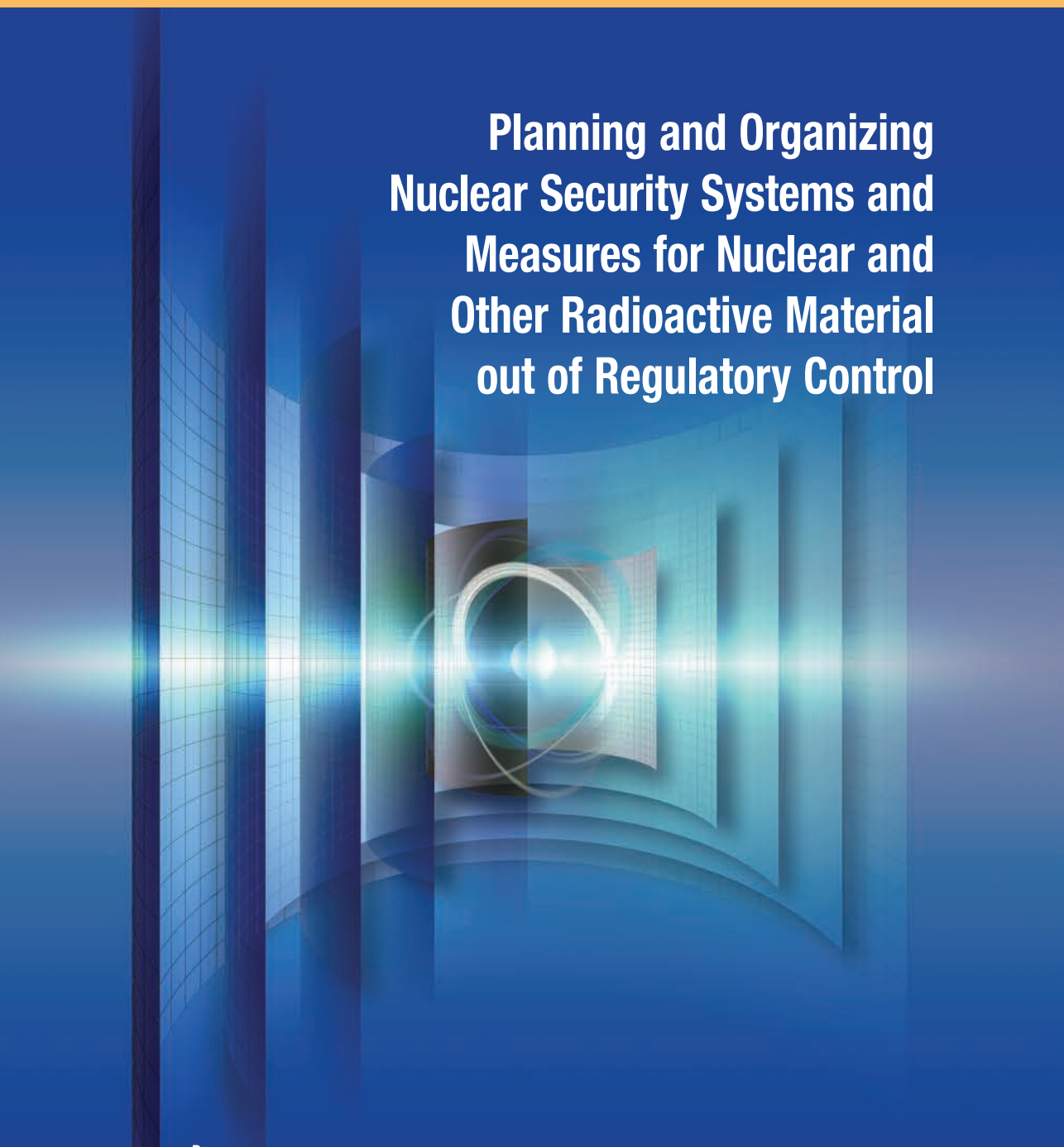
IAEA Nuclear Security Series No. 34-T

Technical Guidance

Planning and Organizing Nuclear Security Systems and Measures for Nuclear and Other Radioactive Material out of Regulatory Control



IAEA
International Atomic Energy Agency

IAEA NUCLEAR SECURITY SERIES

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

CATEGORIES IN THE IAEA NUCLEAR SECURITY SERIES

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

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

DRAFTING AND REVIEW

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

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

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

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

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

PLANNING AND ORGANIZING NUCLEAR SECURITY SYSTEMS AND MEASURES FOR NUCLEAR AND OTHER RADIOACTIVE MATERIAL OUT OF REGULATORY CONTROL

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

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

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

IAEA NUCLEAR SECURITY SERIES No. 34-T

PLANNING AND ORGANIZING NUCLEAR SECURITY SYSTEMS AND MEASURES FOR NUCLEAR AND OTHER RADIOACTIVE MATERIAL OUT OF REGULATORY CONTROL

TECHNICAL GUIDANCE

INTERNATIONAL ATOMIC ENERGY AGENCY
VIENNA, 2019

COPYRIGHT NOTICE

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

Printed by the IAEA in Austria
March 2019
STI/PUB/1842

IAEA Library Cataloguing in Publication Data

Names: International Atomic Energy Agency.
Title: Planning and organizing nuclear security systems and measures for nuclear and other radioactive material out of regulatory control / International Atomic Energy Agency.
Description: Vienna : International Atomic Energy Agency, 2019. | Series: IAEA nuclear security series, ISSN 1816–9317 ; no. 34-T | Includes bibliographical references.
Identifiers: IAEAL 19-01221 | ISBN 978–92–0–100119–1 (paperback : alk. paper)
Subjects: LCSH: Radioactive substances — Detection. | Nuclear non-proliferation. | Security systems. | Nuclear industry — Security measures.
Classification: UDC 341.67 | STI/PUB/1842

FOREWORD

by Yukiya Amano
Director General

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

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

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

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

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

EDITORIAL NOTE

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

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

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

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

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

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

CONTENTS

1. INTRODUCTION

BACKGROUND

1.1. Paragraph 2.1 of the Nuclear Security Fundamentals, IAEA Nuclear Security Series No. 20, Objective and Essential Elements of a State's Nuclear Security Regime [1], states that "The objective of a State's *nuclear security regime* is to protect persons, property, society, and the environment from harmful consequences of a *nuclear security event*." The nuclear security regime covers nuclear material and other radioactive material, whether it is under or out of regulatory control, and associated facilities and associated activities throughout their lifetimes [1].

1.2. This objective can be achieved by applying the principles set out in the Nuclear Security Fundamentals [1] and implementing recommendations contained in the set of Recommendations publications of the IAEA Nuclear Security Series:

— IAEA Nuclear Security Series No. 13, Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5) [2];
— IAEA Nuclear Security Series No. 14, Nuclear Security Recommendations on Radioactive Material and Associated Facilities [3];
— IAEA Nuclear Security Series No. 15, Nuclear Security Recommendations on Nuclear and Other Radioactive Material out of Regulatory Control [4].

This publication is complementary to, and consistent with, Refs [1–4].

1.3. A nuclear security event involving nuclear or other radioactive material out of regulatory control may lead to harmful health, economic, environmental and societal consequences. The phrase 'out of regulatory control' is used to describe a situation where nuclear material or other radioactive material is present without the appropriate authorizations, either because controls have failed for some reason or they never existed [4]. Reference [4] describes the objectives of the parts of the nuclear security regime relating to nuclear and other radioactive material out of regulatory control and detection and response measures to be used to achieve those objectives.

1.4. IAEA Nuclear Security Series No. 21, Nuclear Security Systems and Measures for the Detection of Nuclear and Other Radioactive Material out of

Regulatory Control [5], describes the necessary features of an effective nuclear security detection capability, and other guidance under preparation within the IAEA Nuclear Security Series, such as the national framework for managing the response to nuclear security events.

1.5. Because of the complexity of building an effective detection capability and response framework, a clear and structured process that accounts for the particular features of each, as well as the particular situation of the State, is needed. This publication provides detailed guidance in this area.

OBJECTIVE

1.6. The objective of this publication is to provide guidance on planning and organizing nuclear security systems and measures for the detection of criminal or intentional unauthorized acts[1] involving material out of regulatory control (the detection architecture, as described in Ref. [5]) and for the response to nuclear security events. The guidance includes processes for the identification of existing nuclear security systems and measures, determination of resource and capability gaps, and the design of new systems and measures to address identified gaps.

1.7. This publication is intended for States and relevant personnel from competent authorities responsible for the planning and organization of nuclear security systems and measures for material out of regulatory control.

SCOPE

1.8. The scope of this publication is the effective planning and organizing of nuclear security systems and measures for nuclear and other radioactive material out of regulatory control.

1.9. This publication covers an integrated planning process for designing the parts of a State's nuclear security regime that relate to material out of regulatory

[1] Criminal or intentional unauthorized acts involving material out of regulatory control may include the trafficking of material within and across State boundaries, the deliberate exposure (or attempt) of the public by the construction of a radiation exposure device, the deliberate dispersal (or attempt) of radioactive material by the construction of a radiological dispersal device, or the acquisition and use of nuclear material to build an improvised nuclear device.

control, specifically the nuclear security detection architecture for material out of regulatory control [5] and the framework for managing the response to nuclear security events. This includes:

(a) Relevant legislation, regulations, administrative arrangements and nuclear security risk assessments;
(b) Competent authorities and other organizations with responsibilities relating to material out of regulatory control, including a coordinating body or mechanism;
(c) Nuclear security systems and measures for the prevention of, detection of and response to nuclear security events involving material out of regulatory control.

1.10. This publication is not intended to provide guidance on the implementation and evaluation of nuclear security systems and measures and is not intended to provide guidance for preparedness and response to a nuclear or radiological emergency (for this, see Refs [6–8]).

1.11. The planning process presented in this publication is described at the State level; however, it may be applicable for planning at other levels (e.g. organizational or local).

STRUCTURE

1.12. Following this introduction, Section 2 provides an overview of an integrated planning process that may be used to design a State's nuclear security detection architecture for material out of regulatory control and a framework for managing the response to nuclear security events. Section 3 describes the functional outcomes and how to develop and review them. Section 4 explores assessing capabilities and resources. Section 5 presents the development an integrated design plan. Appendices I–III provide supplemental guidance for developing communication strategies, coordination mechanisms and establishing sustainability mechanisms. Annexes I and II provide examples of nuclear security planning roles and responsibilities and functional outcomes. Annex III provides a template that may be used by planners in following the planning and organization process described in this publication.

2. OVERVIEW OF AN INTEGRATED PLANNING PROCESS

2.1. States should develop a multilayered and risk informed approach to design and implementation of nuclear security systems and measures that incorporates the concept of defence in depth. Such an approach would include systems and measures: to prevent materials from leaving regulatory control through loss or theft; to detect materials out of regulatory control; and to respond to potential nuclear security events. This publication focuses on the State level planning of systems and measures for the detection of criminal or intentional unauthorized acts involving material out of regulatory control (the detection architecture, as described in Ref. [5]) and for the response to potential nuclear security events.

2.2. Using a clearly defined process for planning enables a State to establish or enhance its detection architecture for material out of regulatory control and its response framework in a structured and integrated manner. The use of the process described in this publication can strengthen a State's capability to prevent, detect and respond to criminal or intentional unauthorized acts with nuclear security implications involving material out of regulatory control, by assisting planners:

(a) To avoid systematic gaps;
(b) To enhance communication and coordination at all levels because input from all levels is needed in the planning process;
(c) To ensure clarity and transparency to all relevant competent authorities and other stakeholders, on account of their participation in the planning process;
(d) To integrate systems and measures for material out of regulatory control with other nuclear security and national security areas;
(e) To improve the effectiveness of the use of resources and to avoid duplication of efforts;
(f) To demonstrate a commitment to sustainability and continuous improvement, including the incorporation of increased flexibility and the ability to adapt to changing needs, priorities and availability of resources.

