PLANNING AND ORGANIZATION OF NUCLEAR SECURITY SYSTEMS AND MEASURES FOR NUCLEAR AND OTHER RADIOACTIVE MATERIALS OUT OF REGULATORY CONTROL

DRAFT TECHNICAL GUIDANCE

INTERNATIONAL ATOMIC ENERGY AGENCY

VIENNA, 20XX
FOREWORD

[Standard NSS Foreword to be added]
REFERENCES ......................................................................................................................... 37

ANNEX I. EXAMPLE NUCLEAR SECURITY INFRASTRUCTURE FOR MORC ROLES AND RESPONSIBILITIES ................................................................. 41

ANNEX II. EXAMPLE FUNCTIONAL OUTCOMES ................................................................. 43

ANNEX III. PLANNING AND ORGANIZATION TEMPLATE ............................................. 45
1. INTRODUCTION

1.1. BACKGROUND

The overall objective of a State’s nuclear security regime is to protect persons, property, society, and the environment from the harmful consequences of a nuclear security event [1]. Therefore, States should plan, implement, and evaluate an effective and appropriate nuclear security regime to prevent, detect and respond to such nuclear security events. A comprehensive national nuclear security regime should include effective nuclear security measures for nuclear and other radioactive materials that are either under or out of regulatory control.

This objective is achieved by the implementation of all Nuclear Security Recommendations-level publications:

— Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5) [2]
— Nuclear Security Recommendations on Nuclear and Other Radioactive Material out of Regulatory Control [4]

A nuclear security event involving nuclear or other radioactive material out of regulatory control has the potential for catastrophic health, economic, environmental, and societal consequences. Therefore, States should consider developing a multi-layered, defence-in-depth approach to design and implementation of nuclear security systems and measures. This includes measures to prevent materials from leaving regulatory control through loss or theft, detect materials that have become out of regulatory control, and respond to any potential nuclear security event.

The Implementing Guide Nuclear Security Systems and Measures for Detection of Nuclear and other Radioactive Material out of Regulatory Control describes the necessary features of an effective nuclear security detection capability [5] and the Implementing Guide Development of a National Framework for Managing the Response to Nuclear Security Events describes those for an effective response framework [6]. This Technical Guidance document is intended to describe in more detail a process for planning and organization of...
those parts of a State’s nuclear security regime that relate to nuclear and other radioactive material out of regulatory control (MORC).

1.2. OBJECTIVE

The objective of this publication is to provide guidance for States and relevant competent authorities on planning and organization for the identification and design of systems and measures for the detection of MORC and response to criminal or intentional unauthorized acts involving MORC.

1.3. SCOPE

This publication describes a planning process to design an effective framework and set of nuclear security systems and measures for the detection of and response to criminal and intentional unauthorized acts involving MORC. In this document, the term ‘nuclear security infrastructure for MORC’ is used to describe those parts of a nuclear security regime at the State level that are applicable to nuclear and other radioactive material out of regulatory control [4]. The elements of the nuclear security regime that relate to MORC comprise:

— The relevant legislation, regulations and administrative arrangements that govern nuclear security for MORC;
— The competent authorities and other organizations with responsibilities relating to MORC; and
— Nuclear security systems and measures for the prevention of, detection of, and response to nuclear security events involving MORC.

Developing and sustaining a nuclear security regime is an iterative process that involves planning, implementation, and evaluation phases (see Figure 1). This iterative process promotes continuous improvement and evolution in the nuclear security infrastructure for MORC, which enables it to adapt over time. This document covers a planning process for designing a State nuclear security infrastructure for MORC and it is not intended to provide guidance on the implementation and evaluation. Further, this document is not intended to provide guidance on planning and organization of measures and arrangements intended for preparedness and response to nuclear or radiological emergency [7], [8], [9].

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

Following this introduction, Section 2 provides an overview of an integrated planning process that may be used to design a State’s nuclear security infrastructure for MORC. This overview includes a description of the benefits of using such a process, underlying principles for planning, and the basis and steps of the planning process. The subsequent Sections of this document describe guidance for each step in the planning process. The appendices provide supplemental guidance for communication strategies as well as coordination and sustainability mechanisms. The Annexes provide examples of nuclear security planning roles and responsibilities as well as functional outcomes. In addition, Annex III provides a template that may be used by planners in following the planning and organization process.

2. OVERVIEW OF AN INTEGRATED PLANNING PROCESS

A structured planning process enables a State to establish or enhance its national nuclear security infrastructure for MORC in an integrated manner. The process can strengthen a State’s capability to prevent, detect and respond to criminal or intentional unauthorized acts with nuclear security implications involving MORC, through:

— Avoidance of systemic gaps;
— Enhanced communication and coordination at all levels;
— Assurance of clarity and transparency to all relevant competent authorities and other stakeholders;
— Integration with other nuclear security and national security context areas;
— Effective use of resources and avoidance of duplication of efforts; and
— Commitment to sustainability and continuous improvement including increased flexibility and the ability to adapt to changing needs, priorities, and availability of resources.

2.1. A GENERAL PLANNING PROCESS

The basis for developing a State’s nuclear security infrastructure for MORC is appropriate legislation, regulation, and administrative arrangements that establish roles and responsibilities, authorities, and the national mandate to detect and respond to criminal and intentional unauthorized acts involving MORC.
A general planning process consists of three steps. These steps are not isolated from one another, but instead inform each other and work together to achieve an effective nuclear security infrastructure for MORC. Figure 1 illustrates the steps of the planning process in relation to other phases of nuclear security infrastructure development. The planning process should account for the whole spectrum of nuclear security activities (see Figure 1 in [5]).

**Direction**: This step addresses the questions “What is the desired outcome of the nuclear security infrastructure?” and “What activities are needed to be accomplished to achieve the desired outcome?” In this step, descriptions of what the nuclear security infrastructure for MORC needs to accomplish to fulfill mandates are developed. These descriptions can be developed at different levels of specificity. In this document, ‘goals’ refer to high-level statements that set general direction and ‘functional outcomes’ refer to specific descriptions of actions to be performed.

**Assessment of Capabilities and Resources**: This step addresses the questions “what are the capabilities and resources needed to achieve the functional outcomes?”, “What are the existing capabilities and resources?”, “what are the gaps in capabilities and resources?”, and “how are the gaps prioritized?” In this step, an understanding of the broader context is

---

**FIG. 1. A general planning process.**

These three steps, briefly described below, are discussed in detail in the subsequent chapters of this document.
developed, existing capabilities and resources are identified, and capability and resource gaps are determined and prioritized.

**Design:** This step addresses the “How does the State integrate existing and desired capabilities and resources to achieve the functional outcomes?”, “How does the State address the prioritized gaps?”, and “How does the State coordinate with relevant competent authorities to implement the infrastructure design?” In this step, capabilities and resources are integrated in a strategic manner to achieve the functional outcomes. The design step considers priorities and trade-offs to determine the best options under existing constraints. This step develops and formalizes an integrated design plan for the structured development and implementation of the necessary capabilities and resources. This plan promotes a more effective and efficient set of capabilities through cooperation and coordination among various competent authorities and other stakeholders as well as synergies among capabilities and resources.

The development of an integrated design plan is the expected output of the planning phase of the nuclear security infrastructure for MORC development. The respective competent authorities that are responsible for implementing portions of the design plan will then begin the implementation phase.

