

NST061

DRAFT

STEP 8: Soliciting comments by Member
States

2
3
4
5
6
7
8
9 DETECTION IN A STATE'S INTERIOR OF
10 NUCLEAR AND OTHER RADIOACTIVE
11 MATERIAL OUT OF REGULATORY CONTROL

12 DRAFT TECHNICAL GUIDANCE
13

1

FOREWORD

2

[Standard NSS foreword to be added]

3

DRAFT

CONTENTS

1		
2	1.	INTRODUCTION 4
3		BACKGROUND 4
4		OBJECTIVE 5
5		SCOPE 5
6		STRUCTURE 6
7	2.	DETECTION IN A STATE'S INTERIOR AS A COMPONENT OF THE NUCLEAR
8		SECURITY DETECTION ARCHITECTURE 6
9		CHALLENGES AND OPPORTUNITIES FOR DETECTION IN THE INTERIOR 8
10		TRAINING FOR DETECTION OPERATIONS IN THE INTERIOR..... 10
11		EVALUATION OF DETECTION SYSTEMS AND MEASURES IN THE INTERIOR12
12	3.	DETECTION OPERATIONS IN A STATE'S INTERIOR..... 14
13		INTEGRATION OF NUCLEAR SECURITY INTO EXISTING OPERATIONS IN A
14		STATE'S INTERIOR..... 14
15		COMMON TYPES OF DETECTION OPERATIONS IN THE INTERIOR 15
16		ELEMENTS OF DETECTION OPERATIONS IN THE INTERIOR..... 18
17		SPECIAL CONSIDERATIONS FOR DETECTION DURING ROUTINE
18		OPERATIONS 19
19		SPECIAL CONSIDERATIONS FOR DETECTION DURING ENHANCED
20		OPERATIONS 28
21		SPECIAL CONSIDERATIONS FOR DETECTION DURING TARGETED OR
22		SPECIFIC OPERATIONS 30
23	4.	ROLE OF INFORMATION FOR DETECTION OPERATIONS IN THE INTERIOR.. 34
24		COLLECTION OF INFORMATION..... 35
25		ANALYSIS OF INFORMATION AND DATA 37
26		DISSEMINATION OF INFORMATION 37
27	5.	ROLE OF EQUIPMENT FOR DETECTION IN THE INTERIOR 38
28		INSTRUMENT DEPLOYMENT PLAN FOR DETECTION IN THE INTERIOR AND
29		EQUIPMENT SELECTION 39
30		OPERATION OF RADIATION DETECTION EQUIPMENT 40
31		REFERENCES..... 42
32		ANNEX I – EQUIPMENT FOR RADIATION DETECTION 45
33		ANNEX II - JOINT AGENCY DETECTION OPERATIONS PLAN FOR MATERIAL OUT
34		OF REGULATORY CONTROL..... 47
35		ANNEX III – INFORMATION ALERTS OBTAINED FROM MEDICAL SURVEILLANCE
36		 49

37

1. INTRODUCTION

BACKGROUND

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

“A nuclear security regime ensures that nuclear security systems and nuclear security measures are in place at all appropriate organizational levels to detect and assess nuclear security events and to notify the relevant competent authorities so that appropriate response actions can be initiated, including:

...

(c) At major public events or strategic locations, including locations of critical infrastructure, as designated by the State;

(d) In searches for, recoveries of, or discoveries of nuclear material or other radioactive material that is missing or lost or otherwise out of regulatory control;

(e) Within the State's territory or on board its ships or aircraft, and at its international borders.”

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

1.2. As part of a comprehensive nuclear security regime, IAEA Nuclear Security Series No. 15, Nuclear Security Recommendations for Nuclear and Other Radioactive Material out of Regulatory Control [2] addresses prevention, detection and response measures for nuclear and other radioactive material out of regulatory control. Ref. [2] includes recommendations for the detection and assessment of instrument alarms and information alerts related to nuclear or other radioactive material out of regulatory control.

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

1.4. This publication provides guidance on the detection of nuclear and other radioactive material out of regulatory control in a State's interior following a comprehensive approach that involves planning, implementing and evaluating systems and measures in the interior of a State.