2.3. The basis for developing a State's detection architecture and response framework includes the following:

(a) Appropriate legislation, regulation and administrative arrangements that establish roles, responsibilities and authority;
(b) Nuclear security threat and risk assessments;
(c) A national mandate to detect and respond to criminal and intentional unauthorized acts involving material out of regulatory control.

PLANNING PROCESS

2.4. Effectively developing and sustaining a detection architecture and response framework involves planning, implementation and evaluation processes. These three processes are performed iteratively, so that the results of the planning process provide input to the implementation process, and the results of the implementation process are then evaluated during the evaluation process. The next iteration of the planning process is based on the results of the evaluation process, and so forth. Such an iterative system promotes continuous improvement and evolution, enabling the detection architecture and response framework to adapt over time. This publication focuses on the planning process.

2.5. The planning process comprises three steps: direction, assessment and design. Figure 1 illustrates these steps of the planning process in relation to other phases of developing and sustaining the detection architecture and response framework. The planning process should account for the full spectrum of nuclear security activities in these areas (see also fig. 1 of Ref. [5]).

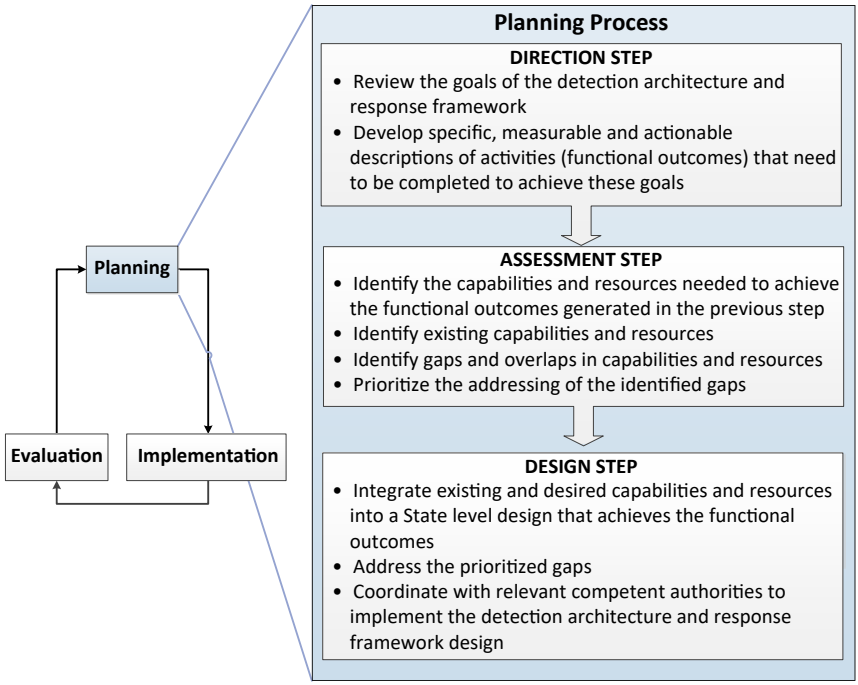


FIG. 1. The planning process.

2.6. The development of an integrated design plan is the expected output of the planning process. An integrated design plan, through promoting cooperation and coordination among various competent authorities and other stakeholders, can result in a more effective use of resources and capabilities. When the integrated design plan is complete, the planning process is complete, and the respective competent authorities that are responsible for implementing portions of the design plan can then begin the implementation process.

2.7. The three steps of the planning process are briefly described in paras 2.8–2.12 and are discussed in detail in Sections 3–5.

Direction step

2.8. In the direction step, planners review the goals[2] of the detection architecture and response framework and develop specific, measurable and actionable descriptions of activities that need to be completed to achieve these goals.

2.9. These descriptions, referred to as functional outcomes[3], can be developed at different levels of specificity, and articulate specific directions for the design of the detection architecture and response framework.

Assessment step

2.10. In the assessment step, an understanding of the broader context of the detection architecture and response framework is developed. To build this context and to provide input into the design step, the planners:

(a) Identify the capabilities and resources needed to achieve the functional outcomes generated in the previous step;
(b) Identify existing capabilities and resources;
(c) Identify gaps and overlaps in capabilities and resources;
(d) Prioritize the addressing of the identified gaps.

[2] In this publication, 'goals' refer to high level statements that set the general direction.

[3] In this publication, 'functional outcomes' refer to specific descriptions of actions to be performed.

Design step

2.11. In the design step, capabilities and resources identified in the assessment step are strategically integrated to achieve the functional outcomes. To accomplish this, planners consider methods for:

(a) Integrating existing and desired capabilities and resources into a State level design that achieves the functional outcomes;
(b) Addressing the prioritized gaps;
(c) Coordinating with relevant competent authorities to implement the detection architecture and response framework design.

2.12. Priorities and trade-offs are considered to determine the best options to achieve the functional outcomes given existing constraints, and an integrated design plan is developed and formalized for the structured development and implementation of necessary capabilities and resources.

UNDERLYING PRINCIPLES FOR PLANNING

2.13. Eight principles should be considered when executing all three steps of the planning process (see paras 2.14–2.22):

(1) Goal oriented development;
(2) Broad engagement among competent authorities and other stakeholders;
(3) Clear definition of roles, responsibilities, authority and accountability;
(4) Establishment of mechanisms for communication and coordination;
(5) Integration with other safety and security measures;
(6) International cooperation;
(7) Continuous evolution of the detection architecture and response framework;
(8) Promotion of a nuclear security culture.

Goal oriented development

2.14. Capabilities and resources should be developed in support of the goals and functional outcomes for the detection architecture and response framework that are established by relevant national policies and strategies. From early in the planning process, planners should ensure that each capability or resource included in the design explicitly contributes to the goals and functional outcomes. Performance indicators evaluating the contribution of each capability or resource

to the goals and functional outcomes should be established early in the planning process for each capability or resource.

Broad engagement among competent authorities and other stakeholders

2.15. Engagement with all relevant stakeholders can provide technical, legal and operational expertise and enhance integration of capabilities by improving communication among stakeholders with regard to priorities, resources and needs, with the aim of improving mutual understanding. The transparency in the development process built through such engagement may contribute to stakeholders' understanding of the context of their role within the nuclear security regime and may also increase their recognition of the importance of the threat and the importance of the measures to counter it taken by their organization.

Clear definition of roles, responsibilities, authority and accountability

2.16. The development and operation of the full set of systems and measures for material out of regulatory control require the coordination of many competent authorities and other stakeholders. Each stakeholder needs to understand its respective roles and responsibilities, be provided with the requisite authority to undertake the roles and responsibilities and be held accountable by the State for the performance of these roles and responsibilities.

Establishment of mechanisms for communication and coordination

2.17. Effective communication of relevant information and coordination of operational activities are essential to the performance of the detection architecture and response framework in a dynamic security environment. Mechanisms should be established for communication and coordination as part of the planning process. Additional guidance on communication and coordination mechanisms is provided in Appendices I and II.

2.18. Communication mechanisms should preserve the security of sensitive information, including through communicating sensitive information only on a 'need to know' basis.

Integration with other safety and security measures

2.19. Measures carried out under the detection architecture and response framework operate in conjunction with measures carried out under other parts of the nuclear security regime (e.g. measures for facility security), other national

security measures (e.g. anti-terrorism measures) and nuclear safety measures. The experience, infrastructure and resources relating to these other measures can be used to increase the efficiency of the detection architecture and response framework, so that the detection and response measures reinforce, rather than compete with, other national priorities.[4]

International cooperation

2.20. Cooperation with international and regional organizations as well as with other States can provide additional knowledge and expertise for the development of the detection architecture and response framework.

Continuous evolution of the detection architecture and response framework

2.21. An effective detection architecture and response framework is responsive to shifting national needs and priorities as well as external factors, such as the emergence or disappearance of specific nuclear security threats.[5] States should conduct periodic as well as ad hoc reviews of the threat and risk assessments for the detection architecture and response framework [9].

Promotion of a nuclear security culture

2.22. An effective nuclear security culture (as described in detail in Ref. [10]) can strengthen the detection architecture and response framework by emphasizing the core beliefs that there exists a credible threat and that nuclear security is important, as well as through organizational principles and a well developed management system. Though an effective nuclear security culture can be difficult to cultivate, many mechanisms can facilitate its adoption by organizations, such as professional training and qualifications and awareness programmes. Demonstration by leadership at all levels of their commitment to effective nuclear security is important for this culture to be adopted at all levels [10].

---

[4] For example, a measure such as an X ray scanner at a border crossing point could provide detection capability not only for the detection of smuggling activities unrelated to nuclear and other radioactive material but also for the detection of material out of regulatory control.

[5] In this publication, the term ‘nuclear security threat’ is used to refer to the meaning expressed by the definition in the Nuclear Security Fundamentals [1]. The unqualified term ‘threat’ is used more generally to refer to either the threat actor (also termed adversary) or the threat object (also termed device).

BASIS FOR THE PLANNING PROCESS

National security context

2.23. During the planning process, States should consider the broader national security context in which the nuclear security regime operates. In particular, States should take into account:

(a) Relevant national legislation, regulations and policies in nuclear security and national security;
(b) Relevant national plans and strategies;
(c) Results of the national risk assessment;
(d) Regional and global considerations that could affect nuclear security in the State.

These considerations are briefly discussed in paras 2.24–2.27.

2.24. To the extent possible, the detection architecture and response framework should be based on existing laws and regulations, although it may be determined during the planning process that new laws or regulations may be needed. Because modifications to laws and regulations may take time to process, administrative agreements such as memoranda of understanding could be developed to serve this purpose in the interim, where applicable [11, 12].

2.25. When planning the detection architecture and response framework, the State should also take into account relevant national plans and strategies which may or may not directly address nuclear security, such as emergency or civil defence response plans. For example, existing planning documents may have codified goals that can be used as part of the planning process.

2.26. Risk assessment combines the estimated likelihood of particular nuclear security events, expressed as a function of the threat and vulnerability, with their consequences to provide an overall measure useful for the design or improvement of nuclear security systems and measures [9]. States should consider performing a national level risk assessment for nuclear security, as described in Ref. [9]. Such an assessment provides a basis for implementing a graded approach and prioritizing capabilities and resources.

2.27. States should consider relevant international agreements and legal instruments, international consensus guidance and other guidance relevant to nuclear security. States should also consider how the national nuclear

security regimes of neighbouring States might influence their risk assessment as part of planning and implementation of the detection architecture and response framework. In addition, international organizations may be consulted as necessary.

Key roles within the detection architecture and response framework

2.28. The planning, implementation and evaluation of the detection architecture and response framework involves multiple competent authorities as well as other stakeholders. Key nuclear security roles, as well as the relevant organizations that may fulfil those roles, should be identified early in the planning process in order to facilitate information sharing, build consensus and foster communication. The level of involvement of relevant competent authorities and other stakeholders may change during the planning, implementation and evaluation processes, depending on their respective roles and responsibilities.

2.29. Relevant competent authorities and other stakeholders who should be involved in the planning process may be identified by considering the following questions:

(a) Are there legal mandates or national policies that specify organizations for national security, nuclear security, and preparedness and response to radiological emergencies?
(b) Which jurisdictions or geographical regions are relevant to the detection architecture and response framework [5]?
(c) Are there facilities or organizations that use, store or transport nuclear material and other radioactive material?
(d) Are there governmental or non-governmental organizations with the relevant capabilities or expertise?
(e) Are there organizations responsible for disseminating relevant information on the detection of criminal or intentional acts involving material out of regulatory control or the response to nuclear security events to the general public?
(f) Are there international partners or organizations with capabilities, expertise or experience that could contribute to the development of the detection architecture and response framework?

2.30. Typical stakeholders involved in the detection of criminal or intentional unauthorized acts involving material out of regulatory control or in the response to nuclear security events include: intelligence and security personnel; operational

personnel such as law enforcement officers; policy, legal and regulatory subject matter experts; and technical subject matter experts.

