of detection instruments (i.e. fixed, handheld and mobile detection systems), as well as physical screening and other defensive measures.

2.4. Reference [3] outlines a multilayered approach to designing the nuclear security detection architecture. Paragraph 3.8 of Ref. [3] defines the three primary layers as follows:

> "— 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 [points of entry and/or exit]) 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."

2.5. Paragraph 2.9 of Ref. [3] states that "The detection strategy should be based on a risk-informed approach and be reviewed and updated in accordance with changes to the threat assessment." A methodology for assessing threats, vulnerabilities and consequences related to material out of regulatory control is presented in Ref. [4]. A State should use information from the threat and risk assessment as a basis to direct detection operations in the interior for nuclear security related to nuclear and other radioactive material out of regulatory control. More specifically, this assessment should assist in the identification of locations and opportunities for screening and detection (e.g. interior transport routes, public transport hubs). The assessment might further inform the prioritization of strategic locations and potential targets to be protected by detection operations in the interior of the State.

2.6. Law enforcement, national security organizations, regulatory bodies and other organizations providing emergency services[1] are likely to have their own risk informed strategies to address traditional security threats and conventional risks. The threat and risk assessment for nuclear and other radioactive material out of regulatory control should therefore be coordinated with, and integrated into, existing threat and risk assessments, as well as national security and conventional emergency response strategies (e.g. counterterrorism, counter-intelligence, anti-organized crime strategies) at both the national and organizational levels.

2.7. Paragraph 3.12 of Ref. [2] states that (footnote omitted) "All nuclear security activities involving nuclear or other *radioactive material* that are out of *regulatory control* should be coordinated by a body or an effective mechanism in accordance with national legislation and regulations." All competent authorities

[1] The fire service or other civil protection services can be involved in emergencies during their routine work, prior to the declaration of a nuclear or radiological emergency, or during conventional emergency responses that do not involve the presence of radiation.

participating in detection activities in a State's interior should be included in the coordination mechanism. This coordination mechanism should do the following:

(a) Support the process of developing and implementing the interior layer of the national nuclear security detection strategy;
(b) Resolve potential disputes among authorities participating in detection activities;
(c) Ensure adequate training for all competent authorities;
(d) Establish sustainability mechanisms for the planning of resources and evaluation of operations needed to ensure the long term effectiveness of national capabilities for detection;
(e) Establish a mechanism for the exchange of operational information among competent authorities participating in detection in the interior;
(f) Ensure that appropriate information exchange channels with border monitoring agencies and relevant authorities in neighbouring countries are in place.

2.8. Paragraph 3.18 of Ref. [3] states:

> "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."

2.9. This data exchange infrastructure should include two way communication between different levels (e.g. strategic, operational, tactical) of an organization in order to guarantee that relevant threat information is shared at all levels. Differences in threat and risk perceptions in relation to the interior of a State should be clarified within the organization before information is shared with other organizations.

2.10. Multiple organizations with different responsibilities are involved in nuclear security operations. The organizational policies and procedures of these organizations should provide the basis for the operational level of the interior detection architecture of the State. As part of a broader nuclear security strategy, a joint detection operation plan could be developed for nuclear and other radioactive material out of regulatory control in the State's interior. This plan should involve

all competent authorities and other stakeholders[2] with roles and responsibilities in detection activities within the State's interior. Annex II provides an example template with the components to be included in such a plan.

CHALLENGES AND OPPORTUNITIES FOR DETECTION IN A STATE'S INTERIOR

2.11. The complexity, size and geography of a State's interior create specific challenges for the detection of nuclear and other radioactive material out of regulatory control. However, they also create opportunities to encounter and detect criminal or intentional unauthorized acts involving nuclear and other radioactive material out of regulatory control. States should address the challenges and exploit the opportunities that exist to develop the interior layer of the State's nuclear security detection architecture in an effective and efficient manner.

2.12. A wide range of criminal or intentional unauthorized acts involving nuclear or other radioactive material out of regulatory control can occur in a State's interior, with or without nuclear or other radioactive material, devices (i.e. improvised nuclear devices, radiological dispersal devices or radiation exposure devices) or adversaries crossing the State's borders. Such acts may include the unauthorized acquisition of material, possession of material and/or devices, device fabrication, material and/or device movement and malicious use, threats or attempts to commit an unauthorized act, and unlawful scams or hoaxes with nuclear security implications.

2.13. States should plan and conduct detection operations in the interior to prevent, detect and interdict criminal or intentional unauthorized acts involving material of domestic origin; material that has been smuggled into the interior of the State; material that is being moved along domestic pathways (i.e. between the domestic point of origin or point of entry into the State and the destination or target); material in the vicinity of a target (i.e. near the target, but at a sufficient distance to ensure that the target can still be protected); and material at the target. States should consider that nuclear or radioactive material can be found at various locations across the interior. A large number of potential domestic pathways exist

[2] The term 'other stakeholders' refers to organizations that are impacted by or expected to contribute to the detection architecture but do not have official or legal authority for nuclear security. These stakeholders may include private and public sector organizations as defined in Ref. [3]; for example, private companies, facility operators and other users of nuclear and other radioactive material, academic and research institutions, or private health institutions.

for the unauthorized movement of material, and a large number of potential targets can be exploited by adversaries.

2.14. The most efficient way to detect criminal or intentional unauthorized acts involving nuclear and other radioactive material out of regulatory control is by integrating nuclear security measures into existing security systems and measures. The integration of nuclear security into common security operations in the interior of a State is addressed in detail in Section 3.

2.15. The interior of a State typically comprises a large area, and it is not possible to fully cover it with radiation detection equipment. Most detection equipment is designed to scan a limited, defined area under controlled conditions. Given the fact that resources are often limited, States generally focus on deploying radiation detection equipment to cover only a selected number of pathways or potential targets. To ensure that the deployment of equipment is as effective as possible, these pathways and potential targets should be identified using a risk informed approach. Section 4 outlines the process for information collection, analysis and dissemination to support detection operations in a State's interior.

2.16. A considerable number of competent authorities and other stakeholders operate in the interior of a State, each having different missions, operating under procedures specific to their organizations, and potentially having different levels of awareness and practical experience with nuclear security. The administrative division of a State results in different levels and jurisdictions (e.g. federal, regional, local). This division is also reflected among competent authorities and relevant stakeholders and can create challenges in communication and coordination.

2.17. Given the disposition of security resources in the interior of a State, the timeline to interrupt a criminal or intentional unauthorized act may be compressed. The farther away from the target detection occurs, the more time a State will have to neutralize the threat to the target. However, security resources are often concentrated in the immediate vicinity of potential targets, and detection may occur in close proximity to the intended target. In this case, the consequences of a potential nuclear security event are likely to be more severe. Strategies to address this challenge include performing detection activities at a distance that would ensure adequate protection of the target. For the design and implementation of these strategies, the State should undertake an ongoing evaluation of nuclear security threats and risks and should attempt to identify potential targets. In addition, detection operations can be incorporated into routine security operations occurring throughout the interior. States could also consider implementing low visibility or discreet detection operations so as to avoid prematurely alerting

potential adversaries of the existence of detection systems and measures at specific locations.

2.18. To ensure a strong link among competent authorities and other stakeholders responsible for detection and response in the interior layer, States might consider establishing and deploying specialized operational teams, which include personnel who are qualified in nuclear security detection and response (see Ref. [10]) and/or emergency response operations, in accordance with Refs [11, 13]. Training and standard operating procedures should account for the fact that actions taken during detection activities may facilitate follow-on response efforts. For example, implementing proper procedures and ensuring chain of custody in the handling of nuclear and other radioactive material are important for successful future prosecution of potential criminal activity.

2.19. Sustainability considerations, including the provision of financial, human and technical resources in the long term, should be taken into account when designing detection operations, along with the associated systems and measures in the interior. Paragraph 7.21 of Ref. [3] states:

> "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."

Guidance on developing national and operational sustainability objectives can be found in IAEA Nuclear Security Series No. 30-G, Sustaining a Nuclear Security Regime [14].

TRAINING FOR DETECTION OPERATIONS

2.20. IAEA Nuclear Security Series No. 31-G, Building Capacity for Nuclear Security [15], provides information on the systematic approach to training. Paragraph 3.12 of Ref. [15] states:

> "The first phase of the SAT [systematic approach to training] is to determine the training needs of personnel at all levels and with all types of responsibility for nuclear security. This is a major task that involves analysis of the performance requirements (i.e. duties and tasks) of individuals who

have direct responsibility for planning, implementing and/or evaluating the effectiveness of the nuclear security programme."

2.21. Paragraphs 3.25 and 3.26 of Ref. [15] state:

"3.25. In order to establish a strategy for developing an awareness programme, goals should be established to focus awareness raising efforts, including the following:

(a) Providing individuals with foundational knowledge and guidance relevant to their roles and responsibilities for nuclear security (e.g. information on nuclear security threats, detection options and operations) for building an effective nuclear security culture. This knowledge can provide a basis for advanced training and a broader understanding of one's responsibilities.
(b) Fostering the development of political will of government entities and organizations to build and sustain nuclear security capabilities and programmes. It is believed that institutionalizing nuclear security within the responsible organization will enhance the effectiveness of national nuclear security capabilities.
(c) Promoting a common terminology and basis for raising awareness with the general public and non-governmental organizations.

"3.26. To accomplish these goals, States may draw upon the following set of guidelines for planning, developing, implementing and sustaining effective nuclear security awareness raising:

(a) Communicate the need for nuclear security efforts;
(b) Include a core set of themes;
(c) Develop awareness for all roles and audiences;
(d) Customize efforts to specific audiences;
(e) Plan and organize to promote effectiveness;
(f) Establish awareness as a continuous process;
(g) Evaluate awareness efforts regularly and update as necessary."

2.22. Given the diversity and number of competent authorities and other stakeholders operating in the State's interior, it is important to implement a graded approach to training. The State should establish awareness building and training curricula tailored to the needs of the target audience, depending on their specific roles and functions in the nuclear security detection architecture.

2.23. Basic nuclear security awareness training should be provided to the personnel of all competent authorities and other stakeholders who participate in detection operations in the interior of a State. Regardless of whether personnel are equipped with nuclear security detection equipment, they might encounter nuclear and other radioactive material out of regulatory control, or they might be in a position to generate information alerts for criminal or intentional unauthorized acts. Having a basic level of awareness will ensure that the personnel are able to identify signs of suspicious activity involving material out of regulatory control.