### 2.2. UNDERLYING PRINCIPLES FOR PLANNING

Several principles are ideally considered across all steps of the planning process for implementing an effective, integrated nuclear security infrastructure for MORC.

--- **Goal-oriented development.** Capabilities and resources for the nuclear security infrastructure for MORC should be developed in support of the goals established by the relevant national policies and strategies. Performance criteria should be established early in the planning process to ensure the implemented infrastructure is evaluated against the full set of goals.

--- **Broad engagement among competent authorities and other stakeholders.** Engaging with all relevant stakeholders provides technical, legal, and operational expertise and enhances integration of elements through a comprehensive understanding of the priorities, resources, and needs of the stakeholders. Transparency in the development process may contribute to stakeholders’ understanding of the context of their role within the infrastructure and to mission acceptance.
— **Clear definition of roles, responsibilities, authorities, and accountability.** Both the development and operation of the infrastructure require the coordination of many competent authorities and other stakeholders. Ensuring effectiveness necessitates that each stakeholder understands its respective role(s) and responsibilities, is provided with the requisite authority, and is accountable.

— **Establishment of mechanisms for communication and coordination.** Communication and coordination of both information and operational activities are essential to the nuclear security infrastructure’s performance in a dynamic security environment. However, communication mechanisms should preserve the security of sensitive information and follow a “need-to-know” basis. Additional guidance on communication and coordination mechanisms is provided in Appendix I and II, respectively.

— **Integration with other security and safety activities.** A nuclear security infrastructure for MORC is not an isolated system, but instead operates in conjunction with other security and safety activities. The experience, infrastructure, and other resources from these other activities can be used to create a more efficient infrastructure that reinforces, rather than competes with, other mission areas.

— **International cooperation.** Cooperation with international and regional organizations as well as other States can provide additional knowledge and expertise, both technical and non-technical, for the development of the infrastructure.

— **Continuous infrastructure evolution.** An effective infrastructure responds to shifting needs, priorities, and environment, such as the emergence or disappearance of a nuclear security threat. States should conduct periodic as well as ad hoc review of the nuclear security infrastructure.

— **Promotion of a nuclear security culture.** Fostering an effective nuclear security culture can help develop and sustain the infrastructure by facilitating awareness and buy-in among stakeholders, as well as motivating personnel (including managers and implementers) by reinforcing the need for nuclear security. Though this nuclear security culture may be difficult to cultivate, many mechanisms exist to help personnel adopt it, including education and awareness programmes, and training. Reinforcement

---

1 In this publication, the specific 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) [10].
by leadership at all levels is important for the culture to be adopted at all levels. As an example, establishing a culture of accountability may include not punishing personnel for reporting material out of regulatory control [11].

2.3. BASIS FOR THE PLANNING PROCESS

2.3.1. National security context

States should consider the broader national security context in which the nuclear security regime will operate. Key aspects of a national security context include:

— **Relevant national legislation, regulations, and policies in nuclear security and national security:** To the extent possible, the nuclear security infrastructure should be based on existing laws and regulations although 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) may be developed to serve this purpose in the interim [12], [13].

— **Relevant national strategy documents:** The nuclear security infrastructure for MORC should consider relevant documents, such as emergency or civil defence response plans. Existing planning documents may have codified goals that can be used in this planning process.

— **Risk Assessment:** States should consider assessing relative nuclear security risks. This assessment provides a basis for prioritizing capabilities and resources. Risk assessments consider both the likelihood and consequences of an act [10].

— **International context:** States should consider relevant international agreements and instruments as well as guidance, standards, and other documents. States may also consider how the national nuclear security regimes of neighbouring States influence each other. International organizations may be consulted for additional international context and guidelines as necessary.

2.3.2. Key roles within the nuclear security infrastructure for MORC

The planning, implementation, and evaluation of a nuclear security infrastructure for MORC involves multiple competent authorities and 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 depending on their respective roles and responsibilities within the
planning, implementation, and evaluation phases of the nuclear security infrastructure development. Competent authorities and other stakeholders may be identified by considering the following questions:

— Are there legal mandates or national policies that specify organizations for national security, nuclear security, and preparedness and response to radiological emergencies? [5]

— What jurisdictions or geographical layers are relevant to the nuclear security infrastructure?

— Are there facilities or organizations that use, store, and/or transport nuclear and other radioactive materials?

— Are there governmental and/or non-governmental organizations that have capabilities or expertise that can be used for nuclear security infrastructure activities?

— Are there organizations responsible for disseminating information to the general public?

— Are there international partners or organizations with capabilities, expertise or experience that could contribute to the development of the nuclear security infrastructure?

Typical stakeholders of nuclear security infrastructure activities come from the following fields and areas of expertise:

— **Intelligence and security personnel:** identify where and how current operational information can be utilized in designing and maintaining the nuclear security infrastructure for MORC.

— **Operational personnel:** implement detection and response systems and may include front line officers and first responders. These personnel have expertise in the operational environment, effectiveness of currently deployed capabilities, and the potential for integrating nuclear security capabilities with other ongoing activities.

— **Policy, legal and regulatory subject matter experts:** provide context for the governance of the national nuclear security infrastructure for MORC.

— **Technical subject matter experts:** Provide expertise in specialized fields including science and technology, information sharing and communication, safety and health, training and exercises, psychology and human factors.
Annex I provides an example of the roles and responsibilities that might be needed for implementing the nuclear security infrastructure for MORC, as well as organizations that could fill those roles.

Due to diversity of competent authorities and other stakeholders involved in the nuclear security infrastructure for MORC, a coordinating body or mechanism with the responsibility to develop and coordinate the nuclear security infrastructure, including the necessary policies, plans or programmes and procedures, may need to be established [4]. As consistent with national practice, this coordinating body or mechanism may be established through legislation or administrative arrangements, which should grant the coordinating body or mechanism sufficient authority and resources (technical, financial, and human) to carry out its responsibilities.

3. DIRECTION: DEVELOPING FUNCTIONAL OUTCOMES

This chapter provides guidance for developing the functional outcomes (Direction planning step), which are derived to articulate specific direction for infrastructure design through consideration of the following questions:

— What is the desired outcome of the nuclear security infrastructure?
— What activities need to be accomplished to achieve the desired outcome?

In this step, functional outcomes are developed that provide specific, measurable, and actionable descriptions of what the infrastructure should achieve and establish the foundation for identifying the necessary capabilities and resources. The basis for developing functional outcomes was described in Section 2.3 and is summarized in the figure below.

---

As described in Ref. [4], the coordinating body or mechanism is responsible for coordination of all nuclear security activities involving nuclear or other radioactive material that are out of regulatory control.
Systematic development of functional outcomes has the following purpose and benefits:

— Articulating the activities necessary to achieve the desired outcomes
— Providing a common understanding of the direction for infrastructure development which enables
  o Organization of roles and responsibilities
  o Creation of procedures for communication and cooperation among organizations
  o Identification of evaluation metrics
— Generating acceptance among stakeholders by providing detail and clarity about the infrastructure’s purpose to ensure consistency in infrastructure design
— Coordinating the development of capabilities and resources

3.1. DEVELOP FUNCTIONAL OUTCOMES

Nuclear security infrastructure for MORC goals and functional outcomes must reflect current national priorities and appropriately address the levels and types of threats and risks present in the State (refer to Section 2.3.1). Infrastructure goals are broad descriptions of the desired end-state. Functional outcomes are specific activities the infrastructure must perform to achieve the goals. Functional outcomes are more specific, measureable, and/or actionable than
the infrastructure goal(s) that they support. Functional outcomes are derived from established infrastructure goals and/or national mandates.