2.31. Each type of stakeholder can provide perspectives and insights that are useful in the planning process. Intelligence and security personnel can identify where and how current operational information can be used in designing and maintaining the detection architecture and response framework. Operational personnel who implement detection and response systems and may include front line officers and first responders can provide expertise with regard to the operational environment, the effectiveness of currently deployed capabilities and the potential for integrating nuclear security capabilities with other ongoing activities. Policy, legal and regulatory subject matter experts can provide context for the governance of the detection architecture and response framework. Technical subject matter experts can provide the required expertise in specialized fields including security, safety, health, science and technology, information sharing and communication, training and exercises and human factors.

2.32. On account of the diversity of competent authorities and other stakeholders involved in the detection architecture and response framework, para. 3.8 of Ref. [4] recommends:

> "The State should ensure proper cooperation, coordination, information exchange and integration of activities and clearly defined responsibilities across multiple *competent authorities*, and establish a coordinating mechanism or identify an existing governmental body, committee or organization to act as the coordinating body".[6]

2.33. Consistent with national practice, this coordinating body or mechanism may be established through legislation or administrative arrangements that grant sufficient authority and resources (technical, financial and human) to the coordinating body or mechanism in order to carry out its responsibilities.

2.34. Annex I provides an example of the roles and responsibilities that might be needed for implementing the detection architecture and response framework, as well as examples of organizations that could fill those roles.

---

[6] As described in Ref. [4], the coordinating body or mechanism is responsible for coordination of all nuclear security activities involving nuclear and other radioactive material out of regulatory control.

3. FUNCTIONAL OUTCOMES

3.1. Addressed in Step 1 of the planning process, functional outcomes provide specific, measurable and actionable descriptions of the activities that need to be completed to achieve the goals of the detection architecture and response framework, and to establish the foundation for identifying necessary capabilities and resources.

3.2. While goals are broad descriptions of the desired end state for the detection architecture and response framework, functional outcomes are specific activities that need to be performed in order to achieve these goals. Functional outcomes are derived from established goals or national mandates, and are more specific, measurable and actionable than the infrastructure goals they support.

3.3. The goals and functional outcomes for the detection architecture and response framework should reflect current national priorities and appropriately address the levels and types of threat and risk present in the State (see paras 2.23–2.27).

DEVELOPING FUNCTIONAL OUTCOMES

3.4. To develop functional outcomes, planners should consider: any relevant international and national legislation, regulations, administrative arrangements and policies; the national threat and risk assessments; the goals and scope for the detection architecture and response framework; and the roles of competent authorities and other stakeholders. Using this information, functional outcomes should be developed with the perspectives discussed in paras 3.7–3.15. These functional outcomes should then be reviewed. Ultimately, this process should result in finalized goals and functional outcomes for the detection architecture and response framework that will be provided to the assessment step. The process for developing functional outcomes is summarized in Fig. 2.

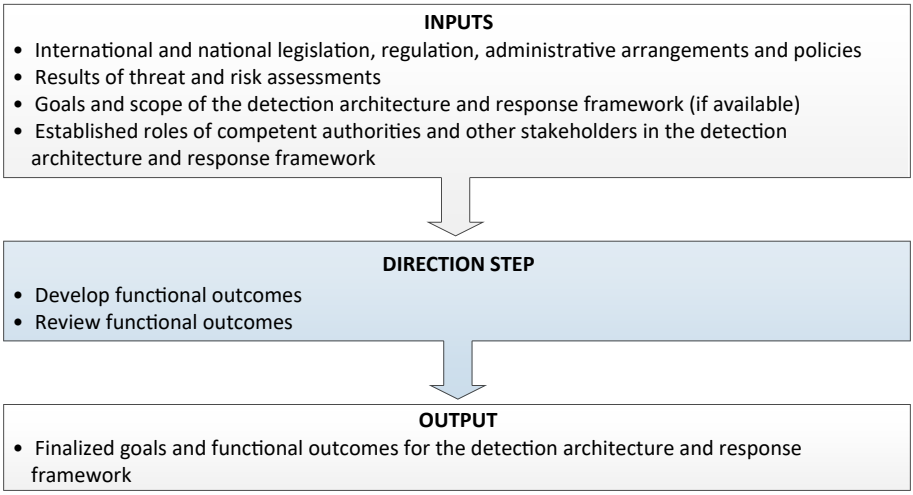


FIG. 2. Overview of the direction step in the planning process.

3.5. The systematic development of functional outcomes can have the following benefits:

(a) The activities necessary to achieve the desired goals for the detection architecture and response framework are clearly articulated.
(b) A common understanding of the direction for development of the detection architecture and response framework is developed, which enables the organization of roles and responsibilities, the creation of procedures for communication and cooperation among organizations and the identification of performance indicators.
(c) Increased acceptance of the threat among stakeholders as well as each organization's role in countering it, built through providing detail and clarity about the purpose of the detection architecture and response framework to ensure consistency in design.
(d) Coordination of the development of capabilities and resources and minimization of capability and resource gaps.

3.6. The systematic development of functional outcomes is discussed in more detail in paras 3.7–3.15.

3.7. One process for developing functional outcomes based on the information available to the planners is the use of perspectives. Perspectives are systems for considering and prioritizing nuclear security activities to facilitate the

development of functional outcomes. They provide practical methods of incorporating a variety of viewpoints on nuclear security, communicating threat and risk related concepts and organizing information on risk.

3.8. In paras 3.10–3.15, four perspectives are discussed: risk oriented, chronological, geographical and threat oriented. Planners can use multiple perspectives in combination when developing functional outcomes. The use of a risk informed approach is recommended in Essential Element 9 of the Nuclear Security Fundamentals [1], as this approach incorporates information relating to threats, vulnerabilities and potential consequences (see also Ref. [9]). However, the other three perspectives may be used in combination with this perspective to ensure a comprehensive set of functional outcomes. The use of different perspectives can assist in developing functional outcomes by providing an organizing structure for key concepts, assumptions and expectations relevant to nuclear security.

3.9. States should consult existing threat and risk assessments to inform the application of the questions in the following section to the development of functional outcomes. Example functional outcomes using the four perspectives outlined here are illustrated in Annex II.

Risk oriented perspective

3.10. A risk oriented perspective assesses nuclear security detection and response activities by considering threats, vulnerabilities and potential consequences. The following questions can help to guide the development of functional outcomes using a risk oriented perspective:

(a) Are there nuclear security systems and measures that are robust against a wide range of threats?
(b) Which nuclear material or other radioactive material (including type, quantity and form) or devices constitute a concern?
(c) Are there nuclear security systems and measures that are effective in detecting particular devices or material of concern?
(d) Are there device components of concern that can be detected that are not composed of nuclear material or other radioactive material?
(e) Are there indications that some potential adversary routes to and from potential targets (pathways) or nuclear security systems and measures may be particularly vulnerable to adversary exploitation?
(f) Have specific pathways been targeted for other forms of trafficking, for example the trafficking of drugs?

(g) What are the potential consequences to be considered when designing the detection architecture and response framework, and what are their type and severity? Which measures can be used to prevent, mitigate or respond to these consequences?

3.11. States should consult existing national risk assessments where possible, as some of these questions may have been addressed in previous all hazards and organizational risk assessments.

Chronological perspective

3.12. A chronological perspective assesses nuclear security detection and response activities based on a time progression for detecting and responding to a nuclear security event. The following questions can help to guide the development of functional outcomes using a chronological perspective:

(a) Which nuclear security activities could deter or dissuade an adversary from planning or executing a criminal or intentional unauthorized act involving material out of regulatory control?
(b) Which nuclear security activities could reduce an adversary's capability to plan or execute a criminal or intentional unauthorized act involving material out of regulatory control?
(c) Which nuclear security activities and capabilities are needed to encounter[7] and track threats?
(d) What kind of information should be collected to support the detection of criminal or intentional unauthorized acts involving material out of regulatory control and the response to nuclear security events?
(e) Which activities are needed to acquire and manage information relating to the detection of criminal or intentional unauthorized acts involving material out of regulatory control and the response to nuclear security events?
(f) Are there safety, security or safeguards measures that can be used to aid in detection of criminal or intentional unauthorized acts involving material out of regulatory control and the response to nuclear security events?
(g) How is information produced, utilized and managed in the detection architecture and in the response framework?

[7] In this context, 'encounter' refers to the collocation of security capabilities and resources with threats, such as a law enforcement officer on patrol confronting a nuclear security threat, a proximity sensor along the undesignated border indicating intrusion, and a radiation detector at a designated point of entry or exit sounding an alarm following the detection of radiation.

(h) Which capabilities and expertise are needed to analyse effectively information relating to nuclear security events?
(i) Which information, capabilities and authorities are needed to adjudicate an encounter?
(j) Which capabilities are necessary to effectively detain or seize, recover and control material, or to render harmless threats or associated devices of concern?
(k) Which capabilities are needed to collect, secure and analyse evidence and exhibits?
(l) Which capabilities are needed to isolate, classify, package and document nuclear material or radioactive material for transport, carriage, storage, disposal or return to regulatory control?
(m) Which communication, coordination, command and control mechanisms are necessary to integrate detection and response activities, including informing the general public, where appropriate?
(n) Which arrangements are needed to notify the IAEA and other international partners and organizations of nuclear security events and to request assistance, where appropriate?

Geographical perspective

3.13. A geographical perspective assesses nuclear security detection and response activities by considering the pathway an adversary might traverse to commit a criminal or intentional unauthorized act involving material out of regulatory control. This pathway can be modelled by considering geographical layers to represent each step through which the adversary may travel to reach the intended target. An example model is shown in Fig. 3, which groups nine layers into three

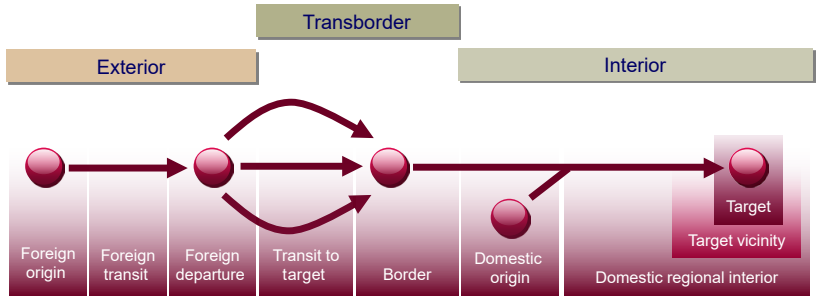


FIG. 3. Geographical perspective of a nuclear security infrastructure and pathways.

regions (exterior, transborder and interior), and the circle represents the nuclear material or other radioactive material. Measures to prevent, detect and respond to a potential nuclear security event involving material out of regulatory control can be implemented within each geographical layer.

3.14. The following questions can help to guide the development of functional outcomes using a geographical perspective:

(a) Are there domestic or nearby foreign facilities with nuclear material or other radioactive material, or associated activities?
(b) What kind of nuclear security activities could be implemented near the pathways that could lead to or from such facilities, and where should they be implemented?
    (i) Which pathways could be used to transport nuclear material or other radioactive material?
    (ii) Are there strategic locations, such as checkpoints or border crossings, which could be used by the detection architecture and response framework?
    (iii) How could geographical features, including structures (e.g. valleys, mountain passes and bridges), be utilized to minimize the number of locations needed to screen large volumes of traffic?
(c) Are there multipurpose activities at the border and in the interior that could be utilized by the detection architecture and response framework?
    (i) Are there locations where other screening or inspection activities have already been implemented where nuclear detection activities could be integrated?
    (ii) Are there existing general response capabilities within a geographical area, such as fire service or public health, where nuclear security response capabilities could be integrated?
(d) How do nuclear security activities in each geographical layer complement and reinforce those activities occurring in other layers?