2.24. The following topics should be included in basic nuclear security awareness training for competent authorities and other stakeholders:

(a) Basic concepts of radiation (e.g. types of radiation emitted by nuclear and other radioactive material, exposure to radiation, radioactive contamination);
(b) Basic concepts of radiation protection (e.g. the effects of time, distance and shielding);
(c) Authorized uses of radioactive material and devices that incorporate radioactive material;
(d) Nuclear security threats involving nuclear and other radioactive material out of regulatory control;
(e) Indicators of suspicious activity involving nuclear and other radioactive material;
(f) Overview of the nuclear security detection architecture, including detection by instrument alarm and information alert;
(g) Procedures for requesting assistance in the case of a potential nuclear security event.

2.25. For the personnel of competent authorities and other stakeholders expected to operate detection equipment or to investigate an instrument alarm or information alert, specialized training should be offered in addition to basic awareness training. This specialized training should be conducted before the deployment of radiation detection equipment and at regular intervals to ensure operational preparedness. Personnel should be aware of how time, distance and shielding affect detection. For example, high activity radiation sources can trigger an alarm from greater distances (e.g. several individuals or vehicles away).

2.26. Specialized training should include the following topics:

(a) Basic principles of radiation detection;
(b) Types of radiation detection equipment;
(c) Operational instructions for the use of equipment;

(d) Daily checks on the functionality of equipment;
(e) Common causes of innocent alarms;
(f) Basic preventive maintenance;
(g) Standard operating procedures for detection operations.

2.27. Competent authorities and other stakeholders can improve the skills of their personnel in relation to nuclear security detection by integrating appropriate modules into existing training programmes. For example, a module on nuclear security threat awareness could be included in basic training for new recruits and then made mandatory as part of periodic refresher training.

EVALUATION OF DETECTION SYSTEMS AND MEASURES

2.28. The establishment of an evaluation framework or process for detection systems and measures can promote consistent improvement across nuclear security detection operations in a State's interior. The evaluation process should cover all essential elements of the national nuclear detection architecture, such as the legal framework, strategies, plans and procedures, risk analyses, human resources and technical assets for detection operations in the interior. This evaluation process should be continuous and should be repeated regularly.

2.29. Evaluating detection operations in the interior of a State can be particularly challenging because of the large number of competent authorities and other stakeholders operating in a wide variety of locations to conduct detection activities related to criminal or intentional unauthorized acts. The scope of the evaluations should be appropriately defined so as to ensure that the results can inform improvements to detection operations. Defining the scope is the process of focusing the evaluation by clarifying its purpose, for example by undertaking the following actions:

(a) Defining what the evaluation will cover. The focus can be on a single component (e.g. a detection instrument), a single process (e.g. the integration of nuclear security detection into routine patrols of the interior), multiple operational components (e.g. officers on routine patrol calling for support from radiation subject matter experts) or the coordinated operation of the interior nuclear security detection architecture as a whole.
(b) Determining the level of the evaluation. Evaluations can be carried out at the organizational level, at the national level or through peer reviews by international experts, using mechanisms such as the IAEA International Nuclear Security Advisory Service (INSServ) (see Ref. [16]).

(c) Identifying the evaluation goal. Evaluation goals can include deliverables such as the evaluation of the operational efficacy of established concepts of operations and standard operating procedures; the qualifications of personnel and their ability to implement and adhere to established concepts of operations or standard operating procedures; or the costs associated with incorporating nuclear security detection into existing security activities in the interior.

2.30. Evaluation criteria and metrics should be used to systematically gauge progress with respect to a stated evaluation goal. Metrics should be relevant to the specific evaluation purpose and scope and should provide information that can be acted upon. The metrics should be measurable, accurately quantifying information related to the corresponding functional objectives of detection in the interior. They should also be objective, independent from external influence and consistent across systems in terms of what the metrics measure, how the metrics are defined and which units are used.

2.31. The evaluation should assess both operational capacity and efficacy. Capacity represents the resources available to achieve the intended results. Examples of capacity based metrics include the percentage of interior security personnel trained in radiation basics and/or equipped with detection instruments. Efficacy represents the ability of the personnel to perform detection operations and achieve the intended results. Examples of efficacy based metrics include the probability of detecting a threat (e.g. material of concern) through deployed detection operations — with or without the use of detection instruments — and the time needed for individuals or vehicles to traverse interior checkpoints with screening procedures.

2.32. The State should decide the evaluation method best suited to assess the desired evaluation goals. Each method may be performed either as a self-assessment or as an independent assessment (see Ref. [15] for examples of evaluation tools). The following evaluation methods can be employed for the assessment of detection operations in the interior of a State:

(a) Exercises "are useful in assessing local and national nuclear security detection capabilities to identify and correct deficiencies in equipment, concept of operations and training" [3]. IAEA Nuclear Security Series No. 41-T, Preparation, Conduct and Evaluation of Exercises for Detection of and Response to Acts Involving Nuclear and Other Radioactive Material out of Regulatory Control [17], introduces a structured approach for the preparation, conduct and evaluation of exercises. Regular multiagency exercises are essential

to promote cooperation among the many competent authorities operating in the interior and to integrate their detection strategies, procedures, operations and other technical means. Exercising simulated nuclear security event scenarios can ensure operational readiness.

(b) 'Red team' testing involves challenging the plans, programmes, assumptions and implementation of detection operations. This method often uses covert testing, whereby the red team serves as a surrogate adversary and attempts to introduce a threat into the system without being detected. Effective red team testing provides an opportunity to assess which defensive measures are working effectively, as well as which areas or processes are likely to be most vulnerable to adversary exploitation.

(c) Modelling and simulation can be used to suggest an outcome or to develop a basis for decision making. Example applications for this type of testing may include evaluation of the effectiveness of instrument alarm algorithms or radionuclide identification algorithms.

(d) Administrative analysis is generally conducted by an evaluator or specialized evaluation unit within the competent authorities. This type of analysis can ensure continuous assessment of the nuclear security detection architecture and can effectively monitor the implementation of improvement plans that result from previous evaluations. A number of the evaluation tools described in Ref. [15] fall within this category. Examples of administrative analyses may include programme evaluation sheets, interviews, observations and feedback from peers or focus groups. These evaluations should follow the strengths, weaknesses, opportunities and threats (also referred to as 'SWOT') analysis process to perform gap analysis, qualitative and quantitative assessments, performance analysis, instrument data analysis or a statistical comparison.

(e) Technical analysis involves performance testing and evaluation to ensure the effectiveness of systems and equipment. It is generally conducted by technical subject matter experts in the competent authority or by a specialized expert support organization.

2.33. The main output of the evaluation process is an evaluation report that documents information on the evaluation, including the methodology used, the evaluation objectives, the data collected, the results and any recommendations for improvement. Recommendations should be relevant to the existing objectives for detection in the interior of a State and should provide actionable steps for the improvement of operations. The evaluation report should be provided to all relevant stakeholders for review, and their feedback should then be incorporated into the report. Since the data collected during such an evaluation, along with the results of the evaluation, are often considered sensitive in terms of national security, the report should be treated in accordance with established procedures for the protection of information.

3. DETECTION OPERATIONS IN A STATE'S INTERIOR

INTEGRATION OF NUCLEAR SECURITY INTO EXISTING OPERATIONS

3.1. Detection operations for nuclear and other radioactive material out of regulatory control in a State's interior can be conducted by law enforcement, emergency services or specialized teams, such as intervention units, hostage rescue teams, explosive ordnance disposal units, crime scene investigation teams, and chemical, biological, radiological and nuclear (commonly known as 'CBRN') teams, in addition to performing their other responsibilities. Paragraph 3.5 of Ref. [1] states:

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

3.2. Competent authorities and other stakeholders in the interior of a State should integrate detection operations into their existing mission areas, concepts of operations, procedures and training programmes, as well as into detection operations conducted at a State's borders. Since a number of competent authorities may have existing capabilities and competencies for detection, the coordination of these detection activities and the development of a joint detection operations plan (see Annex II) could increase the efficiency of detection operations in the interior of a State.

3.3. Competent authorities and other stakeholders in a State's interior do not typically operate radiation detection equipment. As part of the national nuclear

security detection architecture, they should be able to have access to specialized teams or expert support teams that have the capability to operate radiation detection equipment so as to assess information alerts and instrument alarms.

3.4. Law enforcement and emergency services could incorporate the use of radiation detection equipment into their detection operations. If they are equipped with radiation detection equipment, they should also be provided, as appropriate, with the corresponding training (see paras 2.25 and 2.26) and with procedures on how to operate the equipment, interpret data from the measurements and adjudicate on alarms.

COMMON TYPES OF DETECTION OPERATION

3.5. Detection operations in the interior of a State can be categorized into three common types: (1) routine operations (see paras 3.7–3.9); (2) enhanced operations (see paras 3.10–3.13); and (3) targeted or specific operations (see paras 3.14–3.19). Special considerations for detection during routine, enhanced, and targeted or specific operations are outlined in paras 3.22–3.67, and examples are provided for each type of detection operation. These examples, although not exhaustive, can be used as a basis for planning and conducting detection operations.

3.6. The selection of a particular type of detection operation as the most appropriate to mitigate the current threats and risks in a State's interior should be made using a risk informed approach and should take into consideration the threat level, including information originating from information alerts and other relevant security information.

Routine operations

3.7. Routine operations are conducted in the interior of a State by competent authorities and other stakeholders as part of their regular operational activities, and they comprise ongoing control and monitoring activities. They correspond to 'business as usual' — namely, when no specific threat has been identified. Routine operations can take place at any location and might involve the monitoring of large areas, specific locations, people, vehicles and goods.

3.8. When competent authorities and other stakeholders are performing routine operations in the interior, they are not necessarily equipped with radiation detection instruments, and they have to rely on their ability to recognize indicators of suspicious activity involving nuclear and other radioactive material out of

regulatory control to generate an information alert. In this case, coordination and information sharing among competent authorities, specialized teams and/or expert support organizations with access to radiation detection equipment is essential for the confirmation and adjudication of the alert.

3.9. Special considerations for and examples of routine operations are presented in paras 3.22–3.48. These examples include routine patrols, routine checkpoints, conventional operations of emergency services, and detection by information alerts obtained from medical surveillance, public reporting and law enforcement investigations.

Enhanced operations

3.10. Enhanced operations are conducted in the interior of a State by competent authorities and other stakeholders when there is a heightened security posture. The security posture can be heightened as a result of a raised national threat level, a general information alert without information about a specific threat, or a high profile event.

3.11. When conducting enhanced detection operations, competent authorities and other stakeholders should consider the duration of the enhanced phase of operations, since these operations will inevitably employ a larger amount of technical and human resources than routine operations. Cooperation among multiple competent authorities with detection capabilities should also be considered, given the limited resources. Operating jointly with partner competent authorities has the added value of allowing law enforcement and emergency services access to a larger number of radiation detection equipment or more sophisticated technical equipment, as well as to more personnel trained in nuclear security detection.