Planners can use several perspectives to frame the development of functional outcomes. Using different perspectives can aid in determining functional outcomes by providing an organizing structure for key concepts, assumptions, and expectations relevant to nuclear security. These perspectives provide practical methods of incorporating a variety of viewpoints, communicating threat and risk-related concepts, and organizing information on disparate risks. Although described separately, these perspectives are not mutually exclusive. The first perspective, risk-oriented, is the preferred approach according to the Nuclear Security Fundamentals as it incorporates information related to threats, vulnerabilities, and potential consequences (see Essential Element 9 in ) [1]. However, the other three perspectives can be used in combination to ensure a comprehensive set of functional outcomes.

3.1.1. Risk-oriented perspective

A risk-oriented perspective focuses on organizing nuclear security activities by the various threats, vulnerabilities, and potential consequences [10]. The following questions can be used to guide the development of functional outcomes using a risk-oriented perspective:

— Are there systems and measures that are robust against a range of threats?
— What materials (type, quantity and form) or devices constitute a concern?
— Are there systems and measures that are effective in detecting particular devices or materials?
— Are there other device components, beyond nuclear and other radioactive materials, that can be detected?
— Are there indications that specific pathways or systems and measures may be particularly vulnerable to adversary exploitation?
— Have specific pathways been targeted for other forms of illicit trafficking?
— What potential consequences (e.g. health, economic, environmental, and societal) should the infrastructure be designed to prevent, respond to or mitigate?

States should consult existing risk assessments to inform the application of these questions to the development of functional outcomes.
3.1.2. **Chronological perspective**

A chronological perspective organizes nuclear security infrastructure activities based on a possible time progression to detect and respond to a nuclear security event. The following questions can be used to guide the development of functional outcomes using a chronological perspective [4]:

- What activities could deter or dissuade an adversary from planning or executing a criminal or intentional unauthorized act involving MORC?
- What activities could reduce an adversary’s capability to plan or execute a criminal or intentional unauthorized act involving MORC?
- What activities are needed to encounter and track threats?
- What kind of information should be collected to support the detection of and response to MORC?
- What activities are needed to acquire and manage information related to the detection of and response to MORC?
- Are there safety, security, and/or safeguards measures that can be used to aid in detection and response to MORC?
- How is information produced, utilized, and managed in the nuclear security infrastructure?
- What capabilities and expertise are needed to effectively analyse nuclear security event-related information?
- What information, capabilities, and authorities are needed to adjudicate an encounter?
- What capabilities are necessary to effectively detain and/or seize, recover and control material, or render harmless any threat or associated device?
- What capabilities are needed to collect, secure, and analyse evidence/exhibits?
- What capabilities are needed to isolate, classify, package, and document any nuclear or radioactive material for transport, carriage, storage, or disposal and placement under regulatory control?

---

3 In this context, “encounter” refers to the collocation of security capabilities and resources with threats. Example encounters may include a law enforcement officer on patrol confronting a nuclear security threat, a proximity sensor along the undesignated border providing an indication of a potential intrusion, and a radiation detection instrument at a designated point of entry/exit alarming due to the presence of radiation.
— What communication, coordination, command, and control mechanisms are necessary to integrate prevention, detection, and response activities, including informing the general public as appropriate?
— What arrangements are needed to notify IAEA and other international partners and organizations, and request assistance as appropriate?

3.1.3. Geographical/Pathway perspective

This perspective considers the pathway through geographical layers that an adversary might use to carry out a criminal or intentional unauthorized act involving MORC. Measures to prevent, detect and respond to a nuclear security event involving MORC may be implemented within each geographical layer. A nine-layer pathways model as shown in Figure 3 may be used for this perspective [5].

In addition to considering the geographical/pathway perspective in Figure 3, the following list of questions can guide the development of functional outcomes:
— Are there domestic or nearby foreign facilities with nuclear or other radioactive materials, or associated activities? What kind of nuclear security activities can be integrated near the pathways that lead to or from such facilities?
— Where should nuclear security activities take place?
  o What pathways could be used to transport nuclear or other radioactive materials?
  o Are there strategic locations, such as checkpoints or border crossings, which can be used by the nuclear security infrastructure?
How can geographical features (e.g., valleys, mountain passes, and bridges) be utilized to minimize the number of locations needed to screen large volumes of traffic?

— Are there multi-purpose activities at the border and in the interior that can be utilized by the nuclear security infrastructure?

— Are there locations where other screening or inspection activities have already been implemented where nuclear detection activities can be integrated?

— Are there existing general response capabilities within a geographical area, such as fire service or public health, where nuclear response capabilities can be integrated?

— How do nuclear security activities at each layer complement and reinforce those activities occurring in other layers?

3.1.4. Threat-oriented perspective

A threat-oriented perspective focuses on milestones associated with an adversary’s ability to commit a criminal or unauthorized act involving nuclear or other radioactive material out of regulatory control. The list below presents some questions that may be used to guide the development of functional outcomes using a threat-oriented perspective: [10]

— What are the potential motivations, capabilities and intent for an adversary?

— Are there strategic locations, critical infrastructure or other points of interest that may be targeted by an adversary? What are the pathways to such locations?

— Are there multiple adversaries? Are there implications if adversaries cooperate with each other?

— What tactics have adversaries previously used? What tactics can an adversary use to counter or avoid the State’s nuclear security efforts?

— What materials (type, quantity, and form) would an adversary need?

— Is there specialized knowledge related to nuclear and other radioactive materials or devices (e.g., improvised nuclear device, radiological dispersal device) that an adversary must learn?

— What resources, capabilities, and infrastructure are needed to develop a threat device?

States should consult existing threat assessments to inform the application of these questions to the development of functional outcomes. Example functional outcomes using these four perspectives are illustrated in Annex II.
3.2. REVIEW FUNCTIONAL OUTCOMES

Once a set of functional outcomes has been developed it should be reviewed by appropriate competent authorities with the criteria listed below. If the review determines that some of the criteria are not satisfied, then the set of functional outcomes should be modified accordingly.

A set of functional outcomes meeting the criteria promotes a comprehensive foundation and clarity for design, implementation, and evaluation.

Criteria for reviewing individual functional outcomes include:

— **Goal-oriented:** Each functional outcome should have a clear link to one or more infrastructure goals and/or mandate. Establishing clear links enables the design step to understand the relationship between functional outcomes and the impact of each functional outcome on the achievement of the infrastructure goals.

— **Sufficient:** Functional outcomes should be detailed enough to provide guidance for the design step without dictating specification of implementation or operational constraints. The functional outcomes should provide wide flexibility for the design step to consider multiple solutions.

— **Time-bound:** This criterion emphasizes the importance of grounding the functional outcomes within a time-frame. A commitment to a timeframe helps focus the planning team focus their efforts on an infrastructure design that can be planned for, and implemented, within the designated time frame.