Threat oriented perspective

3.15. A threat oriented perspective assesses nuclear security detection and response activities based on significant events associated with an adversary's ability to commit a criminal or intentional unauthorized act involving nuclear or other radioactive material out of regulatory control. The following questions can help to guide the development of functional outcomes using a threat oriented perspective (see also Ref. [9]):

(a) What are potential motivations, capabilities and intentions for an adversary? Are there other attributes (e.g. history) that can be used to characterize an adversary?
(b) Are there strategic locations, critical infrastructure or other points of interest that may be targeted by an adversary? What are the geographical pathways to such locations?
(c) Are there multiple adversaries? Are there implications if adversaries cooperate with each other through collusion?
(d) Which tactics have adversaries previously used? Which tactics might an adversary use to counter or avoid the State's nuclear security efforts?
(e) Which nuclear material and other radioactive material (type, quantity and form) might an adversary need to achieve his or her goal?
(f) Is there specialized knowledge relating to nuclear material and other radioactive material or devices that an adversary would need to learn (e.g. for the construction of an improvised nuclear device or radiological dispersal device)?
(g) Which resources, capabilities and infrastructure would be needed to carry out a successful nuclear security event involving material out of regulatory control?

REVIEWING FUNCTIONAL OUTCOMES

3.16. Once a set of functional outcomes has been developed, it should be reviewed by appropriate competent authorities using the appropriate criteria (see paras 3.17–3.21). If the competent authority determines that criteria have not been satisfied, then the functional outcomes should be modified accordingly. The functional outcomes should be reviewed not only individually, but also as a set, to provide insights into the completeness of the detection architecture and response framework.

3.17. Criteria for reviewing individual functional outcomes should be goal oriented, sufficient, time bound and assessable, as discussed in paras 3.18–3.21.

3.18. Each functional outcome should have a clear link to one or more infrastructure goals and/or a legislative or regulatory mandate. Establishing clear links enables the personnel carrying out the design step of the planning process to understand the impact of each functional outcome on achieving the goals of the detection architecture and response framework.

3.19. Functional outcomes should be detailed enough to provide sufficient guidance for the personnel carrying out the design step of the planning process, but not overly complex so that they dictate the specifics of implementation or the operational constraints. The functional outcomes should provide the required flexibility for the designers of the detection architecture and response framework to consider multiple solutions.

3.20. Functional outcomes should be achievable within a specified timeframe. A clearly defined timeframe for accomplishing the outcome helps the planning team to focus their efforts on an infrastructure design that can be planned for, and implemented within, the designated timeframe.

3.21. Performance indicators should exist to assess the execution of the functional outcomes. These metrics should generally consist of either direct or proxy criteria[8] for assessing performance.

3.22. In addition to reviewing the individual functional outcomes, planners should also consider reviewing the full set of functional outcomes to ensure that the set is comprehensive and that each functional outcome is unique. The full set of functional outcomes should encompass all activities needed to achieve the goals of the detection architecture and response framework. Excluding activities from consideration due to constraints should be reserved for the design step, so that capabilities selected are based on the entire set of functional outcomes. The functional outcomes should also minimize duplication to the extent possible. A functional outcome is unique if its removal results in the full set of functional outcomes no longer being comprehensive.

3.23. The developed and reviewed functional outcomes should be formalized before proceeding to the next step in the planning process.

[8] Proxy data are data used when actual event data are not available. For example, if real data on response times to a nuclear security event are not available, exercises can be used to estimate response times.

4. CAPABILITIES AND RESOURCES

4.1. Once the direction step of the planning process has been completed and the functional outcomes have been developed and formalized, the next step is the assessment of capabilities and resources.

4.2. The goals and functional outcomes generated in the direction step serve as the input for the assessment step, in which the following four tasks are completed:

(1) The current situation is assessed to determine the capabilities and resources required to meet the functional outcomes (see paras 4.4 and 4.5).
(2) Existing capabilities and resources are identified (see paras 4.6–4.9).
(3) Gaps in capabilities and resources are determined (see paras 4.10 and 4.11).
(4) Gaps in capabilities and resources are then prioritized (see paras 4.12–4.14).

The output of this step is a list of desired capabilities and resources to be used in the detection architecture and response framework as well as a list of prioritized gaps and a justification for the prioritization. This information is then used in the next step of the planning process, the design step. The process for assessing capabilities and resources is summarized in Fig. 4.

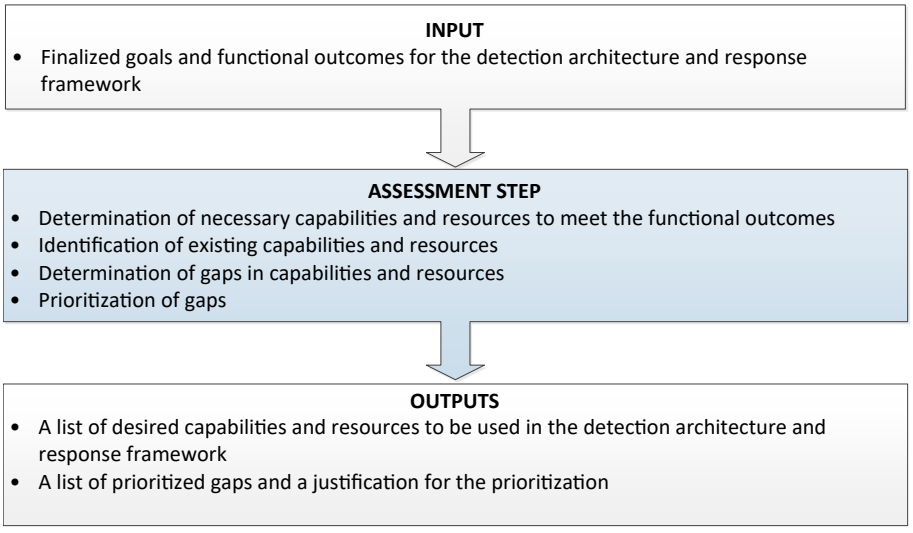


FIG. 4. Overview of the assessment step in the planning process.

4.3. A systematic assessment of capabilities and resources can have the following benefits:

(a) Organizational capabilities and resources are linked to functional outcomes.
(b) An opportunity is provided to address capability and resource gaps and vulnerabilities.
(c) A basis is provided for the design of the detection architecture and response framework.

DETERMINING NECESSARY CAPABILITIES AND RESOURCES

4.4. Different capabilities and resources may be necessary to meet various functional outcomes. For instance, the determination of necessary capabilities and resources should account for the different operational needs that apply in the exterior, transborder and interior regions. In reaching this determination, planners should seek to understand the expected function and performance of the various capabilities.

4.5. The following questions can be used by States to determine the capabilities and resources required for the detection architecture and response framework:

(a) Which capabilities are needed to effectively complete key nuclear security activities (see fig. 1 of Ref. [5]), including assessing threats, detecting criminal or intentional unauthorized acts involving material out of regulatory control, assessing alarms and alerts, interdiction, managing radiological crime scenes, protecting and analysing evidence and/or exhibits, conducting nuclear forensic examinations (including coordination with traditional forensic examinations) and regaining regulatory control?
(b) What are the potential consequences associated with the assessed nuclear security event scenarios and how could these consequences be mitigated?
(c) Are different capabilities needed for each of the relevant regions (i.e. exterior, transborder and interior)?
(d) Are different capabilities needed for detection and response relating to various transit modes (e.g. air, land and maritime)?
(e) Which response actions and associated capabilities are needed to manage a crime scene [13]?
(f) Which considerations should be taken into account for protecting and analysing evidence or exhibits from a crime scene, including nuclear material and other radioactive material or evidence or exhibits possibly contaminated with radioactive material?

(g) Which capabilities are needed to conduct successful nuclear forensic examinations [14]?
(h) Which capabilities are needed to regain regulatory control of material out of regulatory control (e.g. radiological surveys, decontamination, packaging, transport, storage and documentation)?
(i) Which information sharing mechanisms are needed to enable all relevant stakeholders to coordinate and communicate?

IDENTIFYING EXISTING CAPABILITIES AND RESOURCES

4.6. The detection architecture and response framework should use existing capabilities and resources to the extent possible, which may be available from local, national or international sources [5, 6]. Frequently, capabilities and resources used to address other areas of national priority are, or can be, integrated with nuclear security. For example, existing capabilities and resources for border security and emergency response may apply to nuclear security. These existing capabilities and resources can exist in governmental, domestic non-governmental, and international or regional entities.

Governmental capabilities and resources

4.7. Most States have established governmental capabilities and resources that can be expanded or augmented to address nuclear security goals, such as:

(a) Personnel and infrastructure relating to law enforcement, public safety organizations and the military;
(b) Laws and regulations already in place;
(c) Communication and coordination mechanisms in place for situations such as natural disasters;
(d) Command and control protocols, such as an emergency management system;
(e) Technical expertise in fields such as data analysis and spectroscopy;
(f) Infrastructure, such as border crossing checkpoints, laboratories and electric grids;
(g) Other financial and human resources.

Non-governmental capabilities and resources

4.8. Non-governmental entities, such as private industry, academia and non-governmental organizations can also have capabilities and resources that can be used as part of the detection architecture and response framework, such as:

(a) Technical expertise;
(b) Capabilities for commercial design, testing and manufacturing of equipment;
(c) Infrastructure such as training facilities and laboratories;
(d) Other financial and human resources.

International and regional capabilities and resources

4.9. A State may use existing bilateral, regional and international programmes to strengthen its national nuclear security infrastructure. For example, international networks, databases and notice systems might be used, such as the IAEA Incident and Trafficking Database and the INTERPOL CBRNE Monthly Digest, its intelligence reports and Operation Fail Safe. In addition, States may choose to use international, regional and professional organizations, meetings and training, such as those conducted by the Joint Research Centre of the European Commission, Europol, the Global Initiative to Combat Nuclear Terrorism, INTERPOL, the International Civil Aviation Organization, the International Maritime Organization, the Nuclear Forensics International Technical Working Group and the World Customs Organization. States may also benefit from the use of international nuclear security guidance in this area.

DETERMINING GAPS IN CAPABILITIES AND RESOURCES

4.10. After existing capabilities have been identified, a gap analysis should be performed to determine and document the discrepancies between necessary and existing capabilities and resources. It should reveal areas for improvement, areas of redundant or overlapping capabilities and the significance of the gap.

4.11. Types of gap include the following:

(a) Governance gaps, such as policy, legal and regulatory shortcomings;
(b) Management gaps, such as changes in leadership;
(c) Knowledge gaps, such as deficiencies in training, awareness and expertise;

(d) Operational gaps, such as environmental unsuitability, absence of procedures, too little coordination among authorities and difficulties in using equipment;
(e) Technical gaps, such as inadequate detector sensitivity and resolution, and software incompatibility when sharing information;
(f) Resource gaps, such as insufficient financial support for detection and response, insufficient staffing levels and poor access to equipment;
(g) Sustainability gaps, such as insufficient maintenance of equipment and lack of knowledge management.

PRIORITIZING GAPS IN CAPABILITIES AND RESOURCES

4.12. The priority of addressing the identified gaps can be determined based on criteria reflecting the gap's significance to the detection architecture and response framework. Such a set of criteria allows relevant competent authorities to determine which gaps merit their immediate efforts. They also provide justification for decisions on detection architecture and response framework needs and resource allocations.

4.13. Prioritization of gaps can involve multiple criteria and reflect national and international policies as well as political considerations, including the following:

(a) The likelihood or potential consequences of a nuclear security event as a result of a gap;
(b) Shortcomings in performance measured against the functional outcomes;
(c) The effect the gap might have on national security;
(d) Public perception of risk;
(e) The frequency of occurrence of a particular gap.

4.14. On account of the various competent authorities and other stakeholders involved, it might be difficult to achieve consensus on a prioritization for addressing gaps in the detection architecture and response framework. In such cases, it is important for planners to seek to understand the priorities and constraints of all stakeholders as well as to identify commonalities and origins of differences, and the responsibility and authority for the final prioritization should be transparent and clearly defined.