3.12. For enhanced operations, additional resources may be allocated to law enforcement and emergency services in order to detect the presence of material out of regulatory control in accordance with a risk informed, graded approach. On the basis of information gathered on the potential threat, enhanced detection operations can be integrated into law enforcement operational duties, including roadside checks, routine patrols, dignitary protection, and security at high profile events.

3.13. Special considerations and further examples of enhanced operations are provided in paras 3.49–3.57 and include operations after a general information alert and operations at a high profile event.

Targeted or specific operations

3.14. Targeted or specific detection operations are conducted by competent authorities on the basis of specific, credible and actionable information that indicates with high probability that a nuclear security event is in preparation, is ongoing or has taken place.

3.15. Targeted or specific operations can be conducted by competent authorities and other stakeholders as part of initial assessment activities when a specific threat has been detected by an information alert or instrument alarm; when an event involving material out of regulatory control has already occurred; or when investigative or special operation units make a specific request for such operations based on precise information or intelligence.

3.16. When planning targeted or specific detection operations, competent authorities and other stakeholders should consider (a) the nature of the operation (e.g. overt, discreet); (b) the aim of the operation (e.g. detection or deterrence of a criminal or intentional unauthorized act); (c) the availability of human and technical resources; and (d) the number and level of expertise of trained personnel.

3.17. In order to effectively implement targeted or specific operations, the competent authorities conducting these operations should have specialized training in nuclear security threats and be equipped with, and trained to use, radiation detection equipment.

3.18. All information or intelligence accumulated before the initiation of targeted or specific operations will aid competent authorities and other stakeholders in selecting the appropriate detection equipment and in determining how to adapt existing standard operating procedures to the specific scenario.

3.19. Depending on the severity of the situation, these operations may be conducted in parallel with emergency management processes and nuclear security arrangements as described in the State's national response framework. In such cases, the relevant authorities should ensure that the operations are conducted in a coordinated manner. References [2, 10, 11] address specific nuclear security measures and radiological emergency response actions, including emergency response plans. Special considerations and examples of targeted or specific operations are provided in paras 3.58–3.67 and include area searches and undercover operations.

ELEMENTS OF DETECTION OPERATIONS

3.20. Paragraphs 3.22–3.67 present special considerations for, and detailed examples of, the different types of detection operation. Guidance is provided on each type of detection operation concerning the personnel typically involved in the specified detection activities, the preparatory activities that should be completed prior to the conduct of the detection operations and the steps to be followed by personnel when implementing the detection operations. Where applicable, operational steps and examples are provided for the conduct of detection operations, both with and without the use of radiation detection equipment.

3.21. Across all detection operations in the interior of a State, the following elements should be in place to ensure that operations are conducted effectively:

(a) Authority to conduct operations. Before the implementation of detection activities, the State should ensure that the personnel conducting these activities have the necessary authority and jurisdiction to do so. In the particular case of a targeted search, additional steps may have to be taken to ensure that the personnel have authorization to conduct the search or to proceed with undercover operations.
(b) Procedures for the detection of criminal or intentional unauthorized acts. Competent authorities and other stakeholders should develop concepts of operations and standard operating procedures for detection. They could also establish interagency agreements, as appropriate, and any necessary arrangements for the involvement of expert support.
(c) Procedures for information management. Arrangements for information sharing should be established to manage the exchange of information within an organization and among different organizations (see also Section 4).
(d) Training for the implementation of different types of detection operation. Personnel should have received the appropriate training for the detection of criminal or intentional unauthorized acts, as described in paras 2.20–2.27. Training should be provided to personnel on the appropriate use of any deployed equipment that personnel are expected to operate in support of these operations.
(e) Domain awareness. Personnel should have prior knowledge of their areas of responsibility and the situational context, including the presence of authorized nuclear and other radioactive material (e.g. in nuclear, medical, research or industrial facilities) in the area of operations and any pre-existing locations with elevated radiation levels within that area.
(f) Nuclear safety awareness. Personnel should have received awareness training on nuclear safety. Requirements on the safety of radioactive

material are established in IAEA Safety Standards Series No. GSR Part 3, Radiation Protection and Safety of Radiation Sources: International Basic Safety Standards [18].

(g) Procedures for managing the interfaces with nuclear or radiological emergency response. If an information alert or instrument alarm has been confirmed not to be a false alarm (i.e. nuclear or radioactive material is present), the personnel should determine whether it is safe to proceed with the adjudication of the alert or alarm. If it is determined that it is unsafe to proceed because of the presence of an actual or potential radiation hazard, the appropriate response organizations should be notified, and appropriate protective actions and other response actions should be implemented in accordance with Refs [10, 11] and IAEA Safety Standards Series No. GSG-2, Criteria for Use in Preparedness and Response for a Nuclear or Radiological Emergency [19]. Appropriate response actions include identification of whether the operational criteria warranting appropriate protective actions are met (see Refs [11, 19]).

SPECIAL CONSIDERATIONS FOR DETECTION DURING ROUTINE OPERATIONS

Detection operations during routine patrols

3.22. The personnel involved in routine patrols typically belong to law enforcement or security agencies. They could also be private stakeholders, such as private site security contractors. Patrols within a defined area of operation are regularly carried out by such competent authorities and other stakeholders as part of routine operations.

3.23. The competent authority or stakeholder should incorporate a concept of operations on nuclear security detection to the existing standard operating procedures of routine patrols, taking into consideration whether the personnel have detention and interdiction authority; whether they have access to radiation detection equipment; and if so, the type of equipment that they use.

3.24. Personnel should be aware of the domain in which they have been designated to patrol. They should have received basic nuclear security awareness training, and if they are provided with detection equipment, they should also have specialized training in the use and basic maintenance of such equipment in advance of their deployment on routine patrols.

3.25. The actions to be undertaken during routine patrols by the personnel, depending on whether they have radiation detection equipment or not, are described as follows:

(a) If the personnel are on patrol without radiation detection equipment and observe or receive information on any suspicious activities or materials that could indicate the presence of nuclear or other radioactive material out of regulatory control, they should assess the credibility of the information and adjudicate on the alert.

(b) If the personnel are on patrol carrying radiation detection equipment and they receive an instrument alarm, they should confirm the validity of the primary detection to determine whether or not it is a false alarm. Applicable radiation detection equipment for use during routine patrols can include personal radiation detectors worn by the operational personnel or other handheld equipment.[3]

(c) If the alarm or alert is confirmed, and it has been determined that there is no radiation hazard, the personnel on patrol proceed to the initial assessment of the alarm or alert. The initial assessment may result in localizing the potential source of radiation and securing the scene. It may also result in isolating any individuals present at the scene or separating these individuals from materials or property, and detaining and interdicting the suspect material as well as the individuals. The personnel can then request expert support to assist in the secondary assessment of the alarm or alert. The expert support team may consist of subject matter experts equipped and trained to use radiation monitoring instruments for categorization of radioactive material and to perform radiation protection tasks. Given the limited capabilities of most handheld equipment and personal radiation detectors, it is likely that even personnel carrying such equipment will need to contact expert support for spectrometric analyses, analysis of results, scientific advice for further measurements in the field or deployment of more sensitive detection instruments to complete the alarm assessment and identify the material present at the scene.

[3] See Annex I for a description of the equipment used for radiation detection.

(d) If the assessment concludes that the alarm is false or innocent[4], the personnel may resume their patrols. If the alarm is confirmed not to be innocent, the appropriate response organizations should be notified in accordance with the relevant procedures, and protective actions and response actions should be implemented in accordance with Refs [10, 11].

3.26. The following are example scenarios for detection during routine law enforcement patrols:

(a) A law enforcement officer on patrol, without radiation detection equipment, discovers a package with the radiation trefoil symbol displayed on the exterior of the package. The officer secures the area around the package and notifies the shift supervisor to request expert support for the deployment of detection equipment to identify the package contents.
(b) A law enforcement officer on patrol walks past a waste container and receives an alarm on a personal radiation detector. The officer follows the established procedures to confirm that it is not a false alarm. When the presence of radioactive or nuclear material is confirmed, the officer uses the detector to locate the area of elevated radiation. The officer then secures the area and notifies the shift supervisor to request expert support in order to proceed with the identification of the material and determine whether the alarm was an innocent alarm or an indication of a real nuclear security concern.

Detection operations at routine checkpoints

3.27. The personnel typically involved in routine checkpoint operations belong to law enforcement and security agencies. They may also be private stakeholders, such as private site security contractors. Checkpoints can be established at points of traffic congestion, regional commercial hubs, inspection stations or transport hubs, as well as entrances to buildings or facilities.

3.28. The location of checkpoints is decided using careful planning. Checkpoint planning includes ensuring that the appropriate human resources will be available, setting up traffic control measures, selecting locations to perform the

[4] Reference [3] defines these terms as follows:
— False alarm: "An alarm found by subsequent assessment not to have been caused by the presence of nuclear or radioactive material."
— 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."

identification of persons and/or vehicle isolation, and determining locations to conduct secondary inspections.

3.29. Personnel should be well aware of the domain in which they have been designated to conduct checks. They should have received basic nuclear security awareness training, and if they are provided with detection equipment, they should also have received specialized training in the use and basic maintenance of such equipment in advance of deployment. The personnel conducting checks should have the legal authority and ability to detain and pursue vehicles, as well as to detain suspects.

3.30. The concept of operations should be designed to ensure that personnel can quickly identify the person or vehicle that is the source of the alarm.

3.31. The actions to be undertaken by the personnel deployed in routine duties at a checkpoint, depending on whether the personnel have radiation detection equipment or not, can be summarized as follows:

(a) If the personnel are operating a checkpoint without radiation detection equipment and observe a suspicious person or material pass through the checkpoint, they should isolate the suspected individual and/or material from the checkpoint flow and follow standard procedures to interview the person and inspect the material in order to assess the potential alert (see also item (f) of this list). The credibility of the information gathered may be assessed against known threats.
(b) If the personnel have radiation detection equipment and an instrument alarm is triggered, they should isolate the suspected individual and/or material from the checkpoint flow and confirm the validity of the primary detection, determining whether it is a false alarm, an innocent alarm or an indication of a real nuclear security concern.
(c) If it is a false alarm, the personnel should resume their operations. Applicable radiation detection equipment for use at checkpoints can include personal radiation detectors worn by the operational personnel, vehicle mounted radiation detection systems for temporary checkpoints or radiation conveyor belt monitors designed to scan cargo or other goods.
(d) If the assessment has determined that it is an innocent alarm, the personnel may resume their checkpoint activities.
(e) If the alarm is determined not to be innocent, the appropriate response organization(s) should be notified, and protective actions and other response actions should be implemented in accordance with Refs [10, 11].