— **Assessable:** A clear link to evaluation metrics for assessing the execution of the functional outcomes should exist. Either direct or proxy criteria[^4] for assessing performance should be generally envisioned.

— In addition to reviewing the individual functional outcomes, planners should consider reviewing the entire set of functional outcomes according to the following criteria:

— **Comprehensive:** The set of functional outcomes should describe all activities needed to achieve the infrastructure goals. Excluding activities from consideration due to constraints should be reserved for the design step, so that capabilities selection can be informed by the entire breadth of the functional outcomes.

[^4]: Proxy data refers to data that must be used when actual event data is not available. For example, if real data does not exist regarding response times to a nuclear security event, exercises may be used to estimate this response time.
— **Unique**: The functional outcomes should minimize duplication to the degree possible.

A functional outcome is unique if its removal would violate the comprehensive criterion.

The developed and reviewed functional outcomes should be formalized in order to proceed to the next step in the planning process.

### 4. ASSESSMENT: ASSESSING CAPABILITIES AND RESOURCES

The assessment of capabilities and resources step addresses the questions “What is the current situation?”, “what are the gaps in capabilities and resources?”, “how are the gaps prioritized?”

An overview of this assessment process is provided in Figure 4.

A systematic assessment of capabilities and resources has the following purpose and benefits:

— Linking organizational capabilities and resources with functional outcomes.
— Providing an opportunity to address capability and resource gaps and vulnerabilities.
— Providing a basis for infrastructure design.
4.1. DETERMINE NECESSARY CAPABILITIES AND RESOURCES

The goal of this step in the planning process is to identify the capabilities and resources needed to achieve the functional outcomes. Different capabilities may be necessary to meet various functional outcomes. For instance, the determination of necessary capabilities should account for the different operational needs in the exterior, trans-border, and interior layers. This step also needs understanding of their expected function and performance.

To determine the set of necessary capabilities and resources for the nuclear security infrastructure for MORC, States may use the following questions:

— What capabilities are needed to effectively complete key nuclear security activities (see Fig 1 from [5], including assess threats, detect MORC, assess alarms/alerts, interdict, manage radiological crime scene, protect and analyse evidence/exhibits, conduct nuclear forensic examinations, and regain regulatory control?  
— What are the potential consequences of the assessed threats and how can they be mitigated?  
— Are different capabilities needed for each of the relevant geographic layers (exterior, trans-border, interior)?  
— Are different capabilities needed for different transit modes (e.g., air, land, sea)?  
— What response actions and associated capabilities are conducted when managing a crime scene? [14]  
— What are the considerations to protect and analyse evidence/exhibits on a crime scene, including nuclear or radioactive materials or evidence/exhibits from a crime scene possibly contaminated with radioactive material?  
— What capabilities are needed to conduct successful nuclear forensic examinations [15]? What are the considerations to regain regulatory control of MORC (e.g., radiological surveys, decontaminate, package, transport, store, document)?  
— What information sharing mechanisms are needed for all relevant stakeholders to coordinate and communicate?

4.2. IDENTIFY EXISTING CAPABILITIES AND RESOURCES

A national nuclear security infrastructure for MORC should use existing capabilities and resources, which may be available from local, national or international sources [5], [6]. Typically, the nuclear security context is integrated with capabilities and resources from existing security fields and ongoing activities. For example, existing capabilities and
resources for border security and emergency response may have applicability to nuclear
security. These existing capabilities and resources may come from governmental, domestic
non-governmental and international entities. Examples of these capabilities and resources are
provided in the following sections.

4.2.1. Governmental capabilities and resources

Most States have established governmental capabilities and resources that can be augmented
to include the nuclear security context, such as:

— Law enforcement, public safety organizations, and military personnel;
— Legal and regulatory authorities;
— Communication and coordination mechanisms;
— Command and control protocols (e.g. incident management system);
— Technical expertise (e.g. data analysis, spectroscopy);
— Infrastructure (e.g. border crossing checkpoints, electricity) and;
— Financial and human resources.

4.2.2. Non-governmental capabilities and resources

Non-governmental entities, such as private industry, academia, and non-governmental
organizations (NGOs), may have additional capabilities and resources that can be used in the
nuclear security infrastructure, such as:

— Technical expertise;
— Commercial design, testing, and manufacturing of equipment;
— Infrastructure (e.g., training facilities and laboratories); and
— Financial and human resources.

4.2.3. International and regional capabilities and resources

A State may use existing bilateral, regional, and international programmes to strengthen their
national nuclear security infrastructure. Examples include the following:

— International networks, databases, and notice systems, such as the IAEA’s Incident
  and Trafficking Database (ITDB) and INTERPOL’s CBRNE Intelligence Report and
  Operation FAIL SAFE.
— International, regional, and professional organizations, meetings, and training, such as
  INTERPOL, World Customs Organization, International Civil Aviation Organization,
  International Maritime Organization, Global Initiative to Combat Nuclear Terrorism
(GICNT), Nuclear Security Summits, Nuclear Forensics International Technical Working Group (ITWG), European Commission Joint Research Centre, EUROPOL.

In addition, States may benefit from the use of international guidance, such as the IAEA Nuclear Security Series.

4.3. IDENTIFY GAPS IN CAPABILITIES AND RESOURCES

The State should identify gaps in the existing capabilities and resources. A gap analysis determines and documents the discrepancies between needed and existing capabilities and resources; and reveals areas for improvement, areas of redundant or overlapping capabilities, and the significance of the gap. Types of gap may include:

— Governance gaps, such as policy, legal, and regulatory shortcomings;
— Management gaps, such as changes in leadership;
— Knowledge gaps, such as lack of training, awareness, and expertise;
— Operational gaps, such as environmental unsuitability, procedural issues, lack of coordination, and difficulty of use;
— Technical gaps, such as detector sensitivity and resolution as well as software incompatibility when sharing information;
— Resource gaps, such as insufficient financial support, staffing levels, and availability of equipment;
— Sustainability gaps, such as in insufficient maintenance of equipment as well as lack of knowledge management.

4.4. PRIORITIZE GAPS IN CAPABILITIES AND RESOURCES

The identified gaps can be prioritized based on a set of criteria that reflect the gap’s significance to the nuclear security infrastructure. This set of criteria allows relevant competent authorities to determine which gaps merit their immediate efforts. They also provide justification for decisions regarding nuclear security infrastructure needs and resource allocations.

Numerous criteria can be used for this purpose, including:

— **Risk**: Prioritization based on the likelihood and/or potential consequences of a nuclear security event as a result of a gap.
— **Performance**: Prioritization based on the shortcomings in performance measured against the functional outcomes.
Impact on other security contexts: Prioritization based on the impact the gap may have on other security context areas.

Perception: Prioritization based on the public perception of risk.

Prevalence: Prioritization based on frequency of gap occurrence.

Prioritization of gaps may involve multiple criteria and reflect national and international policies as well as political considerations.

Because of the various competent authorities and other stakeholders involved in the nuclear security infrastructure it may be difficult to achieve consensus on the gap prioritization. In such cases, it is important to understand the priorities and constraints of all stakeholders, identify commonalities and origins of differences, and transparently define the responsibility and authority for the final prioritization.