5. INTEGRATED DESIGN PLAN

5.1. The design step uses the outputs of the direction step and the assessment step — the goals and functional outcomes, existing capabilities and resources, and prioritized gaps and justification — to design the detection architecture and response framework. This design should aim to integrate existing and desired capabilities and resources effectively and strategically to achieve the functional outcomes and to address the prioritized gaps identified, given existing constraints and taking into consideration priorities and trade-offs. The completed design should be reviewed and assessed to understand how well it will address the prioritized gaps, then formalized in a design plan document and approved by the coordinating body or mechanism. Thus, the output of the design step is a formal design plan for the detection architecture and response framework. The process for developing a design is summarized in Fig. 5.

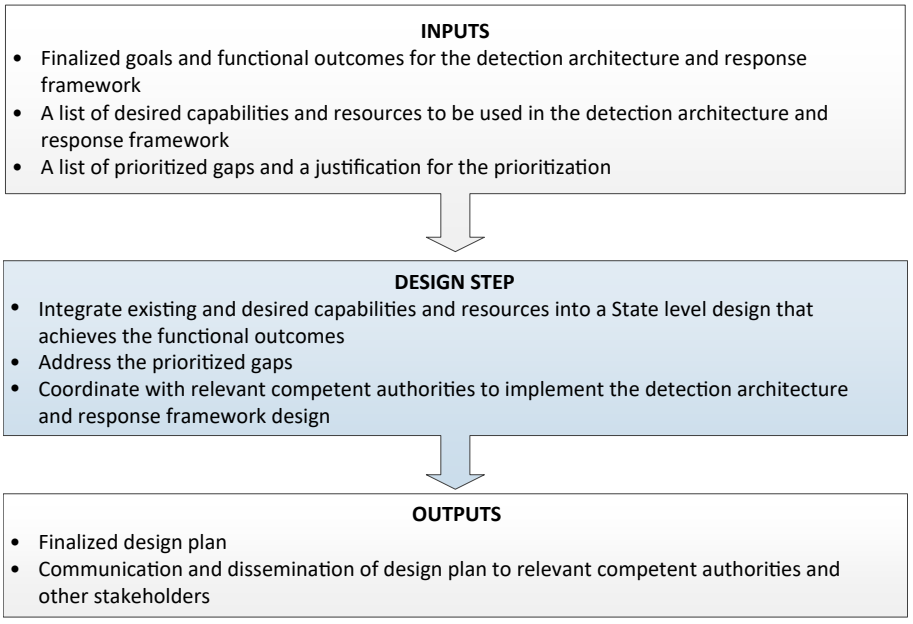


FIG. 5. Overview of the design step in the planning process.

5.2. The reviewed and approved design plan should be disseminated to the competent authorities and other stakeholders responsible for implementing portions of the plan. This design plan can be further refined by the competent authorities for application at the local or organizational level.

5.3. Such a structured approach to designing the detection architecture and response framework can provide the following benefits:

(a) Identification of alternatives for achieving functional outcomes and addressing prioritized gaps;
(b) Integration of systems and measures to develop a more effective and efficient set of capabilities;
(c) Optimization of resource allocation across the detection architecture and response framework;
(d) Definition and communication of the roles and responsibilities for the management, operation and sustainability of capabilities and resources;
(e) Establishment of mechanisms for continued coordination and communications to ensure integration and sustainability;
(f) Provision of an effective basis for implementation of the detection architecture and response framework.

5.4. In the following, detailed guidance is provided on how to conduct each of the four tasks of the design step:

(1) Developing the design of the detection architecture and response framework (see paras 5.5–5.31);
(2) Reviewing the design plan (see paras 5.32–5.48);
(3) Documenting the design plan (see paras 5.49–5.51);
(4) Communicating and disseminating the design plan (see para. 5.52).

DEVELOPING THE DESIGN OF THE DETECTION ARCHITECTURE AND RESPONSE FRAMEWORK

5.5. The design for the detection architecture and response framework should effectively integrate both existing and desired capabilities and resources to achieve the functional outcomes. Paragraphs 5.6–5.14 describe four broad approaches for addressing the prioritized gaps, and paras 5.15–5.31 highlight some considerations for integrating capabilities and resources into a design.

Approaches for addressing prioritized gaps

5.6. Four approaches for addressing the prioritized gaps include:

(a) Reallocating existing nuclear security capabilities and resources;
(b) Deploying capabilities and resources from other areas;
(c) Partnering with other States and international organizations;
(d) Investing in new capabilities and resources.

These approaches may be used in combination with one another to address a particular gap.

Reallocating existing nuclear security capabilities and resources

5.7. Nuclear security capabilities and resources can be reallocated from a geographical or organizational area where redundant capability exists to another to address a gap. Operations can also be modified and refined to address any gaps. Additional resources can be drawn from other nuclear security activities where overlaps or redundancies are identified.

5.8. The potential for reallocation of existing capabilities and resources is limited by the capabilities and resources that are already in place and thus might be insufficient to address major gaps. Moreover, some stakeholders may be reluctant to agree to the reallocation of capabilities and resources owing to the potential for creating new gaps in the areas from which resources are drawn. Notably, permanent reallocations may face substantial scrutiny.

Deploying capabilities and resources from other areas

5.9. Some capabilities and resources used for areas outside of nuclear security (e.g. border controls) can used to detect criminal or intentional acts involving material out of regulatory control and to respond to nuclear security events as well as to address their primary missions. Such an application of capabilities and resources could also lead to increased efficiency and effectiveness. However, this approach might result in short term inefficiencies as agencies and organizations adjust to their new roles and responsibilities.

5.10. Formal arrangements between agencies or organizations may be required to deploy capabilities and resources from other areas.

Partnering with other States and international organizations

5.11. Other States and international organizations can have complementary capabilities and resources that could be used to address identified gaps.[9] To be effective, capabilities and resources provided by other States and international organizations should explicitly address the accepting States' prioritized gaps. Although political differences might restrict the capability and resource sharing, even limited cooperation of this nature can provide alternatives for improved infrastructure effectiveness.

5.12. Such cooperation between States and international organizations can be achieved through formal or informal international agreements.

Investing in new capabilities and resources

5.13. Investing in new capabilities and resources typically involves acquiring these capabilities and resources from either public or private sources. States may also wish to invest in their own research and development if their circumstances are unique, highly sensitive or if existing solutions are inadequate.

5.14. Budget constraints typically represent the primary challenge to investing in new capabilities and resources. In some cases, decision makers might be reluctant to promote additional spending. However, they might be more receptive to such alternatives when it can be demonstrated that an identified gap cannot be addressed through the reallocation or sharing of existing capabilities and resources.

Considerations for integrating capabilities and resources into the design

5.15. Once the approaches for addressing identified and prioritized gaps have been considered, the identified capabilities and resources should be integrated into an overall design for the detection architecture and response framework. Paragraphs 5.16–5.31 provide guidance on specific considerations for integrating these capabilities and resources to develop a design (see also Ref. [5]). The application of the following considerations to the final design

[9] An example of an approach that uses cooperative arrangements with other States and international organizations is to have a formal agreement in place for an international or regional partnership to perform nuclear forensic analysis of samples of nuclear material and other radioactive material as needed.

can enhance robustness and effectiveness of the detection architecture and response framework.

Risk informed and tailored

5.16. The design should be risk informed. A risk informed approach to designing a detection architecture and response framework should include careful analysis of domestic and international threats, vulnerabilities and potential consequences to inform design trade-offs and to facilitate the efficient allocation of resources for maximum risk reduction [9]. As the design is developed, maintaining awareness of the relevant risks may aid in prioritizing design choices and tailoring the design to address the significant risks. Moreover, there is no universal solution for the detection architecture and response framework design. Each State should tailor its design according to its specific conditions and circumstances, including the unique features needed for its geographical and environmental conditions, the availability of resources and legal and regulatory constraints.

Multilayered and defence in depth

5.17. Early in design development, it is necessary to consider the breadth of systems and measures available and capitalize on their respective and complementary advantages, including through the application of defence in depth and the use of multiple layers of systems and measures.

5.18. The Nuclear Security Fundamentals [1] defines defence in depth as "The combination of successive layers of *nuclear security systems* and *nuclear security measures* for the protection of *targets* from *nuclear security threats*." Applied to the design step of the planning process for the detection architecture and response framework, a defence in depth approach uses overlapping but independent measures to ensure that there are multiple opportunities to achieve functional outcomes and that there is no common failure across multiple layers of systems and measures.

5.19. The use of multiple layers of systems and measures can ensure that a deficiency or failure of one layer can be mitigated by capabilities in another layer (see Ref. [15]).[10] In addition, adversary countermeasures which might be effective

[10] For example, in the absence of additional detection layers, an adversary capable of penetrating the border layer will have unfettered access to the interior layer and a variety of targets. Furthermore, if security is limited to border screening, it does not address the risk posed by domestic sources.

against one layer are not necessarily effective against other layers, providing increased security over the use of a single layer. International cooperation can add layers beyond the national boundaries.

5.20. A multilayered approach can also incorporate redundant components or capabilities into the detection architecture and response framework so that the failure of a single component, technology or capability does not compromise effectiveness, for example through the installation of backups or alternatives for critical system components. Critical components and their potential failure modes should be identified to ensure that redundant and diverse systems, consisting of either the same or different technologies or approaches, can preserve successful functioning of the detection architecture and response framework in the case that these technologies or approaches fail. Identifying these systems during the planning process can improve the integration of the redundant systems.

5.21. In addition to incorporating redundancy, the use of complementary approaches can increase the overall effectiveness of the detection architecture and response framework. For example, complementary approaches for detection may be achieved by using radiation detectors in parallel with observations of behavioural clues by trained personnel or identification of atypical events or circumstances.

Graded and balanced

5.22. The design of the detection architecture and response framework should use graded and balanced approaches, which means that it should address all significant potential risks but should not necessarily assign equal resources to each risk. A graded approach to design ensures that the capabilities and resources allocated are commensurate with the risk. A balanced approach to design ensures that appropriate levels of capabilities and resources are provided for all risks determined to be significant by the State. Graded and balanced approaches can be used when considering different pathways, different threat types and competing priorities.

5.23. As an example, a graded and balanced approach would deploy more resources and/or higher capability resources around critical points of interest such as high volume routes, high value targets or known trafficking routes (graded), yet provide some level of detection capability along all pathways (balanced).

Adaptable, able to evolve and unpredictable to the adversary

5.24. The detection architecture and response framework should be designed to adapt and evolve in response to factors such as: the emergence or discovery of new adversaries; changing goals, tactics and capabilities of existing adversaries; modifications to government policies and priorities; and the availability of resources and technologies. In addition, the detection architecture and response framework should include elements that cannot be predicted by an adversary.[11] However, a reasonable balance between predictability and unpredictability is needed because a heavy reliance on unpredictability may create vulnerabilities in communications as well as challenges with ease of use and sustainability of nuclear security systems and measures.

5.25. Methods to ensure that the detection architecture and response framework is adaptable and able to evolve and incorporate elements of unpredictability include:

(a) Modularity of systems and measures, which can enable an efficient response to changing conditions and circumstances, for example when the upgrading of system components over time could be accomplished without complete restructuring;
(b) Use of systems that are effective against a range of risks can provide a broader defence than those designed to specifically target an individual risk and enables the detection architecture and response framework to remain effective against changing and possibly unknown risks;
(c) Standardized equipment and data formats, which can offer benefits in communications, ease of use and sustainability, but may create vulnerabilities by introducing predictability;
(d) Incorporation of elements of unpredictability[12] into the detection architecture and response framework, which can further reduce the adversary's ability to circumvent nuclear security measures by decreasing the ability to analyse and understand the system, plan evasive measures and rehearse the adversary's plan.

[11] The unpredictability relates to the adversary's understanding of the operations, systems and measures that constitute the regime.