(f) If the alarm or alert is confirmed, and it has been determined that there is no radiation hazard, the personnel should proceed with securing the location, separating people from property, and detaining and interdicting the material and individuals involved. If the personnel are carrying handheld radionuclide identification devices and are trained to operate these devices, then they may perform an initial identification of the interdicted material. Alternatively, they can proceed directly with requesting expert support for further analysis or deployment of additional detection equipment to complete the initial alarm assessment and identify the material.

3.32. Radiation detection instruments can be integrated into operations by equipping the personnel operating routine checkpoints with personal radiation detectors and/or by diverting traffic (i.e. vehicles or pedestrians) past a vehicle mounted detector. In the case of personnel conducting routine vehicle checks using a personal radiation detector that produces an instrument alarm, the personnel should follow the established procedures. The established procedures should typically include the following actions for the personnel: using the detector to search for the source of radiation, securing the area and notifying the shift supervisor to request expert support so as to proceed with identification of the material. For personnel conducting routine vehicle checkpoint operations using a vehicle mounted detector, traffic has to be slowed as it passes through the checkpoint. If an alarm is triggered in the vehicle mounted detector, the personnel should isolate the vehicle and its passengers and should use personal radiation detectors or handheld radionuclide identification devices to search for the source of radiation.

3.33. The following are example scenarios for detection at a routine checkpoint:

(a) A law enforcement officer is operating at a routine vehicle checkpoint for narcotics interdiction and is not equipped with radiation detection equipment. The officer observes a suspicious package in the vehicle and on further inspection suspects that the package might contain a radioactive source. The officer directs the driver to the secondary inspection location after the driver has failed to provide proof of authorization to possess nuclear and other radioactive material. The officer isolates the driver and any other passengers from the vehicle and secures the vehicle. The officer notifies expert support to deploy detection equipment and assist in the confirmation of the alert and in the identification of the package contents.
(b) Mail sent to a State's parliament is routed through a specialized screening facility to scan for nuclear and other radioactive material using fixed radiation portal monitors or radiation conveyor belt monitors. After a parcel

triggers an instrument alarm, the personnel operating the monitors localize the source of radiation to a specific package. Expert support is requested to assist in the confirmation of the alarm and in the identification of the package contents.

Detection during routine operations of emergency services

3.34. The personnel typically involved in providing emergency services may belong to law enforcement, the fire service, specialized response teams and emergency medical services. If the personnel are provided with radiation detection equipment, they should have received specialized training on the use and basic maintenance of such equipment prior to deployment with the detection equipment.

3.35. The actions to be undertaken by emergency services personnel during the conduct of routine duties, depending on whether they have radiation detection equipment or not, can be summarized as follows:

(a) If the personnel do not have radiation detection equipment, and they observe suspicious material or activities that might indicate the presence of nuclear or other radioactive material out of regulatory control (e.g. radiation markings or specialized radiation protective equipment at the scene), they should attempt to localize the potential source of radiation and assess the credibility of the information to confirm the alert on the basis of the information available.
(b) If the personnel are equipped with personal radiation detectors and an instrument alarm is triggered, the personnel should confirm the validity of the primary detection to determine whether it is a false alarm, an innocent alarm or an indication of a real nuclear security concern. The detector can then be used to search for the source of radiation that caused the alarm.
(c) If the alarm is determined to be a false or innocent alarm, the personnel may record the alarm and release the material. If the alarm is confirmed not to be innocent, the appropriate response organizations should be notified, and protective actions and other response actions should be implemented in accordance with Refs [10, 11].
(d) If the alarm or alert is confirmed, and it is safe to proceed according to the assessment of all hazards present at the scene, the personnel should notify both expert support to perform an initial assessment of the alarm or alert and law enforcement to secure the scene. Then, the personnel should continue their operations.

3.36. The following are example scenarios for detection during the routine operations of emergency services:

(a) A fire service inspection team performing a walkthrough at a nightclub observes a package with a radiation trefoil symbol. The fire service inspection team isolates the package, requests expert support to deploy detection equipment and notifies law enforcement using established protocols.
(b) A fire service team responds to a fire alarm at a private residence. An instrument alarm is triggered on a firefighter's personal radiation detector, indicating the presence of radiation. The firefighter follows the established procedures, using the detector to search for the source of radiation. The firefighter requests expert support to assist in the confirmation of the alarm and in the identification of the material and notifies law enforcement.

Detection by information alert obtained from medical surveillance

3.37. The personnel typically involved in detection by an information alert obtained from medical surveillance include medical personnel (e.g. doctors, nurses) at hospitals and clinics, the personnel of other health authorities and law enforcement personnel.

3.38. Medical surveillance is an important potential source of information alerts. Paragraph 5.5 of Ref. [3] states that (footnote omitted) "the appearance of radiation injuries may indicate involvement in a criminal or an unauthorized act with nuclear security implications or the preparation for such acts." To conduct effective medical surveillance, the State should ensure that medical personnel have received appropriate specialized training in identifying radiation injuries or illnesses (see Refs [11, 20]).

3.39. During the conduct of their routine duties, medical personnel may observe symptoms of acute radiation exposure or become aware of suspicious activity that might be linked to the exposure of a patient to nuclear or other radioactive material. If the origin of the radiation that caused the injury or illness cannot be identified or is suspicious, hospitals, clinics or other health authorities should establish a process to notify nuclear security agencies, and law enforcement and other appropriate competent authorities should also be informed as stipulated in Ref. [20]. In such circumstances, the medical personnel should continue with providing necessary treatment (see Ref. [20]).

3.40. A State may decide to use existing notification mechanisms, including those outlined in Ref. [20], or may choose to create a dedicated communication

channel and standard operating procedures specific to the direct notification of law enforcement about a potential nuclear security event. Additional details concerning information sharing in relation to the information alerts obtained from medical surveillance are provided in Annex III.

3.41. An example scenario of detection by information alert obtained from medical surveillance is the following. A medical team identifies a patient with symptoms consistent with radiation exposure, but the patient has no reason to be in contact with nuclear or other radioactive material. The patient in question also exhibits suspicious behaviour when asked about potential exposure to radiation. The medical team isolates the patient and checks for potential radioactive contamination. The patient is then placed under medical treatment. The medical team follows the established notification procedures and informs law enforcement about the incident.

Detection by information alert obtained from public reporting

3.42. The personnel typically involved in detection by an information alert obtained from public reporting are law enforcement personnel or other stakeholders, such as private site security contractors.

3.43. In order to detect criminal or intentional unauthorized acts involving material out of regulatory control as a result of public reporting, the State should establish a process for authorities to receive notifications from members of the public, such as a reporting hotline. Established public security awareness raising channels could also be leveraged.

3.44. If a member of the public observes or becomes aware of any suspicious activity that might indicate the presence of nuclear or other radioactive material out of regulatory control, the following actions should be undertaken. The person should notify law enforcement. Law enforcement should then initiate the established procedures for conducting the initial assessment of an information alert. Depending on the results of the initial assessment of information, a heightened security posture may ensue (see paras 3.49–3.52) or targeted search operations may be initiated (see paras 3.58–3.62). If the presence of radioactive or nuclear material out of regulatory control is suspected, routine patrols could also undertake detection operations for the initial assessment of the alert (see paras 3.22–3.26).

3.45. An example scenario of detection by information alert from public reporting is the following. A commuter observes a suspicious package on the train platform

and reports the package to the local transport police. The transport police arrive to inspect the package and observe radiation symbols on the exterior of the package. The transport police are equipped with personal radiation detectors and receive an instrument alarm. The police secure the package and request expert support for identification of the material.

Detection by information alert obtained during a law enforcement investigation

3.46. Law enforcement should establish procedures for initiating a search for nuclear and other radioactive material out of regulatory control and for requesting technical and scientific expert support when receiving an information alert, investigative lead or other information during the course of regular law enforcement investigation activities. Law enforcement personnel should be able to assess the credibility and source of such information in a timely manner.

3.47. During routine investigations, if the personnel observe or become aware of suspicious activity that might indicate the presence of nuclear or other radioactive material out of regulatory control, the following actions should be undertaken. The personnel should perform an initial assessment to determine the credibility of the information alert. If the alert is deemed credible and is confirmed, the personnel should initiate the established procedures to search for nuclear and other radioactive material. The law enforcement personnel should protect the source of the information that generated the information alert, in accordance with established procedures, since the information may have been obtained through sensitive means (e.g. from an informant or as part of activities gathering evidence for use in criminal proceedings). The steps to be followed during a targeted search are described in paras 3.58–3.62.

3.48. The following are example scenarios for detection by information alert during a law enforcement investigation:

(a) An informant provides information related to the location of a stolen ^{60}Co source to a law enforcement officer. The officer assesses this information and deems it to be credible. A search for the radioactive material is initiated by law enforcement.
(b) Law enforcement officers are surveying a tobacco smuggling operation. During the course of the investigation, the officers set up a telephone interception operation. While monitoring the telephone communications, the officers hear a discussion in which individuals are planning an attack using a radiological dispersal device. The officers assess this information

and determine that it is credible. They notify the specialized operations unit and request the conduct of a targeted search operation.

SPECIAL CONSIDERATIONS FOR DETECTION DURING ENHANCED OPERATIONS

Enhanced detection operations during a heightened security posture

3.49. The personnel typically involved in detection operations during a heightened security posture in a State's interior include law enforcement, security agencies, defence forces and expert support organizations.

3.50. Each of these organizations should develop in advance operational plans for enhanced operations during a heightened security posture. These plans should be based on risk informed scenarios and should be adaptable to the situation that led to the heightened security posture. In planning detection operations, the advantages and disadvantages of overt and discreet operations for the detection of nuclear and other radioactive material out of regulatory control should be considered. The scope of the heightened security posture should be determined based on a risk informed approach and should define the location and time duration of the heightened security posture. The criteria for declaring a heightened security posture and for establishing its scope (including which competent authorities will be involved) should be clearly defined, given the increased resource demands for sustaining such operations.

3.51. The following actions should be undertaken for detection during a heightened security posture resulting from a general information alert. The pre-existing operational plans for enhanced operations should be tailored, and additional resources should be deployed, in accordance with the plan and the situation. This could include the deployment of additional patrols (see paras 3.22–3.26); the establishment of additional checkpoints where personnel could conduct operations according to their assigned duties (see paras 3.27–3.33); and/or the deployment of roving patrols consisting of specially trained teams with portable radiation detection equipment (e.g. backpack based radiation detection systems). Vehicle mounted or airborne radiation detection systems could also be used by roving patrols.

3.52. An example scenario for enhanced detection operations during a heightened security posture is the following. The national threat level in a State is raised after credible but unspecific information is uncovered concerning the threat of illicit

use of nuclear or other radioactive material against the State. No specific material or suspect is identified, but security organizations are instructed to heighten the security posture for a defined time frame around potential targets, transit pathways, and facilities where nuclear or other radioactive material is produced, used or stored. Security organizations adapt the existing operational plan based on the available threat information, in cooperation with technical and scientific experts from the national regulatory authority. The security organizations deploy additional radiation detection capabilities to the locations or pathways deemed most vulnerable to the suspected threat.