5. DESIGN: DEVELOPING AN INTEGRATED DESIGN PLAN

The design step addresses the questions “How does the State integrate existing and desired capabilities and resources to achieve the functional outcomes?”, “How does the State address the prioritized gaps?”, and “How does the State coordinate with relevant competent authorities to implement the infrastructure design?” by creating a design plan that effectively integrates existing and desired capabilities and resources in a strategic manner to achieve the functional outcomes (Figure 5). In order to effectively address these questions, planners should use the nuclear security infrastructure goals and functional outcomes (Direction), the list of existing capabilities and resources to be used in the infrastructure, and a list of prioritized gaps and a justification for the prioritization (Assessment of Capabilities and Resources).
A structured approach to designing a national nuclear security infrastructure for MORC can provide the following benefits:

- Identifying alternatives for achieving functional outcomes and addressing prioritized gaps
- Integrating systems and measures to develop a more effective and efficient set of capabilities
- Optimizing resource allocation across the infrastructure
- Defining and communicating the roles and responsibilities for the management, operation, and sustainability of capabilities and resources
- Establishing mechanisms for continued coordination and communications to ensure integration and sustainability
- Providing an effective basis for implementation

The Design Step considers priorities and trade-offs to determine the best alternatives under existing constraints. A reviewed and approved integrated design plan is developed and disseminated to competent authorities and other stakeholders responsible for implementing portions of the plan.
This design plan may be further refined by competent authorities for application at the local or organizational level.

The design process starts by identifying and integrating capabilities and resources into a infrastructure design for addressing the prioritized gaps and functional outcomes. The design is reviewed and assessed to understand how well it will address the prioritized gaps. The design is then formalized in an integrated design plan document.

5.1. DEVELOP INFRASTRUCTURE DESIGN

A nuclear security infrastructure design will effectively integrate both existing and desired capabilities and resources to achieve the functional outcomes. This section describes four broad approaches for addressing prioritized gaps and considerations for integrating capabilities and resources in a design.

5.1.1. Approaches for addressing prioritized gaps

Four approaches for addressing the prioritized gaps are listed below. These approaches may be used in combination with one another.

--- Reallocate existing nuclear security capabilities and resources: This approach involves shifting capabilities and resources as well as modifying and refining operations in order to better address the gaps. Additional resources may be drawn from other nuclear security activities where overlaps or redundancies are identified. This approach is limited by the capabilities and resources that are already in place and may be insufficient to address major gaps. Moreover, some stakeholders may be reluctant to sanction the reallocation of capabilities and resources due to the potential for creating new gaps in the areas from which resources are drawn. Thus, permanent reallocations may face substantial scrutiny.

--- Employ capabilities and resources from other mission areas: Competent authorities with complementary missions may have capabilities and resources that could be used for nuclear security. A broader application of capabilities and resources may lead to increased efficiency and effectiveness. Such designs may need formal arrangements between agencies. However, such design alternatives may result in short-term inefficiencies as competent authorities adjust to their new relationships, roles, and responsibilities.
— **Partner with other States or international organizations:** Other States and international organizations may have complementary capabilities and resources. Even limited cooperation may provide alternatives for improved infrastructure effectiveness. This may be achieved through international agreements. To be effective, capabilities and resources provided by other States or international organizations should address the accepting States’ prioritized gaps. In addition, political differences may restrict the capability and resource sharing.

— **Invest in new capabilities and resources:** This frequently involves acquisition from 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. Overall, budget constraints represent the primary challenge to investing in new capabilities and resources. Decision makers may be reluctant to promote additional spending. Thus, they may be more receptive to such alternatives when the gap cannot be addressed through the reallocation or sharing of existing capabilities and resources.

### 5.1.2. Considerations for integrating capabilities and resources into an infrastructure design

Security design attributes may serve as a starting point for integrating capabilities and resources into an effective and efficient infrastructure. The following sections provide guidance on how these attributes can be incorporated into the design step of the planning process [5]. The application of the following attributes, or their combination, to the final design can enhance robustness and effectiveness of the infrastructure.

**Risk-informed and tailored:** There is no universal solution to infrastructure design. Therefore, each State should tailor its design according to its specific conditions and circumstances, including the unique features needed for different geographic and environmental conditions, availability of resources, and legal and regulatory constraints. A risk-informed approach to designing a nuclear security infrastructure 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

---

5 An example of a design alternative that uses cooperative arrangements with other States or international organizations is to have a formal agreement in place for an international or regional partnership to perform nuclear forensic analysis of a sample.
risk reduction [10]. All pathways should be considered, but not all pathways present equal risk. As the design is developed, awareness of the risks may aid in prioritizing design choices and tailoring the design to address the significant risks.

**Multi-layered and defence-in-depth:** 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 mode failure across layers. The use of multiple layers provides greater defence than a single layer by ensuring that a deficiency or failure of one layer can be mitigated by capabilities in another layer.\(^6\)^\(^7\) This also ensures that adversary countermeasures effective against one layer are not necessarily effective against other layers. International cooperation can add layers beyond the national boundaries and extend the reach of the infrastructure.

A multi-layered approach may incorporate redundant components or capabilities so that the failure of a single component or technology does not compromise the infrastructure’s effectiveness. Incorporating redundancy may be achieved through installation of backups or alternatives for critical system components. To enhance efficiency, critical components and potential failure modes should be identified to ensure that redundant systems, consisting of either the same or different technologies, can preserve successful functioning of the infrastructure in the presence of each failure mode. Identifying these systems during planning process improves integration of the redundant systems.

The use of complementary approaches to prevention, detection, and response can increase overall infrastructure effectiveness. For example, complementary approaches to 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. Early in the design planning step, it is necessary to avoid focusing on any specific method and instead consider the breadth of approaches available and capitalize on their respective and complementary advantages.

**Graded and balanced:** Infrastructure design should address all significant potential risks, but should not necessarily assign equal resources to each risk. A graded and balanced approach is

---

\(^6\) 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.

\(^7\) Refer to Requirement 7 of [16] for an example of how defence in depth attribute is applied in the design of safety measures for nuclear power plants [16].
one that considers the level of risk. A graded approach ensures that the capabilities and resources allocated are commensurate with the risk. A balanced approach ensures that some level of capabilities and resources is provided for all risks determined to be significant by the State. 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 pathways, high-value targets, or known trafficking routes (i.e., graded), yet provide some level of detection capability along all pathways (i.e., balanced). A graded and balanced approach can be used when considering different pathways, different threat types, and competing priorities.

Adaptable, evolvable, and unpredictable to the adversary: It is beneficial for the nuclear security infrastructure to be designed to adapt and evolve due 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 availability of resources and technologies. Listed below are methods to promote a nuclear security infrastructure that is adaptable, evolving, and incorporates elements of unpredictability:

— **Modularity** enables an efficient response to changing conditions and circumstances. For example, upgrading of system components over time could be accomplished without requiring a complete restructuring of the infrastructure.

— **Use of systems that are effective against a range of risks** provide a broader defence than those designed to specifically target an individual risk. Using equipment and methods that have multiple purposes as well as flexible training and exercises enables the infrastructure to remain effective against changing and possibly unknown risks.

— **Standardized equipment and data formats** can offer benefits in communications, ease of use, and sustainability. However, it may create vulnerabilities by introducing predictability.

— **Incorporating unpredictability** into the infrastructure can further reduce the adversary’s ability to circumvent nuclear security measures by decreasing its ability to analyse and understand the system, plan evasive measures, and rehearse the plan.