1.5. Additional guidance for systems and measures for nuclear and other radioactive material out of regulatory control is presented in the IAEA Nuclear Security Series Nos 24-G Risk Informed Approach for Nuclear Security Measures for Nuclear and other Radioactive Material out of Regulatory Control

[4]; 34-T, Planning and Organizing Nuclear Security Systems and Measures for Nuclear and Other Radioactive Material out of Regulatory Control [5]; and 18, Nuclear Security Systems and Measures for Major Public Events [6].

OBJECTIVE

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

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

SCOPE

1.8. This publication provides guidance on the systems and measures by which nuclear and other radioactive material out of regulatory control can be detected in a State's interior by instrument alarms and by information alerts. The guidance covers planning of detection operations, equipment deployment and human resource development related to detection in a State's interior.

1.9. Nuclear security detection systems and measures at a State's borders are not addressed in this publication. IAEA Nuclear Security Series publication, Detection at a State's Border of Nuclear and Other Radioactive Material out of Regulatory Control (NST 061) [7] "addresses nuclear security detection systems and measures at State borders, with special consideration of designated points of entry and exit and border areas."

1.10. This publication does not cover nuclear and other radioactive material under regulatory control, addressed in IAEA Nuclear Security Series Nos 13, Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5) [8] and 14, Nuclear Security Recommendations on Radioactive Material and Associated Facilities [9], respectively.

1.11. This publication does not address response activities in the situation that nuclear or other radioactive material is detected and a nuclear security event is declared. Guidance on nuclear security related response activities fall within the scope of IAEA Nuclear Security Series No 37-G, Developing a National Framework for Managing the Response to Nuclear Security Events [10].

1.12. This publication references IAEA Safety Standards Series No. GSR Part 7, Preparedness and Response for a Nuclear or Radiological Emergency [11] as appropriate regarding identification of and

notification on a radiological emergency during detection activities as well as relevant activation of emergency response plans.

STRUCTURE

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

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

2.1. Ref. [2] states:

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

2.2. The detection strategy should define how a State plans to accomplish its detection mission in both the interior and at the borders of a State. An integrated planning process for nuclear security systems and measures is described in Ref. [5]. Additional information can be found in IAEA Nuclear Security Series No. 29-G, Developing Regulations and Associated Measures for Nuclear Security [13].

2.3. When a State designs and develops the national nuclear security detection architecture, it should apply the defence in depth principle and follow a multi-layered approach “including measures at and between points of entry or exit (POEs) into the State, within the State and in other cooperating States” [3].

2.4. According to Ref. [3] the nuclear security detection architecture and its systems and measures have three primary layers: the exterior, the trans-border and the interior. Ref. [3] states that: “The

1 interior layer, within the target State, represents the final opportunity to detect and interdict nuclear and
2 other radioactive material out of regulatory control before it could be used in a criminal act or
3 unauthorized act.”

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

13 2.6. Law enforcement, national security organizations and other organizations providing emergency
14 services¹ are likely to have their own existing risk-informed strategies for addressing traditional security
15 threats and other conventional risks. The nuclear security threat and risk assessment for nuclear and
16 other radioactive material out of regulatory control should be coordinated with and integrated into these
17 other existing threat and risk assessment processes and national security and conventional emergencies
18 response strategies (e.g. counter-terrorism, counter-intelligence and counter-organized crime strategies)
19 at both the national and organizational levels.

20 2.7. Paragraph 3.12 of Ref. [2] states that “All nuclear security activities involving nuclear or other
21 radioactive material that are out of regulatory control should be coordinated by a body or an effective
22 mechanism in accordance with national legislation and regulations.” All competent authorities and other
23 stakeholders participating in detection in a State’s interior should be included in the coordination
24 mechanism. This coordination mechanism could support the process of developing and implementing
25 the interior component of the national nuclear security detection strategy, resolving potential disputes
26 between relevant authorities, ensuring adequate training among all relevant stakeholders, establishing
27 sustainability mechanisms and exchanging operational information among relevant competent
28 authorities in the interior.