[12] Unpredictability can be introduced through measures such as continually adjusting patrol schedules and coverage areas or randomly selecting targets for enhanced screening.

Operationally flexible

5.26. Operating procedures should be sufficiently flexible to meet the needs of the detection architecture and response framework under varying conditions. In order to successfully integrate operational flexibility into the design of the detection architecture and response framework, knowledge of the existing, relevant missions is needed as well as identification of the kinds of scenarios and situations in which additional capabilities may be necessary on an occasional basis.

5.27. Operational flexibility can be increased through integrating nuclear security systems and measures with other safety and security systems and measures, as appropriate. For example, a State might plan for surge or search capabilities that can be used to respond to specific risks, could increase security for major public events or choose to secure strategic locations as necessary.[13] In parallel, it can be useful to identify opportunities for nuclear security capabilities to support other capabilities outside nuclear security by allowing them to serve multiple purposes as risks or priorities change.

Strategic communication

5.28. States may choose to manage the potential deterrent effect of nuclear security systems through several communication mechanisms, including observation, demonstration and public communication, and incorporate these mechanisms into the design.

5.29. Some security systems can be directly observed by an adversary. For example, radiation portal monitors can be observed at international border crossings or personal radiation detectors can be observed on the belts of law enforcement officers. In contrast, some security systems may not be directly observable or permanently deployed. In this case, the State can undertake observable training and exercises to demonstrate detection and response capabilities.

[13] A surge capability is a capability that is not usually deployed for day to day nuclear security operations. For example, a laboratory can be designated for nuclear forensic analysis if needed while having a different day to day function outside nuclear security or specialized law enforcement teams (e.g. special weapons and tactics) may be deployed in response to a confirmed information alert.

5.30. States might also choose to release information about detection and response capabilities through public communication mechanisms, such as the media.

International and regional cooperation

5.31. International cooperation may provide access to more information and technical expertise than is available to a State working individually. Methods of cooperating with international organizations and other States that might be included in the design include the following:

(a) Designating a point of contact and establishing communications protocols to facilitate communication and cooperation with regional partners and international organizations;
(b) Sharing best practices, lessons learned and technical expertise;
(c) Notifying international organizations and other potentially affected States, as appropriate, of nuclear security events or seizures of nuclear material and other radioactive material, including participation in international databases, as appropriate;
(d) Providing or requesting assistance for designing, implementing, and evaluating the detection architecture and response framework. Topics for assistance may include joint training and exercises, exchange of technical specifications and benchmarks, technical expert support, risk information, support for major public events and joint research and development.

REVIEWING THE DESIGN PLAN

5.32. After the detection architecture and response framework design is developed, it should be reviewed to verify that it will address the functional outcomes and the prioritized gaps. A clear set of criteria for this review should be developed. These criteria should reflect both the security design considerations listed above and how well the design enables the functional outcomes of the nuclear security infrastructure to be achieved.

5.33. Criteria for reviewing the design might include the following:

(a) Resources needed for the design (see paras 5.34–5.37);
(b) The effectiveness of the design in supporting the detection of criminal or unintentional acts involving material out of regulatory control and the response to nuclear security events (see para. 5.38);
(c) The feasibility of the design (see para. 5.39);

(d) Legal and regulatory implications of the design (see para. 5.40);
(e) Local and national effects of the design (see paras 5.41–5.46);
(f) Stakeholder acceptance of the design (see para. 5.47);
(g) Long term sustainability of the design (see para. 5.48).

Resources

5.34. The resources needed for various components of the design — including funding, people and time — are an important consideration for assessing the viability of the design. Identifying the available resources can provide critical insight into detection architecture and response framework design constraints. Important and specific criteria for reviewing the design with regard to resources are explored in paras 5.35–5.37.

5.35. An important criterion is the life cycle cost of the design, including the cost of development, implementation and operation of the detection architecture and response framework, as well as maintenance, replacement and disposition of the components. Organizational resources should also be considered, including those needed for components of the infrastructure design to be designated to competent authorities for implementation.

5.36. The human resources for the design — including personnel staffing and training — is another important criterion for consideration, as are budget constraints, both long and short term, the time needed to deploy or implement alternative solutions and the technology readiness level of the components contained in the design.

5.37. The ease with which a design can be implemented should also be considered. For example, designs that include commercially available equipment can be easily implemented, resulting in the need for fewer resources.

Effectiveness

5.38. The effectiveness of the design in supporting the prevention of, detection of and response to nuclear security events involving material out of regulatory control should be considered. The ability of the design to support the prevention of, detection of and response to such events can be understood in both an analytical sense (e.g. increasing the probabilities of encounter, detection and identification of material out of regulatory control) as well as an operational sense (e.g. rate of false positives). The criteria for effectiveness may be different for different risks and environments.

Feasibility

5.39. Operational suitability and efficiency is important to ensure the feasibility of implementation of the design. Feasibility considerations for particular components of the design may include, for example, necessary staffing level, screening or scanning time and wait time.

Legal and regulatory implications

5.40. The legal and regulatory framework of the State might constrain the ability to implement some components of the design and should be considered. Such constraints can include privacy laws, radiation exposure limits and transport infrastructure regulations.

Local and national effects

5.41. The local and national effects of the design should be considered and could include economic, safety, environmental and societal effects as well as effects on other national programmes, such as border controls.

5.42. Efficient trade and commerce may need to be balanced with national security when reviewing the design. For example, for detection equipment deployed at borders, high innocent and false alarm rates for detectors can impede the flow of commerce and trade. Reducing this effect might be necessary to minimize the negative impact to the economy.

5.43. The safety of both front line officers and the general public should be considered when reviewing the design. For example, a design that does not have adequate temporary storage for seized nuclear material or other radioactive material could create a safety risk.

5.44. Environmental effects of the design should also be considered. For example, the installation of checkpoints or equipment and the materials used in the components could have environmental impacts that would need to be mitigated. The use of existing facilities and infrastructure can help to minimize these impacts in some cases.

5.45. The impact on the general public may also need to be considered when reviewing the design. The general public could provide support or opposition to nuclear security efforts. Concerns about public perception might also need to be

balanced between increasing public knowledge while preserving the security of sensitive activities.

5.46. Finally, the detection architecture and response framework can both contribute to other missions undertaken by the State and have an effect on their resources. For example, when capabilities or resources are used for multiple purposes, personnel need to undergo additional training, carry additional equipment or execute supplemental operational tasks that may affect their other ongoing activities.

Stakeholder acceptance

5.47. Stakeholder commitment to the design is essential for effective implementation. However, their acceptance can be difficult to achieve due to competing priorities among stakeholders. Therefore, it is important to integrate relevant stakeholders into the planning process to build understanding of the varying perspectives and priorities with which they might approach the design.

Long term sustainability

5.48. The long term functionality and viability of the design should be considered. Sustainability considerations for the design include long term staffing and training needs, facility maintenance, suitability of the design to changes in threat and risk and the potential for long term support from the public and from decision makers (see Appendix III for additional information on establishing sustainability mechanisms).

DOCUMENTING THE DESIGN PLAN

5.49. After review, the design should be documented and formalized into a design plan. The decisions that were made as well as the rationale for them should be accurately documented and codified through established channels. The documentation might contain sensitive information and should be protected according to national procedures.

5.50. The design plan should describe the competent authorities involved in developing and approving the design plan and the basis for the detection architecture and response framework design. This basis includes: international and national legislation and regulations; relevant administrative arrangements and policies; nuclear security infrastructure for material out of regulatory

control goals and scope, where available; threats and risk assessment; competent authorities and other stakeholders and their role in nuclear security; and key decision makers.

5.51. The plan should also include a summary of the key findings and decisions made throughout the planning process, including:

(a) Nuclear security infrastructure goals and functional outcomes;
(b) Performance indicators for future evaluation;
(c) Assessment of capabilities and resources;
(d) A list of existing capabilities and resources to be used in the infrastructure;
(e) A prioritized list of gaps and a justification for the prioritization;
(f) A description of how existing and desired capabilities and resource are integrated to achieve the functional outcomes;
(g) A description of capabilities and resources that will need to be acquired or reallocated to address prioritized gaps;
(h) A recommended timeline for implementing the design plan (start time and duration);
(i) A mapping of the elements of the design to competent authorities who will implement them.

COMMUNICATING AND DISSEMINATING THE DESIGN PLAN

5.52. The coordinating body or mechanism should ensure the design plan is appropriately communicated and disseminated to the competent authorities and other stakeholders, so that they have a clear understanding of their role in implementation of the design plan. In addition to domestic communication efforts, portions of the design plan may include capabilities and resources from international or regional partners. Implementation of these components may involve ongoing international communication, which should be conducted as appropriate. The communication strategies described in Appendix I may assist in these efforts.

Appendix I

DEVELOPING COMMUNICATION STRATEGIES

I.1. To ensure appropriate communication among organizations, the planning process should include development of communications strategies. A national effort should promote consensus on the importance of nuclear security and a shared vision of how the infrastructure should be implemented. Simultaneously, individual organizations will need to develop internal communications strategies to build awareness and support for nuclear security among personnel.

I.2. It may be helpful to categorize organizations and to develop different communication strategies for each group. The following considerations should be taken into account when developing a plan for communicating with a particular organization:

(a) The level of interest in, and existing knowledge about, the detection architecture and response framework;
(b) Expectations for participation in, and communication about, the detection architecture and response framework;
(c) The sensitivity of the information to be shared as well as the information access levels granted to personnel;
(d) Whether the communication will be bidirectional or unidirectional (i.e. will the implementing organization participate in an active dialogue about the infrastructure or will it be solely the recipient of infrastructure related information);
(e) The implementing organization's role (e.g. legal/regulatory, scientific/technical, law enforcement and operational);
(f) The ability to engage in communications, which may be limited by that organization's resources.

I.3. Having identified these factors for each organization, a communication strategy can then be developed to address the timing and frequency of communications with each group, the type of information to be communicated and the method of communication.

I.4. When communicating among organizations, it is important to frame the communication in local and accessible terms. Defining tangible and manageable tasks for organizations enhances their ability to quickly contribute to the mission. Identifying some overlaps with other mission areas and integrating nuclear

security awareness activities with those of other missions can help to foster engagement. This may also serve to inform implementers of the role they have in the success of the infrastructure and to reassure them that taking on nuclear security context responsibilities will consist of an extension of their existing responsibilities and not an entirely new set of responsibilities.

I.5. Communication strategies should also provide opportunities for interaction between participants and establish methods for updating and sustaining communication channels. Communication strategies should include building a shared understanding of organizational responsibilities and encouraging mission acceptance, as described in paras I.6–I.10.

BUILDING A SHARED UNDERSTANDING OF ORGANIZATIONAL RESPONSIBILITIES

I.6. To ensure all participants share a common understanding, the roles and responsibilities associated with implementing the detection architecture and response framework may be formalized, either through laws or other policies or by inter-organization agreements, such as memoranda of understanding. Codifying formal written documentation of cooperative intent can preclude disagreements or confusion about areas of responsibility, as well as encourage inter-organizational accountability.

I.7. Communication among organizations further helps to ensure that the detection architecture and response framework is planned and implemented in a manner that recognizes each organization's constraints, goals, and competing needs and missions. It also provides an opportunity to determine whether each organization perceives that it has the necessary authority to participate. It is particularly important to engage in active dialogue with any organizations that currently have control over capabilities and resources that will be reallocated during the implementation of the design plan. The reallocation should be conducted in cooperation with all impacted implementing organizations to ensure awareness of the purpose of the reallocation and to ensure any impacts on other mission areas are appropriately addressed.

ENCOURAGING MISSION ACCEPTANCE

I.8. Consistent, well planned communication with organizations will contribute substantially to mission acceptance. Communicating the overall strategy

of the infrastructure and the critical role that each organization plays in its success helps to foster support, both at the individual and organizational levels. Similarly, creating awareness of the risks and how the detection architecture and response framework can help to reduce associated risks is likely to encourage active participation.