---

8 The unpredictability relates to the adversary’s understanding of the operations, systems, and measures that constitute the regime.

9 Unpredictability can be introduced through measures such as continually adjusting patrol schedules and coverage areas or randomly selecting targets for enhanced screening.
**Operationally flexible:** Operating procedures should be flexible to meet the needs of the nuclear security infrastructure under varying conditions. A method for ensuring operational flexibility is to integrate the nuclear security context with other safety and security activities, as appropriate. For example, a State might plan for surge or search capabilities that can be used to respond to specific risks, increase security for major public events, or secure strategic locations as necessary. In parallel, it can be useful to identify opportunities for nuclear security capabilities to support other missions by allowing them to serve multiple purposes as risks or priorities change. Successfully integrating operational flexibility into the design of the infrastructure needs knowledge of the existing, relevant missions to be used and identification of the kinds of scenarios for which surge-type capabilities may be necessary.

**Strategic communication:** States may manage the potential deterrent effect of nuclear security systems through several communication mechanisms, including [17]:

- **Observation:** Some security systems can be visibly seen by an adversary directly. For example, radiation portal monitors can be observed at international border crossings or personal radiation detectors on the belts of law enforcement officers.

- **Demonstration:** Some security systems may not be directly observable or permanently deployed. In this case, the State can use observable training and exercises to demonstrate detection and response capabilities.

- **Public communication:** States may choose to release information about detection and response capabilities through public communication mechanisms such as the media.

**International and regional cooperation:** International cooperation may provide access to more information and technical expertise than is available to any individual State. For example, methods of cooperating with international organizations and other States may include:

- **Designating a point of contact and establishing communications protocols to facilitate communication and cooperation with regional partners and international organizations.**

- **Sharing best practices, lessons learned, or technical expertise**

---

10 A surge capability is a capability that is not usually employed 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 or SWAT) may be deployed in response to a confirmed information alert.
— Notifying international organizations and other potentially affected States, as appropriate, of nuclear security events or seizures of nuclear or other radioactive materials, including participation in international databases as appropriate.

— Providing or requesting assistance for designing, implementing, and evaluating a nuclear security infrastructure. Topics for assistance may include joint training and exercise, exchange of technical specifications and benchmarks, technical expert support, risk information, support for major public events, and joint research and development.

5.2. REVIEW AND FINALIZE INFRASTRUCTURE DESIGN

The infrastructure design identified should be reviewed to understand how the design will address the prioritized gaps and functional outcomes. A clear set of review criteria can provide a common basis for reviewing and refining the infrastructure design. These criteria should reflect security design attributes and how well the design supports the functional outcomes of the nuclear security infrastructure. Example criteria include:

— **Resources:** The resources needed for various components of the design—in terms of funding, people, and time—are another important consideration. Identifying the available resources may provide critical insight into infrastructure design constraints. Important criteria to consider may include the following:
  - Life-cycle cost, including the cost of development, implementation, operation, maintenance, replacement, and disposition
    - Organizational resources, including designation of components of the infrastructure design to competent authorities that will implement the design plan
  - Human resources, including personnel staffing and training
  - Budget constraints, including both the long and short term
  - Schedule and timeframe, including the time needed to deploy or implement alternatives and the technology readiness level
  - The ease with which a design can be implemented; for example, designs that include commercially available equipment can be easily implemented

— **Effectiveness in supporting the nuclear security context:** Ultimately the proposed design should support the detection of and response to MORC. The ability of the design to contribute to this mission can be understood in both an analytical sense (e.g., probabilities of encounter, detection, and identification) as well as an operational sense
(e.g., false positive rates and coverage). The criteria for effectiveness may be different for different risks and environments.

— **Feasibility:** Operational suitability and efficiency is important to ensure the feasibility of implementation. Feasibility considerations may include necessary staffing level, screening and/or scanning time, and wait time.

— **Legal and regulatory implications:** The legal and regulatory framework of the State may constrain the ability to implement some component of the design. Such constraints may include privacy laws, radiation exposure limits, or transportation infrastructure regulations.

— **Impact:** The design may have different local and national effects:
  
  o **Economic:** Efficient trade and commerce may need to be balanced with national security. For example, high innocent and false alarms rates for detectors may impede the flow of commerce and trade. Reducing this effect may be necessary to minimize the negative impact to the economy.
  
  o **Safety:** The safety of both front line officers and the general public should be considered when assessing the design. For example, a design that does not have adequate temporary storage location for seized nuclear or other radioactive materials can create a safety risk.
  
  o **Environmental:** The installation of checkpoints or equipment and the materials used could have environmental impacts that need mitigation. The use of existing facilities and infrastructure can help minimize these impacts.
  
  o **Societal/community:** The impact on the general public may need to be considered. Depending upon the public’s perception of priorities, the general public could provide significant support or opposition to the nuclear security efforts. Concerns about public perception may also need to be balanced between increasing public knowledge while preserving the security of sensitive activities.
  
  o **Other mission areas:** The nuclear security infrastructure can both contribute to other mission areas and impact their deployed resources. Integrating the nuclear security context may mean that personnel need to undergo additional training, carry additional equipment, or execute supplemental operational tasks that may affect their other ongoing activities.

— **Stakeholder acceptance:** Stakeholder commitment to the design is paramount to effective implementation. Stakeholder acceptance can be difficult to achieve because
there are often competing priorities among stakeholders. Therefore, it is important to integrate relevant stakeholders into the planning process in order to gain a better and shared understanding of the varying perspectives and priorities.

— **Sustainability:** The long-term functionality and viability of the design should be considered and balanced. Sustainability considerations include long-term staffing and training needs, facility maintenance, suitability of the design to changes in risks, and long term support from the public and from decision makers. Appendix III provides additional information on establishing sustainability mechanisms.

### 5.3. DOCUMENT DESIGN PLAN

After review, the design is documented and formalized in a design plan. The decisions that were made as well as the rationale for them should be accurately documented and codified through established channels. Such documentation may contain sensitive information and should be protected according to national procedures. This plan should specify the following:

— Competent authorities involved in developing and approving the design plan

— Basis for the nuclear security infrastructure design
  - International and national legislation and regulation
  - Relevant administrative arrangements and policies
  - Nuclear security infrastructure for MORC goals and scope (if available)
  - Threats and risk assessment
  - Competent authorities and other stakeholders and their role in nuclear security
  - Key decision makers

— A summary of the key findings and decisions made throughout the planning process.
  - Direction
    - Nuclear security infrastructure goals and functional outcomes
    - Performance criteria for future evaluation
  - Assessment of capabilities and resources
    - A list of existing capabilities and resources to be used in the infrastructure
    - A prioritized list of gaps and a justification for the prioritization
  - Design
    - A description of how existing and desired capabilities and resource are integrated to achieve the functional outcomes
- A description of capabilities and resources that will need to be acquired or reallocated to address prioritized gaps.
- Recommended timeline for implementing design plan (start time and duration)
- Mapping of infrastructure design to competent authorities that will implement the design plan

5.4. COMMUNICATION AND DISSEMINATION OF THE DESIGN PLAN

The coordinating body or mechanism should ensure the design plan is appropriately communicated and disseminated to the competent authorities and other stakeholders so they have a clear understanding of their role in implementation of the design (refer to Figure 1). In addition to domestic communication efforts, portions of the design plan may include capabilities and resources from international and/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

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 of the nuclear security context among personnel.