29 2.8. Paragraph 3.18 of Ref. [3]. states that “Deployed assets, such as detectors, technical support and
30 analysis centres, should have the ability to exchange accurate and timely data. An effective data

¹ Organizations providing emergency services (police, fire brigade, civil protection, etc.) during their routine work prior to the declaration of a nuclear or radiological emergency or during conventional emergency response not involving radiation.

exchange infrastructure should have a combination of effective connectivity (robust, redundant and of sufficient bandwidth) and appropriate data standards or protocols to allow the recipient to understand the transmitted information. Effective data exchange also enables necessary situational awareness.”

2.9. Two-way communication among different levels (e.g. strategic, operational, tactical) guarantees that all relevant information is shared among the different levels in an organization and that differences in threat and risk perceptions for a State’s interior can be clarified before information is shared with other organizations.

2.10. Organizational policies and procedures should provide the basis for the operational level of the detection architecture for a State’s interior. Nuclear security operations cross multiple organizations with different responsibilities. A State should consider developing a joint agency detection operation plan for the detection of nuclear or other radioactive material out of regulatory control in the interior as part of the broader nuclear security strategy. This plan should involve all competent authorities and other stakeholders with roles and responsibilities for detection in the interior. Annex II provides a template with the components to be included in this plan.

CHALLENGES AND OPPORTUNITIES FOR DETECTION IN THE INTERIOR

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

2.12. The entire spectrum of criminal or intentional unauthorized acts involving nuclear or other radioactive material out of regulatory control can occur entirely in a State’s interior with or without material, device, or adversary crossing the State’s borders. This includes unauthorized acquisition of material, possession of material and/or device, device fabrication, material and/or device movement and malicious use, threats or attempts to commit an act, unlawful scams or hoaxes with nuclear security implications.

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

1 the unauthorized movement of material and a large number of potential targets that can be exploited by
2 the adversary.

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

7 2.15. The interior of a State is typically too large to achieve full coverage with equipment for radiation
8 detection. Due to limited resources, at any given time States are usually able to focus on only a selected
9 number of pathways or potential targets, that should be identified using a risk-informed approach,
10 Additionally, most detection equipment is designed to scan a limited, defined area under controlled
11 conditions. Therefore, the use of information is of paramount importance to prioritize the effective
12 deployment of these limited resources. Section 4 outlines the process for information collection,
13 analysis and dissemination to support effective detection operations in a State's interior.

14 2.16. A large number of competent authorities and other stakeholders² operate in the interior. Each
15 authority has a different mission, operates under its own procedures and might have different levels of
16 awareness and practical experience with nuclear security. The administrative division of a State might
17 create different levels and jurisdictions (e.g., federal, regional, local) of competent authorities and other
18 stakeholders. This division among the many relevant stakeholders can create communication and
19 coordination challenges.

20 2.17. In the interior, the timeline for completing a criminal or intentional unauthorized act might be
21 compressed. If detection occurs in close proximity to an intended target, it might be more difficult to
22 neutralize the threat of the criminal or intentional unauthorized act involving nuclear or other material
23 out of regulatory control and mitigate the consequences of a potential nuclear security event. Strategies
24 to address this challenge include performing detection activities as far away from potential targets as
25 possible or, at least, at a sufficient distance to ensure the protection of the target. For the design and
26 implementation of these strategies, the State should undertake an ongoing evaluation of nuclear security
27 threats and risks and identification of potential targets.

² The phrase 'competent authorities and other stakeholders' is used in this publication to describe all entities that could be involved in the area of detection of nuclear and other radioactive material out of regulatory control. Examples include law enforcement, intelligence and security agencies, fire brigade, civil defence, private security organizations, technical support organizations, defence forces, health authorities and the public.

2.18. States might consider implementing low-visibility or discrete detection operations to avoid prematurely alerting potential adversaries of the existence of detection systems and measures at specific locations in the interior.

2.19. To ensure a strong link between the detection and response competent authorities and other stakeholders within the interior layer, States might consider establishing and deploying specialized operational teams with personnel who are qualified in nuclear security detection and response (See Ref [10]) and/or emergency response operations, in accordance with Refs. [11, 12].

2.20. Sustainability constraints, including long-term financial, human and technical resources, should be considered when designing detection operations and associated systems and measures in the interior. Ref. [3] states that “Sustainability is a key consideration for the nuclear security detection architecture. Significant planning and commitment of resources, both financial and human, are needed to ensure the long-term operational effectiveness of national capabilities for detection of nuclear and other radioactive material out of regulatory control.” Guidance on developing national and operational sustainability objectives can be found in IAEA Nuclear Security Series No. 30-G, Sustaining a Nuclear Security Regime [14].