I.9. At a practical level, organizations and individuals may be more likely to actively support and lead nuclear security efforts if they feel that the detection architecture and response framework has been designed with their needs in mind. This can be achieved by focusing on specific, relevant mission tasks, integrating nuclear security efforts with other missions and minimizing the operational complexity associated with nuclear security tasks. Clearly documenting processes and procedures can help to avoid frustration and to minimize the additional burdens imposed by nuclear security tasks. Organizations, as well as personnel, should be provided with the resources needed to fulfil their responsibilities within the infrastructure.

I.10. Another effective way of building mission acceptance is to identify strong senior leaders within an organization who can champion the nuclear security effort within the organization. Such efforts can be promoted by providing these leaders with enhanced training to help them to articulate the significance of the nuclear security context.

Appendix II

COORDINATION MECHANISMS

II.1. Effective integration of design components is essential when building a detection architecture and response framework that is more effective than the sum of the individual capabilities and resources. Notably, communication and coordination are needed to develop mechanisms that facilitate long term integration. This appendix identifies several mechanisms that may be used by organizations, as appropriate.

SHARED DATA AND INFORMATION MECHANISMS

II.2. Multiple organizations might use similar sets of information, and information collected by one organization might reveal the activities of another. To the extent feasible, and with appropriate security protections, sharing this information can improve the overall effectiveness of the detection architecture and response framework. Depending on the type of information to be shared, access protocols for shared databases or routinely scheduled information exchanges can be useful. This can be applicable both to organizations within a State and to work undertaken with international partners and organizations.

COMMAND STRUCTURE

II.3. A clear command structure, combined with appropriate concepts of operations, plays a critical role in integrating design components. Individual pieces of information from different elements of the detection architecture and response framework can be passed throughout the command structure, where they can be shared within and across organizations to provide cohesive situational awareness. The command structure also provides a means for operations to be adjusted in response to new information.

IDENTIFYING OPPORTUNITIES FOR MULTIMISSION SUPPORT

II.4. Just as the detection architecture and response framework can use capabilities and resources that have been implemented for other missions, some elements of the infrastructure can also provide support for other missions.

For instance, radiography equipment located at a border crossing can be used to scan cargo for nuclear material and other radioactive material, and it can also support customs and immigration enforcement.

TRAINING AND EXERCISES

II.5. Training and exercises conducted at different organizations can transfer knowledge and expertise throughout the detection architecture and response framework. Cooperative training and exercises can also facilitate the development of collaborative protocols and procedures that can effectively utilize the areas of expertise of each organization for a broad array of scenarios and activities. Conducting shared training and exercise activities encourages interaction, communication and the formation of contact networks throughout the infrastructure that can be used for future coordination and development.

WORKSHOPS

II.6. Workshops involving multiple organizations facilitate communication of information and cooperative development of capabilities. Workshops can also encourage the development of professional networks and provide participants with the opportunity to benefit from the knowledge and experience of personnel from other organizations. Workshops also provide an opportunity for multiple organizations to arrive at agreements for cooperative operations.

FOCAL POINTS

II.7. Focal points such as regional centres of excellence, operations and analysis centres and technical expert support can help to identify areas for productive collaboration. These focal points can provide support to operational personnel, giving them a unique, infrastructure wide perspective and creating an environment to support the sharing of critical information across organizations.

ROTATIONS

II.8. Personnel rotations among multiple organizations can help to establish professional networks, allow organizations to learn about the ongoing activities of other organizations, and aid in identifying prospective areas of cooperation.

Cross-organizational information sharing can enable organizations to improve their own capabilities as well as improve their collective ability across multiple organizations to execute the goals of the infrastructure.

Appendix III

ESTABLISHING SUSTAINABILITY MECHANISMS

III.1. Sustainability is an essential part of planning and organization, as it helps to ensure the long term effectiveness of the detection architecture and response [16]. Sustainability should be addressed across the detection architecture and response framework and may include the considerations discussed in this appendix.

OPERATIONS AND MANAGEMENT

III.2. Implementing organizations are responsible for the people, processes and equipment associated with the detection architecture and response framework. The planning process should consider the long term availability of financial resources for ongoing operational expenses and procurement needs within these organizations, including budgetary needs for personnel, training and exercises, equipment life cycle obligations and performance evaluations.

HUMAN RESOURCES

III.3. Staffing needs and workloads should be reconciled with the added duties and tasks associated with operating, maintaining and managing the detection architecture and response framework. The impact of personnel turnover should be correlated with institutionalized training programmes and documentation of procedures. Ongoing refresher training and exercises ensure continual operational readiness and adaptation for emerging areas of concern.

MAINTENANCE AND LOGISTICS

III.4. A capacity for both preventive and corrective maintenance is needed to ensure the continued effectiveness of technical equipment, which relies on processes to track equipment performance, a properly maintained spare parts inventory, and competent and appropriately trained personnel. A sustainable detection architecture and response framework must also account for equipment life cycle obligations, including upgrading or replacing equipment as it fails or becomes obsolete. Conducting such efforts on a rotating basis may help to minimize the financial and operational impacts. Maintenance and calibration

of equipment typically involves the use, transport and storage of radioactive materials, which should be addressed during the planning process.

REFERENCES

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

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

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

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

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

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

[7] FOOD AND AGRICULTURE ORGANIZATION OF THE UNITED NATIONS, INTERNATIONAL ATOMIC ENERGY AGENCY, INTERNATIONAL LABOUR OFFICE, 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).

[8] FOOD AND AGRICULTURE ORGANIZATION OF THE UNITED NATIONS, INTERNATIONAL ATOMIC ENERGY AGENCY, INTERNATIONAL LABOUR OFFICE, PAN AMERICAN HEALTH ORGANIZATION, UNITED NATIONS OFFICE FOR THE COORDINATION OF HUMANITARIAN AFFAIRS, WORLD HEALTH ORGANIZATION, Arrangements for Preparedness for a Nuclear or Radiological Emergency, IAEA Safety Standards Series No. GS-G-2.1, IAEA, Vienna (2007).
[9] INTERNATIONAL ATOMIC ENERGY AGENCY, INTERNATIONAL CRIMINAL POLICE ORGANIZATION–INTERPOL, Risk Informed Approach for Nuclear Security Measures for Nuclear and Other Radioactive Material out of Regulatory Control, IAEA Nuclear Security Series No. 24-G, IAEA, Vienna (2015).
[10] INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Culture, IAEA Nuclear Security Series No. 7, IAEA, Vienna (2008).
[11] INTERNATIONAL ATOMIC ENERGY AGENCY, The International Legal Framework for Nuclear Security, IAEA International Law Series No. 4, IAEA, Vienna (2011).
[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, INTERNATIONAL CRIMINAL POLICE ORGANIZATION–INTERPOL, UNITED NATIONS INTERREGIONAL CRIME AND JUSTICE RESEARCH INSTITUTE, Radiological Crime Scene Management, IAEA Nuclear Security Series No. 22-G, IAEA, Vienna (2014).
[14] INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Forensics in Support of Investigations, IAEA Nuclear Security Series No. 2-G (Rev. 1), IAEA, Vienna (2015).
[15] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety of Nuclear Power Plant Design, IAEA Safety Standards Series No. SSR-2/1 (Rev. 1), IAEA, Vienna (2016).
[16] INTERNATIONAL ATOMIC ENERGY AGENCY, Sustaining a Nuclear Security Regime, IAEA Nuclear Security Series No. 30-G, IAEA, Vienna (2018).

Annex I

EXAMPLE NUCLEAR SECURITY DETECTION ARCHITECTURE AND RESPONSE FRAMEWORK ROLES AND RESPONSIBILITIES

I–1. Table I–1 provides an example of key roles and responsibilities for the nuclear security detection architecture for material out of regulatory control and the framework for managing the response to nuclear security events, as well as organizations that could fill those roles. This list is not exhaustive nor does it represent a recommendation for how a State should structure its nuclear security infrastructure.

TABLE I–1. NUCLEAR SECURITY DETECTION ARCHITECTURE AND RESPONSE FRAMEWORK ROLES AND RESPONSIBILITIES

Role	Description	Example organizations
High level management of the nuclear security detection architecture and response framework	Ensures the effectiveness and continual improvement of the infrastructure and is accountable for the execution and success of the infrastructure	Coordinating body or mechanism
Operation of detection and response systems	Operates nuclear detection and response equipment and ensures its proper operation at their assigned locations	Customs Border protection Law enforcement Nuclear regulatory authority Health authority Local government units Civil defence
Enforcement of laws and regulations	Enforces the established laws and regulations on the possession, use and transport of nuclear material and other radioactive material	Police Security services Nuclear regulatory authority
Expert support of detection architecture and response framework activities	Provides relevant expertise on nuclear material and other radioactive material, implementation, and threat/risk information and provides reach back resources	Subject matter experts Academic institutions Science and technology agencies Nuclear regulatory authority Technical support organizations Industry
Information collection and analysis	Collects and analyses relevant information about the detection architecture and response framework environment and threat/risk information	Intelligence community Law enforcement Conveyance and port operators Medical community
Development and production of detection architecture and response framework related equipment	Researches and develops technologies for radiation detection and response, and other necessary capabilities	Equipment vendors Academic institutions Government science and technology agencies

TABLE I–1. NUCLEAR SECURITY DETECTION ARCHITECTURE AND RESPONSE FRAMEWORK ROLES AND RESPONSIBILITIES (cont.)

Role	Description	Example organizations
Operation of transport and commercial facilities	Coordinates with detection architecture and response framework elements to facilitate operations	Port operators Transport service providers Nuclear regulatory authority First responders
International cooperation	Coordinates and supports international collaborations via information sharing, technical collaboration, and operational cooperation	Relevant implementing organizations from other States Diplomatic agencies International organizations
Public information	Arranges for informing the news media and public, as appropriate, in a coordinated, understandable and consistent manner	Coordinating body Media and other means of disseminating information
Acquisition of equipment	Manages selection and procurement of equipment	Customs Border security Law enforcement Port operators
Investigations of nuclear security events	Collection, handling, and analysis of evidence from the crime scene	Law enforcement Traditional forensic laboratories Nuclear forensic laboratories Nuclear regulatory authority
Training, exercises and evaluation	Develops and conducts training, exercises and evaluation for the nuclear security detection architecture and response framework	Governmental training institutions Non-governmental training providers International organizations and institutions

Annex II

EXAMPLE FUNCTIONAL OUTCOMES

II–1. Figure II–1 demonstrates how different perspectives could be used to develop functional outcomes. While it shows considerations for each perspective individually, in practice a combination of perspectives are typically used to develop a comprehensive and robust set of functional outcomes.

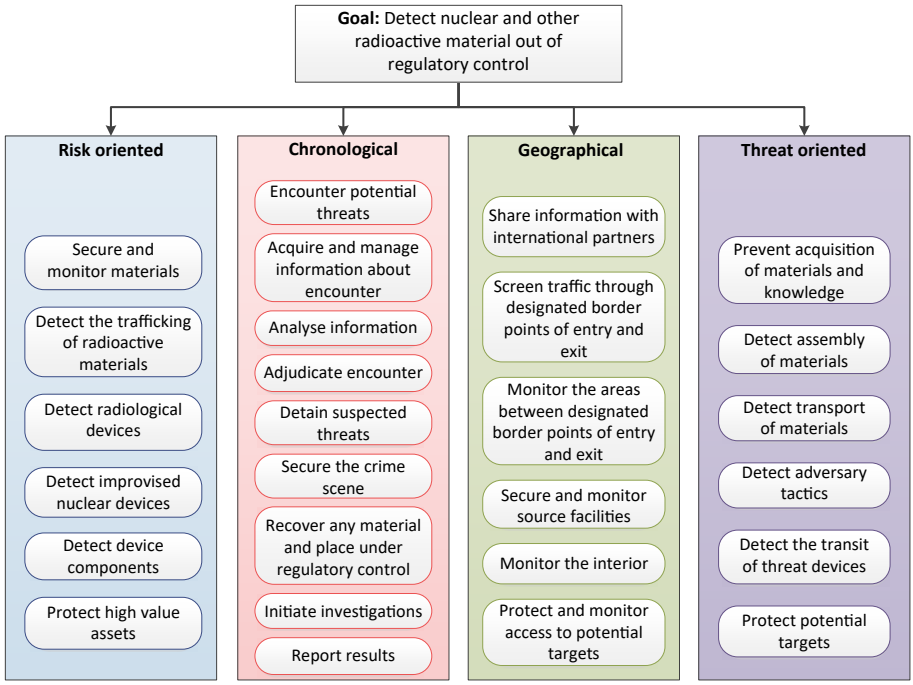


FIG. II–1. Example considerations derived from risk oriented, chronological, geographical and threat oriented perspectives.