Enhanced detection operations during a high profile event

3.53. The personnel typically involved in securing high profile events could include law enforcement, security agencies, explosive ordnance disposal teams, defence forces and private stakeholders, such as private site security contractors for venue security or for the protection of high profile individuals (e.g. politicians, celebrities, dignitaries).

3.54. The operational plan for detection at a high profile event should be developed in advance of the event, in consultation with all the relevant stakeholders. It should also be integrated into the overall security plan for the event. Competent authorities should consider use of both overt and discreet detection operations to develop a defence in depth strategy. They should also take into consideration the scope of the high profile event, its location and its duration. Reference [6] provides further guidance on nuclear security systems and measures that may be established or enforced by States hosting a major public event.[5]

3.55. The following steps should be taken to secure an event and enable the implementation of radiation detection measures. The personnel should conduct an area sweep and a radiation survey before the commencement of the event and in conjunction with other security sweeps (e.g. sweeps for explosives). Such measures help to determine the background radiation levels, whether locations have elevated radiation levels or whether any existing threats are present in the area where the event is scheduled to take place. Radiation surveys can be carried out using portable radiation detection equipment (e.g. backpack based detectors, handheld gamma and/or neutron survey meters, handheld radionuclide

[5] A major public event is defined in Ref. [6] as "[a] high profile event that a State has determined to be a potential *target* to include, for example, sporting, political, and religious gatherings involving large numbers of spectators and participants."

identification devices[6]). After the sweeps and surveys have been concluded, the personnel should secure the venue and establish a perimeter security (i.e. venue lockdown).

3.56. The authorities who are responsible for the security of the event should deploy additional resources, such as routine patrols and checkpoints, for the detection of nuclear and other radioactive material out of regulatory control, in accordance with pre-established processes. The authorities might also choose to specify an area around the location of the event and raise the security posture within that area for the duration of the event. If, during the pre-event area sweep or at any other time during the event, the personnel receive an instrument alarm or information alert, they should follow pre-established procedures for the timely adjudication and confirmation of that alarm or alert.

3.57. An example scenario for enhanced detection operations during a high profile event is the following. A famous musician is performing at a concert hall. Based on the threat and risk assessment, the local authorities decide to deploy radiation detection resources to the concert hall. Local law enforcement officers work in coordination with technical and scientific experts from the national nuclear regulatory body, as well as with the venue and the musician's private security personnel, to develop an operational plan so as to deploy the radiation detection capabilities. This operational plan includes a radiation survey as part of the pre-concert security sweep, deployment of trained personnel with detection equipment at the entrances of the venue to screen incoming patrons, and patrols within the venue during the concert. The operational plan also includes protocols for activating an on-site expert team equipped with handheld radionuclide identification devices so as to quickly resolve any instrument alarms.

SPECIAL CONSIDERATIONS FOR DETECTION DURING TARGETED OR SPECIFIC OPERATIONS

Targeted search operations

3.58. The personnel typically involved in targeted search operations belong to law enforcement, security agencies, defence forces and technical support organizations. The personnel need to obtain legal authority to conduct a search for nuclear or other radioactive material out of regulatory control, in accordance with national legislation and regulations.

[6] See Annex I for a description of the equipment used for radiation detection.

3.59. Based on the information available, the personnel should develop a search plan before undertaking the targeted search operations. The search plan should take into consideration the advantages and disadvantages of overt and discreet detection methods, as well as which entity has the authority and the jurisdiction to conduct the search at a given location in the State. The plan should also include provisions for selecting the appropriate type of equipment for the detection of material at the given location.

3.60. The personnel should have access to, and specialized training on the use of, the equipment and resources to be employed during the search, including handheld or backpack detectors, radionuclide identification devices and vehicle mounted radiation detection systems. The personnel planning and implementing the operations should understand the functions and limitations of each type of equipment. Pre-established processes should be in place to initiate, as appropriate, the local or national response plans, which cover the relevant nuclear security measures and emergency response actions. The trustworthiness of these personnel should be reviewed periodically.

3.61. Competent authorities conducting targeted search operations should take the following actions:

(a) The process for the planning of the targeted search should begin with a determination of the scope of the search, discreet reconnaissance and surveillance of the location, coordination with other competent authorities, and identification of the necessary resources (i.e. specific to the material that the search is designed to locate). The personnel planning and implementing the operations can request technical and scientific expert support from the regulatory body or other expert support organizations to determine the optimal search techniques and to select the appropriate equipment. The personnel should then deploy technical and human resources in accordance with the search plan and use the available radiation detection equipment to detect the nuclear or other radioactive material out of regulatory control. Depending on the material of interest and the search area, radiation detection equipment that can be used to conduct a search includes: personal radiation detectors; handheld gamma and/or neutron survey meters; backpack based radiation detection systems; and vehicle mounted, airborne or maritime radiation detection systems.
(b) If, during the course of the search, an instrument alarm or information alert indicates the potential presence of radiation, the personnel should follow the operating procedure for initial alarm and alert assessment. This includes determining whether the instrument alarm or information alert is a false

alarm, an innocent alarm or an indication of a real nuclear security concern. In the case of an information alert, the validity of the alert should also be confirmed.

(c) If it is determined that the instrument alarm or information alert is a false or innocent alarm, the personnel may record and release any material present. If the alarm or alert is determined not to be innocent, the appropriate response organizations should be notified, and protective actions and other response actions should be implemented in accordance with Refs [10, 11].

(d) More specifically, if the alarm or alert is confirmed, and it has been determined that there is no radiation hazard, the personnel should secure the scene and should proceed to the initial assessment of the alarm or alert. The personnel may also separate or isolate any individuals present at the scene from materials or property, and detain and interdict the suspect material and the individuals. Initial identification can be performed using handheld radionuclide identification devices.

(e) Expert support should be activated to analyse the results and identify whether the material that was found matches the description of the material that was the object of the targeted search. If not, the material should be securely stored, the incident documented and the search continued.

3.62. One example scenario for targeted search operations is the following. An authorized carrier for the transport of a disused ^{60}Co radioactive source reports the theft of the source to the regulatory body. Using law enforcement information, a likely area where the missing source might be located is identified and a search plan is developed. A search team with radiation detection equipment is assembled and deployed in accordance with the search plan. The search team locates and identifies the radioactive source and secures the scene, which is processed as a radiological crime scene. The radioactive material is recovered and transported to a secure storage location.

Detection by information alert obtained from undercover operations

3.63. The personnel typically involved in detection by an information alert obtained from undercover operations include law enforcement, expert support organizations and security agencies.

3.64. Common undercover operations for the detection of nuclear and other radioactive material out of regulatory control may include 'sting'[7] operations, 'buy–bust'[8] operations and 'controlled delivery'[9].

3.65. Competent authorities planning operations should be aware of who has the legal authority to conduct an undercover operation. Before engaging in a specific undercover detection operation, the personnel should obtain authorization to conduct the proposed operation in accordance with existing legal procedures.

3.66. The personnel should have specialized training on the use of the equipment and resources that will be employed during operations, such as handheld detectors or mobile detection systems. The personnel planning and conducting the operation should understand the functions and limitations of each type of equipment deployed in order to determine which, if any, equipment is appropriate for the planned undercover operation.

3.67. The following actions should be undertaken in the case of detection by an information alert obtained during the conduct of undercover operations:

(a) The planning process should include a determination of the scope of operations, reconnaissance of the location, coordination with other competent authorities and identification of the necessary resources for the conduct of the operation. Resources should be deployed by the personnel in accordance with their organization's operational plan.
(b) If a suspicious activity or material is observed, the personnel should use the techniques and information at their disposal to confirm the presence of nuclear or other radioactive material. If radiation detection is not practicable or feasible for the operations, then the personnel should perform a visual examination of the material. The personnel should then decide whether to interdict the suspicious material or to continue with the investigation until more evidence can be collected and the alarm or alert can be confirmed.

---

[7] 'Sting' operations are deceptive actions designed to catch a person committing a crime. A sting operation will typically have an undercover law enforcement officer play the role of a criminal or potential victim and go along with a suspect's actions to gather evidence of the perpetrator's illegal activity.

[8] 'Buy–bust' is a type of undercover operation that involves the controlled purchase by undercover law enforcement officers of illicit material from a perpetrator. After the controlled purchase, the perpetrator is detained and the material is confiscated.

[9] 'Controlled delivery' is a tactic that involves a consignment of illicit material being detected and allowed to go forward under the control and surveillance of law enforcement officers in order to secure evidence against the organizers of the criminal activity.

(c) If the material has been interdicted, the alarm or alert has been confirmed and it has been determined that there is no radiation hazard, the personnel should secure the scene and should proceed to conduct an initial assessment of the alarm or alert. The personnel should contact expert support for radionuclide identification and for confirmation of whether the alarm is an indication of a real nuclear security concern.

(d) If the alarm is determined to be a false or innocent alarm, the personnel may resume their operations. If the alarm is determined not to be innocent, the appropriate response organization(s) should be notified, and protective actions and other response actions should be implemented in accordance with Refs [10, 11].

4. ROLE OF INFORMATION FOR DETECTION OPERATIONS IN A STATE'S INTERIOR

4.1. Information has an essential role in the planning and conduct of detection operations in a State's interior. Paragraph 5.1 of Ref. [3] states that "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."

4.2. Detection operations in the interior of a State should be implemented using a graded approach, on the basis of updates to the threat and risk assessment that are driven by the analysis of information relating to nuclear security. That is, when no specific threat has been identified, routine operations can be implemented; when the information analysis results in the identification of an elevated risk, enhanced operations can be planned and implemented; and when a specific threat has been detected by an information alert or instrument alarm, targeted or specific operations can be planned and implemented.

4.3. The State should use effective processes for the collection, analysis and dissemination of information to determine the best manner of deploying detection resources. Information management can address the challenges presented by detection in the State's interior by informing the prioritization of where, when and how to conduct detection operations.