TRAINING FOR DETECTION OPERATIONS IN THE INTERIOR

2.21. IAEA Nuclear Security Series No. 31-G, Building Capacity for Nuclear Security [15] provides information on a systematic approach to training (SAT). According to Ref. [15], “The first phase of the SAT is to determine the training needs of personnel at all levels and with all types of responsibility for nuclear security. This is a major task that involves analysis of the performance requirements (i.e. duties and tasks) of individuals who have direct responsibility for planning, implementing and/or evaluating the effectiveness of the nuclear security programme.”

2.22. Ref. 13 states that:

“In order to establish a strategy for developing an awareness programme, goals should be established to focus awareness raising efforts, including the following: (a): Providing individuals with foundational knowledge and guidance relevant to their roles and responsibilities for nuclear security (e.g. information on nuclear security threats, detection options and operations) for building an effective nuclear security culture. This knowledge can provide a basis for advanced training and a broader understanding of one’s responsibilities.”

2.23. Ref. 13 states that

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

(a) Communicate the need for nuclear security efforts;

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

Given the diverse set and the large number of competent authorities and other stakeholders operating in the State’s interior, the State should implement a graded approach to training. The State should establish awareness building and training curricula tailored to the needs of the target audience according to their role and function in the interior component of the nuclear security detection architecture.

2.24. Basic nuclear security awareness training should be provided to the personnel of all national competent authorities and other stakeholders that participate in detection operations in the interior of a State. Regardless of whether the personnel are equipped with nuclear security detection equipment, they might encounter nuclear and other radioactive material out of regulatory control or generate information alerts. This basic level of awareness ensures that these personnel are alert to the signs of suspicious activity involving material out of regulatory control. Separately, increasing general public awareness enhances nuclear security culture.

2.25. The following topics need to be included in the basic nuclear security awareness training:

- Basic concepts of radiation (e.g. types of radiation emitted by nuclear and radioactive material, exposure, contamination);
- Basic concepts of radiation protection (e.g. the effect of time, distance, shielding);
- Authorized uses of radioactive material and devices;
- Nuclear security threats involving nuclear and other material out of regulatory control;
- Indicators of suspicious activity involving nuclear and other radioactive material;
- Overview of the nuclear security detection architecture;
- Procedures for requesting assistance in case of a potential nuclear security event.

2.26. For personnel of competent authorities and other stakeholders expected to operate detection equipment or to investigate an instrument alarm or information alert, specialized training should be offered in addition to the basic awareness training. This specialized training should be conducted before the deployment of radiation detection equipment and at regular intervals to ensure operational preparedness.

2.27. This specialized training needs to include the following topics:

- 1 – Basic principles of radiation detection;
- 2 – Types of radiation detection equipment;
- 3 – Operational instructions for the use of the equipment;
- 4 – Daily checks for the functionality of the equipment;
- 5 – Common causes of innocent alarms
- 6 – Basic preventive maintenance;
- 7 – Standard operating procedures for detection operations.

8 2.28. Competent authorities and other stakeholders can improve their personnel's competency in
9 nuclear security detection by integrating appropriate modules into existing training programmes. For
10 example, a module for nuclear security threat awareness could be included in basic training for new
11 recruits and then made mandatory as part of periodic refresher trainings.

12 EVALUATION OF DETECTION SYSTEMS AND MEASURES IN THE INTERIOR

13 2.29. The establishment of an evaluation framework or process can promote consistent improvement
14 across nuclear security detection operations in a State's interior. The evaluation process should cover
15 all essential elements of the national nuclear detection architecture, such as legal framework, strategies,
16 plans, and procedures, risk analysis, human resources and technical assets for detection operations in
17 the interior. The evaluation is a continuous process and should be repeated regularly.

18 2.30. Evaluating detection operations in the interior can be particularly challenging because of the large
19 number of competent authorities and other stakeholders operating in a wide variety of locations and
20 conducting detection of criminal or intentional unauthorized acts.