II–2. As shown in Fig. II–2, a set of functional outcomes can be developed to provide more specific, measurable and actionable descriptions of how the State can achieve a strategic goal. Each functional outcome can be developed using one or more perspectives. For example, the first functional outcome listed (FO 1), Establish information sharing arrangements with other regional regulatory bodies with regard to lost, missing or stolen material, takes into account the geographical (exterior layer), chronological (acquire and manage information) and threat oriented perspective (detect the possible acquisition of materials). Developing and reviewing the set of functional outcomes using these four perspectives will lead to a more comprehensive and robust set.

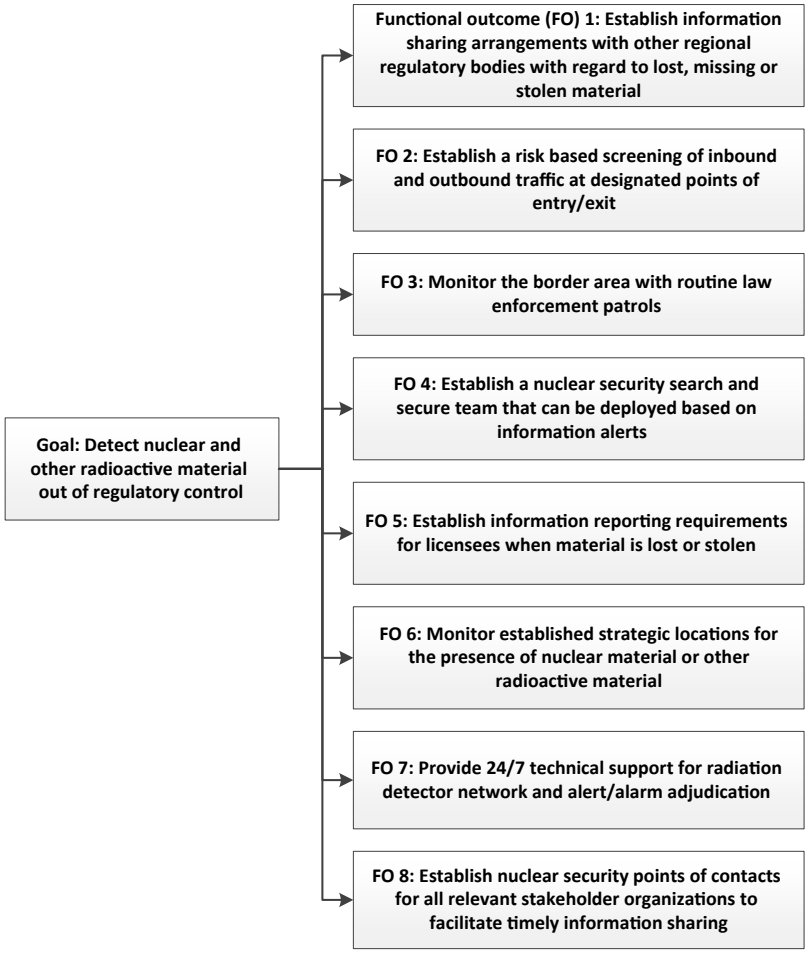


FIG. II–2. An example set of functional outcomes that incorporate multiple perspectives.

Annex III

PLANNING AND ORGANIZING TEMPLATE

PLANNING BASIS

III–1. This section outlines information that provides a basis for the planning process. This information will be applied throughout the planning and organization process to ensure the nuclear security detection for material out of regulatory control and framework for managing response to nuclear security events addresses the relevant context and the State's goals.

NATIONAL SECURITY CONTEXT
List relevant national legislation, regulations and policies on nuclear security and national security, for example national security legislation, anti-terrorism laws and customs regulations (see paras 2.23 and 2.24).
List relevant national strategy documents, for example emergency/civil defence response plans (see para. 2.25).
List relevant risk assessments (see para. 2.26).

List relevant international agreements and instruments, as well as guidance, standards and other documents to which your State is party (see para. 2.27).

List risk informed nuclear security detection architecture and response framework goals and where they are documented, where applicable.	
Goal	Where documented or originated (e.g. strategy/policy documents)

KEY ROLES WITHIN THE DETECTION ARCHITECTURE AND RESPONSE FRAMEWORK FOR MATERIAL OUT OF REGULATORY CONTROL

List key decision makers with respect to developing the detection architecture and response framework (see paras 2.28–2.33).

List relevant competent authorities and roles and responsibilities, as authorized by legal provisions (see paras 2.28–2.33 and Annex I).			
Authority	Preventive role	Detection role	Response role

Describe the mechanisms of coordination among competent authorities with respect to developing the detection architecture and response framework (see Appendices I and II).

STEP 1: DIRECTION

FUNCTIONAL OUTCOMES		
Based on the national security context, list the functional outcomes. Subsequently, review the functional outcomes.		
Goal	Functional outcome (see paras 3.1–3.15)	Review criteria (see paras 3.16–3.23)
		○G ○A ○S ○C ○T ○U
		○G ○A ○S ○C ○T ○U
		○G ○A ○S ○C ○T ○U
		○G ○A ○S ○C ○T ○U

G — goal oriented; A — assessable; S — sufficient; C — comprehensive; T — time bound; U — unique.

STEP 2: ASSESSMENT

CAPABILITIES AND RESOURCES	
Identify necessary capabilities and resources to support each functional outcome.	
Functional outcome	
Capabilities and resources needed to meet functional outcome (see paras 4.4 and 4.5)	
Existing capabilities and resources (see paras 4.6–4.9)	
Gaps between necessary and existing capabilities and resources (see paras 4.10 and 4.11)	
Priority level of gap (H, M, L) and justification (see paras 4.12–4.14)	
SUMMARY OF GAPS BY PRIORITY	
High priority gaps	
Medium priority gaps	
Low priority gaps	

(H)igh — address immediately; (M)edium — address when possible; (L)ow — does not need to be addressed.

STEP 3: DESIGN

DETECTION ARCHITECTURE AND RESPONSE FRAMEWORK DESIGN								
Identify approaches to address the prioritized gaps identified in Step 2 (see paras 5.6–5.14). Assess the alternatives and select for implementation (see paras 5.32–5.51).								
Gap								
Describe alternative and indicate approach	[H/M/L]							[Yes/No]
• Reallocate existing • Deploy from other mission areas • Partner internationally • Invest in new capabilities	Effectiveness	Feasibility	Legal and regulatory implications	Resources	Impact	Stakeholder acceptance	Sustainability	Implement?

(H)igh — best case scenario; (M)edium — some challenges, limitations or negative implications exist; (L)ow — severe challenges, limitations or negative implications exist.

DESIGN PLAN
Finalize and document design plan (see paras 5.52 and 5.53).
List competent authorities involved in developing and approving the design plan.
Basis for detection architecture and framework design.
Direction.
Assessment of capabilities and resources.
Design.

IAEA
International Atomic Energy Agency

No. 25

ORDERING LOCALLY

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

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

CANADA

Renouf Publishing Co. Ltd
22-1010 Polytek Street, Ottawa, ON K1J 9J1, CANADA
Telephone: +1 613 745 2665 • Fax: +1 643 745 7660
Email: order@renoufbooks.com • Web site: www.renoufbooks.com

Bernan / Rowman & Littlefield
15200 NBN Way, Blue Ridge Summit, PA 17214, USA
Tel: +1 800 462 6420 • Fax: +1 800 338 4550
Email: orders@rowman.com Web site: www.rowman.com/bernan

CZECH REPUBLIC

Suweco CZ, s.r.o.
Sestupná 153/11, 162 00 Prague 6, CZECH REPUBLIC
Telephone: +420 242 459 205 • Fax: +420 284 821 646
Email: nakup@suweco.cz • Web site: www.suweco.cz

FRANCE

Form-Edit
5 rue Janssen, PO Box 25, 75921 Paris CEDEX, FRANCE
Telephone: +33 1 42 01 49 49 • Fax: +33 1 42 01 90 90
Email: formedit@formedit.fr • Web site: www.form-edit.com

GERMANY

Goethe Buchhandlung Teubig GmbH
Schweitzer Fachinformationen
Willstätterstrasse 15, 40549 Düsseldorf, GERMANY
Telephone: +49 (0) 211 49 874 015 • Fax: +49 (0) 211 49 874 28
Email: kundenbetreuung.goethe@schweitzer-online.de • Web site: www.goethebuch.de

INDIA

Allied Publishers
1st Floor, Dubash House, 15, J.N. Heredi Marg, Ballard Estate, Mumbai 400001, INDIA
Telephone: +91 22 4212 6930/31/69 • Fax: +91 22 2261 7928
Email: alliedpl@vsnl.com • Web site: www.alliedpublishers.com

Bookwell
3/79 Nirankari, Delhi 110009, INDIA
Telephone: +91 11 2760 1283/4536
Email: bkwell@nde.vsnl.net.in • Web site: www.bookwellindia.com

ITALY

Libreria Scientifica "AEIOU"
Via Vincenzo Maria Coronelli 6, 20146 Milan, ITALY
Telephone: +39 02 48 95 45 52 • Fax: +39 02 48 95 45 48
Email: info@libreriaaeiou.eu • Web site: www.libreriaaeiou.eu

JAPAN

Maruzen-Yushodo Co., Ltd
10-10 Yotsuyasakamachi, Shinjuku-ku, Tokyo 160-0002, JAPAN
Telephone: +81 3 4335 9312 • Fax: +81 3 4335 9364
Email: bookimport@maruzen.co.jp • Web site: www.maruzen.co.jp

RUSSIAN FEDERATION

Scientific and Engineering Centre for Nuclear and Radiation Safety
107140, Moscow, Malaya Krasnoselskaya st. 2/8, bld. 5, RUSSIAN FEDERATION
Telephone: +7 499 264 00 03 • Fax: +7 499 264 28 59
Email: secnrs@secnrs.ru • Web site: www.secnrs.ru

UNITED STATES OF AMERICA

Bernan / Rowman & Littlefield
15200 NBN Way, Blue Ridge Summit, PA 17214, USA
Tel: +1 800 462 6420 • Fax: +1 800 338 4550
Email: orders@rowman.com • Web site: www.rowman.com/bernan

Renouf Publishing Co. Ltd
812 Proctor Avenue, Ogdensburg, NY 13669-2205, USA
Telephone: +1 888 551 7470 • Fax: +1 888 551 7471
Email: orders@renoufbooks.com • Web site: www.renoufbooks.com

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

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

19-00011

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

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

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

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

This publication provides guidance to States and their competent authorities on planning and organizing nuclear security systems and measures for the detection of criminal or intentional unauthorized acts involving material out of regulatory control and for the response to nuclear security events. The guidance includes processes for the identification of existing nuclear security systems and measures, the determination of resource and capability gaps, and the design of new systems and measures to address identified gaps.

INTERNATIONAL ATOMIC ENERGY AGENCY
VIENNA
ISBN 978–92–0–100119–1
ISSN 1816–9317