4.4. Paragraph 3.8 of IAEA Nuclear Security Series No. 23-G, Security of Nuclear Information [21], states that "State policy on the security of information

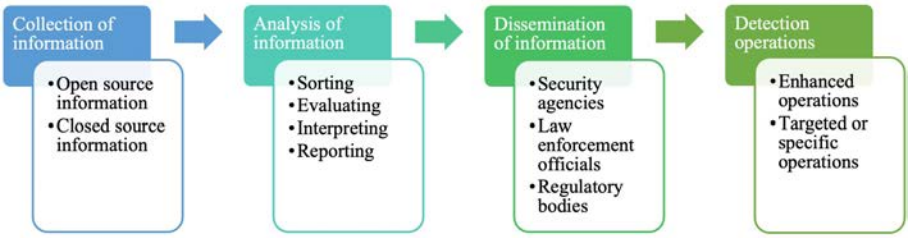

FIG. 1. Information handling process for conducting detection operations.

should define which type of information the State wishes to be secured and indicate how that security is to be applied." Such information security policies and protocols should be incorporated into organizational level processes and the joint detection operations plan for nuclear and other radioactive material out of regulatory control (see Annex II).

4.5. The general process for collecting, processing, disseminating and using information to inform nuclear security detection operations is outlined in paras 4.6–4.20 and depicted in Fig. 1. The State should define the sources of information that may be used, the competent authority responsible for analysing the information and the end users for the analytical reports. Generally, competent authorities and other stakeholders in the State's interior should collect information from all available sources. These raw data should be authenticated and then analysed, which may consist of sorting, evaluating and interpreting the information to produce an analytical report of key findings relevant to detection operations in the State's interior. These analytical reports should be disseminated to relevant competent authorities and may be used by other stakeholders to inform the planning, implementation and evaluation of detection operations in the State's interior.

COLLECTION OF INFORMATION

4.6. Competent authorities can use information to design, implement and conduct effective detection operations in the State's interior. Types of information that may be collected include the following:

(a) Operational information;
(b) Details of medical surveillance;
(c) Reports of regulatory non-compliance by licensees;

(d) Reports of loss of regulatory control of nuclear and other radioactive material;
(e) Information from the public and other external sources that can result in a decision to raise the security posture or can lead to a state of heightened alert.

4.7. Competent authorities can collect or receive information from open sources and from closed sources. Open sources consist of publicly available information (e.g. news media, social media, published materials, the dark web) and closed sources consist of information that is not publicly available and is generated by authorities (e.g. reports of loss of regulatory control of nuclear and other radioactive material, intelligence reports, other information from intelligence gathering activities).

4.8. Information sources can be either national or international. National information sources include intelligence (at both the strategic and operational levels), formal reporting procedures and existing cooperation mechanisms among competent authorities. International information sources include any source of information received from an entity located outside of the State, such as the IAEA Incident and Trafficking Database (ITDB) [22], the IAEA Unified System for Information Exchange in Incidents and Emergencies (USIE) [23], the International Criminal Police Organization (INTERPOL)[10], regional information exchange networks and bilateral information exchanges between neighbouring countries in accordance with cooperation agreements.

4.9. Operational information should include information on the presence of authorized nuclear and other radioactive material in the area in which a competent authority or other stakeholder holds responsibility. Competent authorities should share relevant information from the national radioactive source inventory with authorized personnel in security organizations on a need to know basis. Information on the types and locations of nuclear and other radioactive material present in a State's interior can assist, for example, in selecting the equipment and tactics to be used in detection operations. This information can include the types of radionuclide, the activity, the expected dose rates, the physical characteristics of the material and, for radioactive sources, additional information such as type, model, packaging and labelling.

4.10. Operational information on potential adversaries in a State's interior can also inform the planning and implementation of detection operations.

[10] https://www.interpol.int/en

Investigative leads or information from other law enforcement activities could result in information alerts or in detection operations targeting material out of regulatory control.

4.11. Information relating to other hazards relevant to the planning and conduct of detection operations in a State's interior might include the presence and locations of armed adversaries and of explosives or flammable chemicals.

4.12. Prompt notification by licensees[11] of missing, lost or stolen nuclear or other radioactive material can inform targeted search operations. The regulatory body will often be the first organization to receive such information and should have protocols in place to quickly notify the relevant security organizations (see paras 5.17–5.21 of Ref. [2]), which can then implement the necessary search operations.

4.13. Information from medical services and health authorities on suspected radiation injuries or casualties may signal the occurrence of a nuclear security event. States should define the procedures for the protection of information in the case of sharing sensitive medical data between law enforcement and public health authorities. More information on the management of information alerts obtained from medical surveillance is presented in Annex III.

4.14. Competent authorities may also receive information from the public indicating a threat, suspicious activity, abnormal situation, or a potential criminal or intentional unauthorized act involving nuclear or other radioactive material. Law enforcement and security agencies should establish outreach programmes with other stakeholders, such as industry, academia and licensees of nuclear or other radioactive material, to strengthen working relationships and promote situational awareness among authorities.

ANALYSIS OF INFORMATION

4.15. Analysis of information is a key step for planning and implementing detection operations in a State's interior. Many competent authorities and stakeholders with traditional security mandates have their own processes for information collection

[11] The licensee is defined as the holder of a current licence. The licensee is "the *person or organization* having overall responsibility for a *facility* or *activity*" [24]. For example, a licensee may be the operator of a nuclear facility, industrial facility, hospital or other medical facility, or research facility.

and analysis, which correspond to the four steps involved in the analysis of information: (1) sorting, (2) evaluating, (3) interpreting and (4) reporting.

4.16. The information analysis process for nuclear security detection in a State's interior demands multiagency cooperation, as it relies on the information collection capability, expertise and experience of a wide variety of organizations, including law enforcement, intelligence agencies, regulatory bodies and technical support organizations. Subject matter experts on nuclear and other radioactive material should be involved or consulted as part of the information analysis process because law enforcement and national security organizations might lack the necessary technical knowledge on nuclear and other radioactive material.

4.17. Through this analysis process, the information collected is compiled into an analytical report that can then be used by relevant competent authorities and stakeholders to plan and implement detection operations in a State's interior. Although the quantity of information available may be vast and updated on a continual basis, the personnel who perform these analyses often face time restrictions in delivering the relevant outcomes to operational organizations.

DISSEMINATION OF INFORMATION

4.18. Analytical reports on nuclear security should be disseminated to relevant stakeholders on a need to know basis. Through information exchanges among relevant competent authorities, the multiagency information analysis process can build on, and be complementary to, existing information collection and analysis processes. Secure dissemination of analytical reports should be ensured in accordance with existing policies and procedures for the protection of information (see Ref. [21]).

4.19. Information sharing should also extend to competent authorities and other stakeholders operating at different layers of the detection architecture, including at or beyond the State's borders, since a nuclear security event can move through several layers of the systems and measures in place for the protection of targets. An information dissemination strategy outlining processes to share information with regional and local stakeholders can effectively leverage national, regional and local resources while maintaining information security practices.

4.20. The collection, analysis and dissemination of information enables competent authorities to identify and prioritize strategic locations and pathways for conducting detection operations in the interior.

5. ROLE OF EQUIPMENT FOR DETECTION IN A STATE'S INTERIOR

5.1. While the detection of a potential nuclear security event in the interior of a State can occur by an information alert or an instrument alarm, radiation detection equipment should always be used to confirm the presence of nuclear and other radioactive material out of regulatory control. Confirmation can be obtained using a single type of radiation detection equipment or a combination of different types of equipment, particularly in the case of an initial assessment of an alarm.

5.2. Instrument alarms can derive from a wide variety of radiation detection instruments. Annex I presents some of the different types of equipment that are typically used for radiation detection in the interior of a State. Some are small enough to be worn (i.e. personal radiation detectors), some are handheld or carried as a backpack, and some are vehicle based.

5.3. In accordance with IAEA Nuclear Security Series No. 1, Technical and Functional Specifications for Border Monitoring Equipment [25], the choice of the most appropriate type of detection instrument for any given operation should be determined by the environmental conditions and the scenarios that are likely to be identified through a threat and risk assessment, including the type of material of concern, the material's signature and the expected adversary tactics. Reference [25] further indicates that detection instruments can be used to survey an area, to generate instrument alarms, to search and to localize material (i.e. initial alarm assessment) or to identify radionuclides.

INSTRUMENT DEPLOYMENT PLAN FOR DETECTION

5.4. Paragraph 7.4 of Ref. [3] states:

> "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 [points of entry and/or exit] 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 [improvised nuclear device], RDD [radiological dispersal device] or RED [radiation exposure device].”

5.5. The instrument deployment plan for the interior of a State should include the following components:

(a) Radiation detection instruments: the number and type of instruments to be deployed and their location in the interior;
(b) Complementary technology (see paras 5.17–5.19);
(c) Supporting capabilities and infrastructure needed for the conduct of detection operations (e.g. training, calibration, maintenance, power supply).

Further information on the components of a detection instrument deployment plan is provided in Ref. [3].

5.6. The following factors should be taken into consideration when developing the instrument deployment plan:

(a) The costs for the entire life cycle of the instruments (e.g. acquisition, calibration, maintenance);
(b) The replacement costs after the instruments have been retired from operation;
(c) The personnel needed to operate the instruments;
(d) Other resources needed for alarm assessment and adjudication procedures (e.g. infrastructure, training of personnel).

5.7. The instrument deployment plan should be developed by following a holistic approach as part of a functional nuclear security detection architecture. It should encompass both detection at the State borders and detection in the State’s interior to ensure that the equipment needs of all the competent authorities are met.

5.8. Paragraph 3.63 of Ref. [7] states:

> “Procurement considerations relating to the functionality of the equipment (including associated computer hardware and software) include the following:
>
> (a) Ability to support the concept of operations and the design;

(b) Ability to detect and measure radiation levels associated with materials of concern for nuclear security;
(c) Ability to identify such materials;
(d) Reliability (ability to consistently perform adequately) under expected environmental conditions at the detection location;
(e) Compatibility with existing equipment;
(f) Ability to meet specifications for the display, storage and retention of data;
(g) Ease and reliability of calibration;
(h) Certification as qualified equipment for the intended purpose;
(i) Training needs for operators;
(j) General ease of use."

5.9. The choice of radiation detection equipment for deployment in a State's interior needs to address the challenges that are specific to the State's interior (see paras 2.11–2.19). Performing detection activities with the intention of covering the potential adversary pathways that have the highest risk, across large areas and diverse types of domain, can best be achieved by using mobile and/or portable, durable and versatile equipment. Consideration should be given to such factors during the planning and acquisition phase to help to optimize the performance of detection equipment during operations.

5.10. The deployment plan should consider the appropriate combination of detection equipment to best meet operational needs. Competent authorities and other stakeholders should know the capabilities and limitations of the chosen equipment, including their sensitivity, size, durability, battery life, battery charge time and storage capabilities, so as to determine the most effective way to incorporate the instruments into operational plans and procedures.

5.11. The development of the instrument deployment plan should be a multiagency activity involving all the relevant competent authorities and other stakeholders that take part in the nuclear security detection architecture. This activity should account for the organizational and collective multiagency needs that best meet the goals of the detection strategy at the national and operational levels.