21 2.31. The evaluation should be properly scoped to ensure that its results can inform the improvement
22 of the detection operations in the interior. Scoping is the process of focusing the evaluation by clarifying
23 its purpose and includes the following actions:

- 24 - Defining what the evaluation will cover. The focus can be on a single component (such as a
25 detection instrument), process (such as the integration of nuclear security detection into routine
26 patrols of the interior), multiple operational components (such as officers on routine patrol
27 calling for technical expert support), or the coordinated operation of the interior nuclear security
28 detection architecture as a whole.
- 29 - Determining the level of the evaluation. Evaluations can be done at the organizational level,
30 national level, or through peer reviews by international experts, using mechanisms such as the
31 IAEA's International Nuclear Security Advisory Service (INSServ).
- 32 - Identifying the desired output. Outputs can include deliverables such as the evaluation of
33 operational efficacy of established concepts of operations and standard operating procedures,

1 qualifications of personnel and their ability to implement and adhere to established concepts of
2 operations or standard operating procedures, costs associated with incorporation of nuclear
3 security detection into existing interior security activities.

4 2.32. Evaluation criteria and metrics should be used to systematically gauge progress with respect to a
5 stated evaluation goal. Metrics should be relevant to the specific evaluation purpose and scope, and
6 provide information that can be acted on. The metrics should be measurable, accurately quantifying
7 information related to the corresponding functional objectives of detection in the interior, objective and
8 independent from outside influence and consistent across systems in terms of what the metrics measure,
9 how the metrics are defined, and the units used.

10 2.33. The evaluation should assess both operational capacity and efficacy. Capacity represents the
11 number of resources available to achieve the intended results. Examples of capacity-based metrics
12 include the percent of interior security personnel trained on radiation basics and/or equipped with
13 detection instruments. Efficacy represents the ability to perform and achieve the intended results.
14 Examples of efficacy-based metrics include the probability of detecting a threat material of concern
15 with the deployed detection operations with or without the use of instruments and the time needed for
16 individuals or vehicles to go through interior checkpoints due to screening procedures.

17 2.34. The State should decide the evaluation method best suited to achieve the desired outcomes. Each
18 methodology may be performed either as a self-assessment or as an independent assessment. The
19 following evaluation methods can be employed for the assessment of detection operations in the
20 interior:

21 (a) Exercises can be conducted to assess plans, procedures and performance of individual and joint
22 tasks. Exercises should be structured, capability based, objective driven and scalable to the
23 individual or organizational need. Establishing regular multi-agency exercises is essential for
24 interior competent authorities to integrate detection strategies with existing procedures,
25 operations and other technical means to ensure operational readiness for a nuclear security
26 event. Detailed guidance on the preparation, conduct and evaluation of exercises can be found
27 in Ref. [15] and Nuclear Security Series No. 41-T, Preparation, Conduct and Evaluation of
28 Exercises for Detection of and Response to Acts Involving Nuclear and Other Radioactive
29 Materials out of Regulatory Control [16].

30 (b) Red team testing involves challenging the plans, programmes, assumptions and implementation
31 of detection operations. This method often uses a covert testing method where the red team
32 serves as a surrogate adversary and attempts to introduce a threat into the system without being
33 detected. Modelling and simulation can be used to simulate an outcome or to develop a basis

for decision making. Example application includes the evaluation of the effectiveness of instrument alarm algorithms or radionuclide identification algorithms.

(c) Administrative analysis is generally conducted by an evaluation specialist or unit, structured within the competent authorities, can ensure continuous assessment of the nuclear security detection architecture and can monitor the implementation of improvement plans that result from previous evaluations. Examples of administrative analysis include ‘strengths, weaknesses, opportunities, and threats’ (SWOT) analysis, gap analysis, qualitative and quantitative assessment, performance analysis, instrument data analysis and statistical comparison.

(d) Technical analysis includes performance testing and evaluation to ensure the effectiveness of systems and equipment and is generally conducted by technical subject matter experts within the competent authority or support organization.