It may be helpful to categorize organizations and 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:

— The level of interest in and existing knowledge about the infrastructure
— Expectations, both for participation in and for communication about the infrastructure
— The sensitivity of the information to be shared as well as the information access levels of personnel
— 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)
— The implementing organization’s role (e.g., legal/regulatory, scientific/technical, law-enforcement, operational, etc.)
— Ability to engage in communications, which may be limited by that organization’s resources

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.

When communicating among organizations, it is important to frame the communication in local and accessible terms. Defining tangible and manageable tasks for organizations promotes their ability to quickly contribute to the mission. Identifying overlaps with other mission areas and integrating nuclear security awareness activities with those for 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 reassure them that adopting the nuclear
security context is an extension of their existing responsibilities and not an entirely new set of responsibilities.

Communication strategies should also provide opportunities for interaction between participants and establish methods for updating and sustaining communication channels.

**Build shared understanding of organizational responsibilities**

To ensure all participants share a common understanding, the roles and responsibilities associated with implementing the infrastructure 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 regarding areas of responsibility, as well as encourage inter-organizational accountability.

Communication among organizations further helps to ensure that the infrastructure 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 in the infrastructure. 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 infrastructure. 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.

**Encourage mission acceptance**

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 mission support, both at the individual and organizational levels. Similarly, creating awareness of the risks and how the infrastructure can help reduce associated risks is likely to encourage active participation.

At a practical level, organizations and individuals may be more likely to actively support nuclear security efforts if they feel that the infrastructure 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 documented processes and procedures will help to avoid frustration, as will efforts to minimize the additional burdens imposed by nuclear
security tasks. It is also critical to ensure that organizations, as well as the personnel, are provided with the resources needed to fulfil their responsibilities within the infrastructure.

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 champions with enhanced training to help them articulate the significance of the nuclear security context.
APPENDIX II. COORDINATION MECHANISMS

Integration is essential to building a infrastructure that is more effective than the sum of individual capabilities and resources. Communication and coordination are needed to develop mechanisms that facilitate long-term integration of the nuclear security infrastructure. This appendix identifies several of these mechanisms that may be used by the organizations as appropriate to the infrastructure:

— **Shared data and information mechanisms:** Multiple organizations may have use for similar sets of information, and information collected by one organization may inform the activities of another. To the extent feasible, and with appropriate security protections, sharing this information can improve overall infrastructure effectiveness. Depending on the type of information to be shared, access protocols for shared databases or routinely scheduled information exchanges may be useful. This can be applicable to both organizations within a State and with international partners and organizations.

— **Command structure:** A clear command structure, combined with appropriate concepts of operations, plays a critical role in integrating infrastructure components. Individual pieces of information from different elements of the infrastructure 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 infrastructure-related operations to be adjusted in response to new information.

— **Identifying opportunities for multi-mission support:** Just as the nuclear security infrastructure 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 and other radioactive materials, but it can also support customs and immigration enforcement.

— **Training and exercises:** Training and exercises conducted across multiple organizations can transfer knowledge and expertise throughout the infrastructure. Cooperative training and exercises may 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 [19].

— Workshops: Workshops incorporating multiple organizations facilitate communication of information and cooperative development of capabilities. Workshops may also encourage the development of professional networks throughout the infrastructure and provide implementers with the opportunity to benefit from the related knowledge and experience of personnel from other organizations. Additionally, workshops provide an opportunity for multiple organizations to arrive at agreements for cooperative operations.

— Focal points: Focal points within the infrastructure may 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. Examples include regional centres of excellence, operations and analysis centres, and technical expert support.

— Rotations: Personnel rotations among multiple organizations can help establish professional networks across the infrastructure, allow organizations to learn about the ongoing activities of other organizations, and aid in identifying prospective areas of cooperation within the infrastructure. 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

Sustainability is an essential part of planning and organization, as it helps to ensure the long-term effectiveness of the infrastructure [18]. Sustainability should be addressed across the infrastructure and may include the following considerations:

— **Operations and management**: Implementing organizations are responsible for the people, processes and equipment associated with the nuclear security infrastructure. The planning process should consider the long-term availability of financial resources to provide for ongoing operational expenses and procurement needs within these organizations including budgetary needs related to personnel, training and exercises, equipment lifecycle obligations, and performance evaluations.

— **Human resources**: Staffing needs and workloads must be reconciled with the added duties and tasks associated with operating, maintaining and managing the nuclear security infrastructure. The impact of personnel turnover should be planned for 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**: Ensuring the continued effectiveness of technical equipment needs the capacity for both preventive and corrective maintenance, both of which rely on processes to track equipment performance, a properly maintained spare parts inventory, and competent, appropriately trained personnel. A sustainable nuclear security infrastructure must also account for equipment lifecycle 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


ANNEX I. EXAMPLE NUCLEAR SECURITY INFRASTRUCTURE FOR MORC
ROLES AND RESPONSIBILITIES

The Table below provides an example of the roles and responsibilities for the nuclear security infrastructure for MORC, 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>
<thead>
<tr>
<th>Role</th>
<th>Description</th>
<th>Example Organization(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>High-level management of the nuclear security infrastructure</td>
<td>Ensures the effectiveness and continual improvement of the infrastructure; is accountable for the execution and success of the infrastructure</td>
<td>Coordinating body or mechanism</td>
</tr>
<tr>
<td>Operation of detection and response systems</td>
<td>Operates nuclear detection and response equipment and ensures its proper operation at their assigned locations</td>
<td>Customs, Border protection, Law enforcement, Nuclear regulatory authority, Health authority, Local government units, Civil defence</td>
</tr>
<tr>
<td>Enforcement of laws and regulations</td>
<td>Enforces the established laws and regulations regarding the possession, use, and transport of nuclear and other radioactive materials</td>
<td>Police, Security services, Nuclear regulatory authority</td>
</tr>
<tr>
<td>Expert support of infrastructure activities</td>
<td>Provides relevant expertise on nuclear and other radioactive materials, implementation, and threat/risk information; provides reach-back resources</td>
<td>Subject matter experts, Academic institutions, National laboratories, Nuclear regulatory authority, Technical support organizations, Industry</td>
</tr>
<tr>
<td>Information collection and analysis</td>
<td>Collects and analyses relevant information about the infrastructure environment and threat/risk information</td>
<td>Intelligence community, Law enforcement, Conveyance / Port operators, Medical community</td>
</tr>
<tr>
<td>Development and production of infrastructure-related</td>
<td>Researches and develops technologies for radiation detection and response, and other needed</td>
<td>Equipment vendors, Academic institutions, Government science and technology</td>
</tr>
<tr>
<td>Role</td>
<td>Description</td>
<td>Example Organization(s)</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>equipment</td>
<td>capabilities</td>
<td>agencies</td>
</tr>
<tr>
<td>Operation of transportation and commercial</td>
<td>Coordinates with infrastructure elements to facilitate operations</td>
<td>Port operators&lt;br&gt;Transport service providers&lt;br&gt;Nuclear regulatory authority&lt;br&gt;First responders</td>
</tr>
<tr>
<td>facilities</td>
<td></td>
<td></td>
</tr>
<tr>
<td>International cooperation</td>
<td>Coordinates and supports international collaborations via information sharing, technical collaboration, and operational cooperation</td>
<td>Relevant implementing organizations from other States&lt;br&gt;Diplomatic agencies&lt;br&gt;International organizations</td>
</tr>
<tr>
<td>Public information</td>
<td>Arranges for informing the news media and public, as appropriate, in a coordinated, understandable and consistent manner;</td>
<td>Coordinating body / mechanism&lt;br&gt;Media</td>
</tr>
<tr>
<td>Acquisition of Equipment</td>
<td>Manages selection and procurement of equipment</td>
<td>Customs&lt;br&gt;Border security&lt;br&gt;Law enforcement&lt;br&gt;Port operators</td>
</tr>
<tr>
<td>Investigations of nuclear security events</td>
<td>Collection, handling, and analysis of evidence from the crime scene</td>
<td>Law enforcement&lt;br&gt;Traditional forensic laboratories&lt;br&gt;Nuclear forensic laboratories&lt;br&gt;Nuclear regulatory authority</td>
</tr>
<tr>
<td>Training, exercises, and evaluation</td>
<td>Develops and conducts training, exercises, and evaluation for the nuclear security infrastructure</td>
<td>Governmental training institutions&lt;br&gt;Non-governmental training providers&lt;br&gt;International organizations and institutions</td>
</tr>
</tbody>
</table>
ANNEX II. EXAMPLE FUNCTIONAL OUTCOMES