5.12. A coordinated plan for selecting and deploying equipment allows the State to maximize the use of resources — for example, by avoiding the procurement of redundant or non-applicable equipment — and carefully weigh the trade-offs between the costs and the desired capabilities of the equipment to best counter the identified nuclear security risks.

5.13. When deploying radiation detection equipment in the State's interior, the operational teams can use existing information on locations with elevated radiation levels (i.e. 'hotspots') in the interpretation of field measurements and in alarm adjudication. Such information can be provided by previous radiation monitoring activities in the country (e.g. results from recent background radiation surveys accumulated through interior detection operations).

OPERATION OF RADIATION DETECTION EQUIPMENT

5.14. Paragraph 6.3 of Ref. [3] states:

> "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 protection tasks."

5.15. During the initial assessment of an instrument alarm or an information alert, measurements with radiation detection equipment should be conducted to verify whether the alert or alarm is innocent — in which case, the incident should be recorded and the material released — or whether the presence of material out of regulatory control is confirmed — in which case, a nuclear security event might be declared. These measurements can be performed by trained personnel of the competent authorities conducting the detection operations or by expert support teams.

5.16. The State should consider the response times needed for expert support teams to be deployed in the field to support various types of detection operation. The State should also take into consideration that such operations could take place at any location within the State's interior. The expert support teams should have adequate training and equipment to identify suspect material within the time frame that personnel are able to legally detain suspects and material.

Complementary technology

5.17. In addition to radiation detection instruments, the detection of criminal or intentional unauthorized acts involving nuclear or other radioactive material out of regulatory control in a State's interior can be complemented by other security technologies. For example, competent authorities and other stakeholders operating in the State's interior often deploy or have access to the following technologies:

(a) Equipment for the detection of explosives (traces or larger volumes). The use of such equipment can confirm, in combination with radiation detection equipment, the presence or absence of a radiological dispersal device through an examination of suspicious content.
(b) Classic security monitoring equipment (e.g. surveillance cameras, closed circuit television). The use of this equipment can provide real time information to support detection operations in the interior of the State and can also be used for automatic licence plate recognition, facial recognition, perimeter security and tracking adversary movement.
(c) Non-intrusive equipment. This equipment can be used for the inspection of people or goods to detect contraband. For example, X ray (e.g. metal detectors) and gamma ray imaging systems can detect the presence of shielding or suspicious metal objects indicating the presence of a radioactive source, source shielding or containers.
(d) Global positioning system (GPS) equipment and software. This equipment can be used in combination with radiation detection equipment to map areas that have been surveyed for radiation and to record the relevant radiation measurements.

5.18. Competent authorities and other stakeholders should consider integrating the information generated by these complementary technologies into their detection strategies. They should also consider methods or processes for cross-referencing and/or processing data emanating from different systems.

5.19. The interaction and interoperability of radiation detection equipment with other security technologies should be considered when implementing detection operations in a State's interior. For example, X ray or gamma ray imaging systems can be used to detect shielding that might obscure signatures from nuclear or other radioactive material. However, radiation detection equipment should not be used near such imaging systems, because their emissions might cause interference or false alarms.

REFERENCES

[1] INTERNATIONAL ATOMIC ENERGY AGENCY, Objective and Essential Elements of a State's Nuclear Security Regime, IAEA Nuclear Security Series No. 20, IAEA, Vienna (2013), https://doi.org/10.61092/iaea.ajrj-ymul

[2] 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).

[3] INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Systems and Measures for the Detection of Nuclear and Other Radioactive Material out of Regulatory Control, IAEA Nuclear Security Series No. 21, IAEA, Vienna (2013).

[4] INTERNATIONAL ATOMIC ENERGY AGENCY, Risk Informed Approach for Nuclear Security Measures for Nuclear and Other Radioactive Material out of Regulatory Control, IAEA Nuclear Security Series No. 24-G, IAEA, Vienna (2015).

[5] INTERNATIONAL ATOMIC ENERGY AGENCY, Planning and Organizing Nuclear Security Systems and Measures for Nuclear and Other Radioactive Material out of Regulatory Control, IAEA Nuclear Security Series No. 34-T, IAEA, Vienna (2019).

[6] INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Systems and Measures for Major Public Events, IAEA Nuclear Security Series No. 18, IAEA, Vienna (2012).

[7] INTERNATIONAL ATOMIC ENERGY AGENCY, Detection at State Borders of Nuclear and Other Radioactive Material out of Regulatory Control, IAEA Nuclear Security Series No. 44-T, IAEA, Vienna (2023).

[8] 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), https://doi.org/10.61092/iaea.ko2c-dc4q

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

[10] INTERNATIONAL ATOMIC ENERGY AGENCY, Developing a National Framework for Managing the Response to Nuclear Security Events, IAEA Nuclear Security Series No. 37-G, IAEA, Vienna (2019).

[11] FOOD AND AGRICULTURE ORGANIZATION OF THE UNITED NATIONS, INTERNATIONAL ATOMIC ENERGY AGENCY, INTERNATIONAL CIVIL AVIATION ORGANIZATION, INTERNATIONAL LABOUR ORGANIZATION, INTERNATIONAL MARITIME ORGANIZATION, INTERPOL, ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT NUCLEAR ENERGY AGENCY, PAN AMERICAN HEALTH ORGANIZATION, PREPARATORY COMMISSION FOR THE COMPREHENSIVE NUCLEAR-TEST-BAN TREATY ORGANIZATION, UNITED NATIONS ENVIRONMENT PROGRAMME, UNITED NATIONS OFFICE FOR THE COORDINATION OF HUMANITARIAN AFFAIRS, WORLD HEALTH ORGANIZATION, WORLD METEOROLOGICAL ORGANIZATION, Preparedness and Response for a Nuclear or Radiological Emergency, IAEA Safety Standards Series No. GSR Part 7, IAEA, Vienna (2015), https://doi.org/10.61092/iaea.3dbe-055p

[12] INTERNATIONAL ATOMIC ENERGY AGENCY, Developing Regulations and Associated Administrative Measures for Nuclear Security, IAEA Nuclear Security Series No. 29-G, IAEA, Vienna (2018).

[13] INTERNATIONAL ATOMIC ENERGY AGENCY, Manual for First Responders to a Radiological Emergency, EPR-First Responders 2006, IAEA, Vienna (2006).

[14] INTERNATIONAL ATOMIC ENERGY AGENCY, Sustaining a Nuclear Security Regime, IAEA Nuclear Security Series No. 30-G, IAEA, Vienna (2018).

[15] INTERNATIONAL ATOMIC ENERGY AGENCY, Building Capacity for Nuclear Security, IAEA Nuclear Security Series No. 31-G, IAEA, Vienna (2018).

[16] INTERNATIONAL ATOMIC ENERGY AGENCY, International Nuclear Security Advisory Service (INSServ) Guidelines, IAEA Services Series No. 39, IAEA, Vienna (2019).

[17] INTERNATIONAL ATOMIC ENERGY AGENCY, Preparation, Conduct and Evaluation of Exercises for Detection of and Response to Acts Involving Nuclear and Other Radioactive Materials out of Regulatory Control, IAEA Nuclear Security Series No. 41-T, IAEA, Vienna (2020).

[18] EUROPEAN COMMISSION, FOOD AND AGRICULTURE ORGANIZATION OF THE UNITED NATIONS, INTERNATIONAL ATOMIC ENERGY AGENCY, INTERNATIONAL LABOUR ORGANIZATION, ORGANIZATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT NUCLEAR ENERGY AGENCY, PAN AMERICAN HEALTH ORGANIZATION, UNITED NATIONS ENVIRONMENT PROGRAMME, WORLD HEALTH ORGANIZATION, Radiation Protection and Safety of Radiation Sources: International Basic Safety Standards, IAEA Safety Standards Series No. GSR Part 3, IAEA, Vienna (2014), https://doi.org/10.61092/iaea.u2pu-60vm

[19] FOOD AND AGRICULTURE ORGANIZATION OF THE UNITED NATIONS, INTERNATIONAL ATOMIC ENERGY AGENCY, INTERNATIONAL LABOUR ORGANIZATION, PAN AMERICAN HEALTH ORGANIZATION, WORLD HEALTH ORGANIZATION, Criteria for Use in Preparedness and Response for a Nuclear or Radiological Emergency, IAEA Safety Standards Series No. GSG-2, IAEA, Vienna (2011). (A revision of this publication is in preparation.)

[20] INTERNATIONAL ATOMIC ENERGY AGENCY, WORLD HEALTH ORGANIZATION, Generic Procedures for Medical Response During a Nuclear or Radiological Emergency, EPR-Medical 2005, IAEA, Vienna (2005).
[21] INTERNATIONAL ATOMIC ENERGY AGENCY, Security of Nuclear Information, IAEA Nuclear Security Series No. 23-G, IAEA, Vienna (2015).
[22] INTERNATIONAL ATOMIC ENERGY AGENCY, Incident and Trafficking Database, https://www.iaea.org/resources/databases/itdb
[23] INTERNATIONAL ATOMIC ENERGY AGENCY, USIE User's Manual, https://iec.iaea.org/usie
[24] INTERNATIONAL ATOMIC ENERGY AGENCY, IAEA Nuclear Safety and Security Glossary: Terminology Used in Nuclear Safety, Nuclear Security, Radiation Protection and Emergency Preparedness and Response, 2022 (Interim) Edition, IAEA, Vienna (2022), https://doi.org/10.61092/iaea.rrxi-t56z
[25] INTERNATIONAL ATOMIC ENERGY AGENCY, Technical and Functional Specifications for Border Monitoring Equipment, IAEA Nuclear Security Series No. 1, IAEA, Vienna (2006).

Annex I

EQUIPMENT FOR RADIATION DETECTION

I–1. Personal radiation detectors are pocket sized, lightweight radiation detectors that can be worn on the body for the rapid detection of gamma, and sometimes neutron, radiation. These instruments trigger an alarm (e.g. audio, visual, vibrating) if the measured radiation level exceeds a preset threshold, and they are generally intended to signal potentially unsafe conditions. They are used to ensure personal safety, with little or no disruption to activities, since the wearer is normally able to use the detector effectively while performing other tasks. Given that they are small and compact, can be operated during extreme environmental conditions, are user friendly and involve minimal training, these detectors are primarily used by front line officers (e.g. border guards, the coastguard, customs officers, law enforcement). They are the least expensive type of radiation detection equipment but have limited sensitivity.

I–2. Handheld gamma and/or neutron survey meters are portable radiation detectors used to search for, and locate, nuclear and other radioactive material. They are larger than personal radiation detectors and generally offer greater detection sensitivity, although they are typically less sensitive than radiation portal monitors.

I–3. Handheld radionuclide identification devices are radiation detectors that can collect and analyse the gamma energy spectrum emitted by radionuclides and can provide isotope identification. They may also contain a neutron detector that can indicate the presence of neutron radiation. They have built-in software for spectral analysis and contain libraries of radionuclide data so that they are able to identify the radioisotopes most commonly encountered by front line officers. The main characteristics desired in radionuclide identification devices are sensitivity to gamma radiation, reliability of radionuclide identification and an indication of the approximate exposure rate. When items emitting radiation are detected by screening devices such as radiation portal monitors or personal radiation detectors, radionuclide identification devices may then be used for secondary inspection to determine the source of radioactivity and evaluate the potential threat. Most radionuclide identification devices can also be used as handheld gamma and/or neutron survey meters to locate the source of radiation.

I–4. Backpack based radiation detection systems are carried by the user to execute discreet searches; for example, in public areas. The detector — which

detects gamma and/or neutron radiation and which might or might not have identification capabilities — and the associated electronics are contained in the backpack. This makes backpacks particularly useful for radiation surveys of large areas before or during major public events, or for the detection of radiation in close proximity; for example, while walking down the centre of a passenger train or bus. They may also be used temporarily for area monitoring or they may be mounted on a small vehicle. These systems can be equipped with a global positioning system (GPS) for mapping purposes. Important considerations for their use are weight, ergonomics, battery life, charge time and data transmission capability, as well as ease of use and the time needed for user training.

I–5. Vehicle mounted radiation detection systems are mobile radiation detection systems that are mounted to or placed inside a vehicle. They may also be referred to as mobile detection systems. These systems can measure gamma and/or neutron radiation, and they can also support the identification of radionuclides emitting gamma radiation. They may be equipped with a GPS and may provide search and localization capabilities. Operationally, they can be used either in motion or as stationary equipment, and they offer increased flexibility.

I–6. Fixed radiation portal monitors are pass-through, non-intrusive monitors consisting of one or two pillars that contain gamma radiation detectors. In some cases, these monitors may be complemented by neutron detectors when sensitivity to nuclear material is desired. They can be used for screening pedestrians, vehicles, packages, personal luggage and other cargo. If the radiation measurement exceeds a preset threshold, the radiation portal monitor triggers an alarm to indicate the presence of nuclear or other radioactive material. These monitors include an occupancy sensor and may be linked to video recording equipment. Fixed radiation portal monitors are often deployed to monitor traffic at checkpoints and at designated points of exit or entry, such as seaports, airports, near land borders or rail crossings, and at international mail facilities. Spectroscopic radiation portal monitors can both detect radiation and identify the radionuclides. They are highly sensitive, but they are more expensive to procure, install and maintain than standard radiation portal monitors.

I–7. Radiation conveyor belt monitors are portal monitors that allow material to pass through detectors in a continuous flow by means of a conveyor drive. They are suitable for monitoring large quantities of items, with a typical example being the monitoring of public mail. Parcels and letters are placed on a conveyor belt to detect the presence of gamma and neutron radiation with high sensitivity. Conveyor belt monitors may be combined with X ray screening systems.

I–8. Airborne radiation detection systems can be mounted inside or outside an aircraft, including in uncrewed aerial vehicles, during their operation. They may be used for measurement, detection and localization of radioactive material. These systems may be equipped with a GPS for mapping purposes, and the data obtained by these systems are typically used for area mapping. They may be able to measure gamma and/or neutron radiation and can also incorporate the identification of radionuclides emitting gamma radiation.

I–9. Maritime radiation detection systems can be mounted to or placed inside a maritime vessel. They may be operated either in motion or in stationary mode. They may be able to measure gamma and/or neutron radiation and to support identification of radionuclides emitting gamma radiation and may be equipped with a GPS. They are manufactured for operation exclusively in marine environments.

Annex II

EXAMPLE OF A TEMPLATE FOR A JOINT DETECTION OPERATIONS PLAN FOR NUCLEAR AND OTHER RADIOACTIVE MATERIAL OUT OF REGULATORY CONTROL

II–1. To organize nuclear security detection operations involving multiple competent authorities in a State's interior, the joint detection operations plan for nuclear and other radioactive material out of regulatory control formalizes the coordination of the roles, responsibilities and authorities and the concept of operations of the different authorities. Table II–1 provides an example of the structure and the main components of a joint detection operations plan.

TABLE II–1. EXAMPLE COMPONENTS OF A JOINT DETECTION OPERATIONS PLAN FOR MATERIAL OUT OF REGULATORY CONTROL

Section	Purpose
Title page	Provides the title of the plan, approval date and version number, and is signed by representatives of the participating competent authorities.
Table of contents	Shows the structure of the plan and provides a quick overview of the plan.
Introduction	Provides the purpose and scope of the plan, including the mandate for its development, the participating competent authorities, the definitions of terms used in the plan and a list of the associated plans of the participating competent authorities.
Planning considerations	Describes preparatory activities and the process for assessing the priorities for managing potential incidents and nuclear security events. This section also includes the following: (a) Identification of potential scenarios for detection in the interior of the State that necessitate joint operations, including identification of likely adversaries, tactics and materials of concern;

TABLE II–1. EXAMPLE COMPONENTS OF A JOINT DETECTION OPERATIONS PLAN FOR MATERIAL OUT OF REGULATORY CONTROL (cont.)

Section	Purpose
Planning considerations (cont.)	(b) Description of resources to be deployed to implement joint operations, including the number of personnel, amount of equipment and training needs; (c) Identification of the legal authority under which joint operations may be conducted; (d) Identification of funding sources for joint operations.
Coordination and communication	Describes the chain of command and the coordination and communication mechanisms among all participating competent authorities, including the following: (a) Interface with the national regulatory body and operators of facilities where nuclear or other radioactive material is used, processed or stored; (b) Interface with national response authorities to locate and recover nuclear and other radioactive material out of regulatory control; (c) Interface with competent authorities responsible for nuclear forensics examinations; (d) Description of policies and protocols for information security; (e) Public and media communications strategy.
Concept of operations	Provides a description of the concept of operations and standard operating procedures for potential types of joint operation. The concept of operations generally includes the following: (a) Goals and functional outcomes of the detection process; (b) Existing policies and constraints affecting the operations; (c) Activities and interactions among stakeholders for alarm adjudication.

TABLE II–1. EXAMPLE COMPONENTS OF A JOINT DETECTION OPERATIONS PLAN FOR MATERIAL OUT OF REGULATORY CONTROL (cont.)

Section	Purpose
Roles and responsibilities	Describes the roles, responsibilities and areas of jurisdiction for each competent authority involved in each operation. Defines the lead competent authority for each type of joint operation.
Operational needs	Clarifies the needs for the conduct of operations for detection in the interior of a State and includes the following: (a) Dispute resolution; (b) Joint command structure; (c) Transfer of command; (d) Intelligence activities; (e) Detection; (f) Request for response and assessment of response time; (g) Information release.
Plan review and sustainability	Provides details of the mechanism for plan review and maintenance and covers sustainability considerations, including the following: (a) Regular time frame for conduct of review; (b) Regular review and update of risk and threat assessment; (c) Process for agreeing to, documenting and disseminating changes or amendments to the operational needs; (d) Assessment of training needs and needs for human and financial resources; (e) Maintenance of equipment; (f) Evaluation of the plan, including joint exercises.
Appendices	Includes items that support the plan, including the following: (a) Coordinating plans or protocols; (b) Subordinate plans or protocols.

Annex III

INFORMATION ALERTS OBTAINED FROM MEDICAL SURVEILLANCE

III–1. Law enforcement and health professionals have access to information that could be shared with other competent authorities and stakeholders to prevent or detect criminal or other intentional unauthorized acts involving nuclear and other radioactive material out of regulatory control.

III–2. When law enforcement has information about potential incidents involving nuclear and other radioactive material out of regulatory control, they need to notify hospitals and health emergency services. Raising the threat awareness among health professionals increases the likelihood that they will identify signs of suspicious injuries or activity related to a potential nuclear security event.

III–3. Health professionals (e.g. doctors, nurses, emergency health service personnel) might be the first to become aware of a potential nuclear security event during the performance of their daily duties, by encountering patients exhibiting symptoms of radiation exposure.

III–4. To allow effective communication of information between law enforcement and health professionals, communication protocols need to be developed and communicated to all parties. The establishment of these protocols is essential for the timely exchange of information. The aim is to communicate information at an early stage, if possible before establishing whether a criminal or intentional unauthorized act has taken place. The communication process includes an understanding of the information needs of each side and of who receives what kind of information and why.

III–5. Authorities need to establish the communication process in the form of a written document, enabling information exchange among all entities or parties and ensuring that the process is aligned with national legislation. Information needs to be shared on a need to know basis, using predefined and protected communication channels and with recognized points of contact.

III–6. An important consideration when establishing communication protocols is that medical data are often protected by national legislation concerning patient confidentiality, and therefore they constitute sensitive information. The legislation might include provisions for exemptions, allowing law enforcement

personnel, prosecutors or security agencies to gain access to medical data for specific reasons, such as an ongoing investigation of a potential nuclear security event or protection of the health and safety of the public. However, the legal liability of releasing medical data or patient information without the patient's consent may still be a concern for health professionals.

III–7. Provisions need to be made for compartmentalizing potentially sensitive information available to medical personnel, who do not have security clearance, working with a patient who could be associated with a nuclear security event.

IAEA
International Atomic Energy Agency

No. 27

ORDERING LOCALLY

IAEA priced publications may be purchased from our lead distributor or from major local booksellers.

Orders for unpriced publications should be made directly to the IAEA.

Orders for priced publications

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

Eurospan
1 Bedford Row
London WC1R 4BU
United Kingdom

Trade orders and enquiries:
Tel: +44 (0)1235 465576
Email: trade.orders@marston.co.uk

Individual orders:
Tel: +44 (0)1235 465577
Email: direct.orders@marston.co.uk
www.eurospanbookstore.com/iaea

For further information:
Tel. +44 (0) 207 240 0856
Email: info@eurospan.co.uk
www.eurospan.co.uk

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

Publishing Section
International Atomic Energy Agency
Vienna International Centre
PO Box 100
1400 Vienna, Austria
Telephone: +43 1 2600 22529 or 22530
Email: sales.publications@iaea.org
www.iaea.org/publications

This publication provides guidance on planning, implementing and evaluating systems and measures in a State in order to detect nuclear and other radioactive material out of regulatory control in the State's interior by means of instrument alarms and information alerts. The guidance covers the planning of detection operations, equipment deployment and human resources development. This publication is intended for authorities responsible for designing, implementing and sustaining nuclear security systems and measures within a State, such as personnel from the ministry of interior, law enforcement agencies, health authorities, national regulators, emergency response and national security organizations.

International Atomic Energy Agency
Vienna, 2024
www.iaea.org