The figure below demonstrates how different perspectives may be used to develop functional outcomes. While Figure II-1 shows considerations for each perspective individually, in practice a combination of perspectives will be used to develop a comprehensive and robust set of functional outcomes.

**Goal:** Prevent, detect, and respond to nuclear and other radioactive material out of regulatory control

**FIG. II-1:** Example considerations derived from chronological/functional, geographical/pathway, adversarial, and threat- and risk-oriented perspectives.

As shown in Figure II-2 below, multiple perspectives can be combined to develop functional outcomes.
Goal: Prevent, detect, and respond to nuclear and other radioactive material out of regulatory control

Encounter
Interior
Transport
Radiological Dispersal Device

Functional Outcome:
Create opportunities to encounter the transport of radiological dispersal device in the interior

Chronological / Functional
Geographical / Pathway
Adversarial
Risk-oriented

Acquire data
Border
Shielding
Nuclear materials

Functional Outcome:
Acquire data that would reveal the presence of nuclear materials, through shielding, at designated border crossing points

FIG. II-2. Examples of generation of functional outcomes incorporating multiple perspectives.
ANNEX III. PLANNING AND ORGANIZATION TEMPLATE

BASIS. WHAT DO WE NEED TO DO?

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 infrastructure for MORC addresses the relevant context and the State’s goals.

<table>
<thead>
<tr>
<th>NATIONAL SECURITY CONTEXT</th>
</tr>
</thead>
<tbody>
<tr>
<td>List relevant national legislation, regulations, and policies in nuclear security and national security (e.g., national security legislation, anti-terrorism law, customs law). [2.3.1]</td>
</tr>
<tr>
<td>List relevant national strategy documents (e.g., emergency/civil defence response plans). [2.3.1]</td>
</tr>
<tr>
<td>List relevant risk assessments. [2.3.1]</td>
</tr>
<tr>
<td>List relevant international agreements and instruments, as well as guidance, standards, and other documents to which your country is party. [2.3.1]</td>
</tr>
<tr>
<td>List risk-informed nuclear security infrastructure goals and where they are documented, where applicable.</td>
</tr>
<tr>
<td>Goal</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>KEY ROLES WITHIN NUCLEAR SECURITY INFRASTRUCTURE FOR MORC</th>
</tr>
</thead>
<tbody>
<tr>
<td>List key decision makers with respect to developing the nuclear security infrastructure for MORC. [2.3.2]</td>
</tr>
<tr>
<td>List relevant competent authorities and roles and responsibilities, as authorized by legal provisions. [2.3.2] [Annex I]</td>
</tr>
<tr>
<td>Authority</td>
</tr>
<tr>
<td>-----------</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

Describe the mechanism(s) of coordination among competent authorities with respect to developing the nuclear security infrastructure for MORC. [Appendix I and II]
**STEP 1: DIRECTION.** WHAT IS THE DESIRED OUTCOME OF THE NUCLEAR SECURITY INFRASTRUCTURE FOR MORC? WHAT ACTIVITIES NEED TO BE ACCOMPLISHED TO ACHIEVE THE DESIRED OUTCOME?

<table>
<thead>
<tr>
<th>Goal</th>
<th>Functional Outcome [3.1]</th>
<th>Review Criteria [3.2]</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>□G □A □S □C □T □U</td>
</tr>
<tr>
<td></td>
<td></td>
<td>□G □A □S □C □T □U</td>
</tr>
<tr>
<td></td>
<td></td>
<td>□G □A □S □C □T □U</td>
</tr>
</tbody>
</table>

G=Goal-oriented, S=Sufficient, T=Time-bound, A=Assessable, C=Comprehensive, U=Unique,
**STEP 2: ASSESSMENT.** WHERE ARE THE NECESSARY CAPABILITIES AND RESOURCES NEEDED TO ACHIEVE THE FUNCTIONAL OUTCOMES? WHAT ARE THE EXISTING CAPABILITIES AND RESOURCES? WHAT ARE THE GAPS IN CAPABILITIES AND RESOURCES? HOW ARE GAPS PRIORITIZED?

**CAPABILITIES AND RESOURCES.** Identify necessary capabilities and resources to support each functional outcome. [4.1]

|--------------------|---------------------------------------------------|--------------------------------------------------|------------------------------------------|------------------------------------------------|---------------------------------------------------|

- **H** (High) = Address immediately
- **M** (Medium) = Address when possible
- **L** (Low) = Does not need to be addressed

**SUMMARIZE GAPS BY PRIORITY TO INFORM DESIGN.** [4.4]

<table>
<thead>
<tr>
<th>High Priority Gaps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Medium Priority Gaps</td>
</tr>
<tr>
<td>Low Priority Gaps</td>
</tr>
</tbody>
</table>

INFRASTRUCTURE DESIGN. Identify approaches to address the prioritized gaps identified in Step 2. Assess the alternatives and select for implementation [5.1].

<table>
<thead>
<tr>
<th>Gap</th>
<th>Describe Alternative and Indicate Approach [R/E/P/I]</th>
<th>[H/M/L]</th>
<th>[Y/N]</th>
</tr>
</thead>
<tbody>
<tr>
<td>• [R] Reallocate existing</td>
<td>Effectiveness</td>
<td>Feasibility</td>
<td>Legal and Regulatory Implications</td>
</tr>
<tr>
<td>• [E] Employ from other mission areas</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• [P] Partner internationally</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• [I] Invest in new capabilities</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

H (High) = Best case scenario
M (Medium) = Some challenges, limitations, or negative implications exist
L (Low) = Severe challenges, limitations, or negative implications exist

DESIGN PLAN. Finalize and document design plan. [5.2, 5.3]
List competent authorities involved in developing and approving the design plan [5.3]

Basis for nuclear security infrastructure design [5.3]

Direction [5.3]

Assessment of capabilities and resources [5.3]

Design