The main output of the evaluation process is an evaluation report documenting all information on the evaluation including the methodology used, evaluation objectives, the data collected, the results, and any recommendations. The recommendations should be relevant to the existing objectives for detection in the interior and provide actionable steps for the improvement of the operations. The evaluation report should be provided to all relevant stakeholders for review, and their feedback should be incorporated. As the results of an evaluation and the data collected, are often sensitive to national security, the report should be treated according to established procedures for the protection of information.

3. DETECTION OPERATIONS IN A STATE’S INTERIOR

INTEGRATION OF NUCLEAR SECURITY INTO EXISTING OPERATIONS IN A STATE’S INTERIOR

3.1. Detection operations for nuclear and other radioactive material out of regulatory control in a State’s interior can be conducted by law enforcement, emergency services and specialized teams such as intervention units, hostage rescue teams, explosive ordnance disposal units, crime scene investigation teams and chemical, biological, radiological and nuclear (CBRN) teams. In accordance with essential element 5 for the nuclear security fundamentals, the State should establish offences and penalties, including criminalization, for those acts determined by the State to have an adverse effect on nuclear security that are proportionate to the gravity of the harm that could be caused by commission of the offences or violations [1].

3.2. Competent authorities and other stakeholders in the interior of a State should integrate detection operations into their existing mission areas, concept of operations, procedures and training programmes, as well as with detection operations conducted at a State’s borders. As multiple competent authorities

might already have capabilities and competencies for detection, the coordination of the detection activities conducted by these authorities and the development of a joint agency detection operations plan (see Annex II) increases the efficiency of detection operations in the interior.

3.3. Competent authorities and other stakeholders in the State's interior do not typically operate radiation detection equipment. As part of the national nuclear security detection architecture and to be able to assess information alerts, they should be able to have access to specialized teams or expert support teams that have the capability to operate radiation detection equipment.

3.4. Law enforcement and emergency services could incorporate the use of radiation detection equipment into their detection operations. If law enforcement and emergency services are equipped with radiation detection equipment, they should be provided, as appropriate, with the corresponding training and procedures on how to operate this equipment and interpret data from the measurements.

COMMON TYPES OF DETECTION OPERATIONS IN THE INTERIOR

3.5. Detection operations in the interior can be categorized into three common types: routine operations, enhanced operations and targeted or specific operations. These types of detection operations are described in paras 3.7-3.20. Special considerations for detection during routine, enhanced and targeted or specific operations are elaborated in paras 3.21-3.68 and examples are provided for each type of detection operation. These examples can be used as a basis for planning and conducting detection operations and are not meant to be exhaustive.

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

Routine operations

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

3.8. When law enforcement and emergency services are not equipped with radiation detection instruments, their ability to recognize indicators of suspicious activity involving nuclear and other radioactive material out of regulatory control can generate an information alert. In this case, coordination and information sharing between competent authorities, specialized teams or technical

support organizations with access to radiation detection equipment is essential for confirmation and adjudication of the alert.

3.9. Special considerations and examples of routine operations are presented in paras 3.24-3.49. These examples include routine patrols, routine checkpoints, conventional operations of emergency services, detection by information alert obtained from medical surveillance, public reporting and law enforcement investigations.

Enhanced operations

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

3.11. For enhanced operations, additional resources might be allocated to law enforcement and emergency services to detect the presence of material out of regulatory control in accordance with a risk-informed, graded approach. Based on the information on the potential threat, enhanced detection operations can be integrated into all operational duties including roadside checks, routine patrols, dignitary protection and securing of high profile events.

3.12. When conducting enhanced detection operations, competent authorities and other stakeholders should consider the duration of the enhanced phase as this would employ a larger amount of technical and human resources than routine operations. No competent authority has unlimited resources, therefore cooperation among multiple competent authorities with detection capabilities should be considered. Operating jointly with partner competent authorities enables law enforcement and emergency services to have access to a larger number of radiation detection equipment or more sophisticated technical equipment and to more personnel with training in nuclear security detection.

3.13. Special considerations and examples of enhanced operations are elaborated in paras 3.50-3.57 and include operations after a general information alert and operations at a high profile event.

Targeted or specific operations

3.14. Targeted or specific detection operations are conducted based on specific, credible and actionable information that indicates with high probability that a nuclear security event is in preparation, on-going or has taken place.

3.15. Targeted or specific operations can be conducted as part of the initial assessment activities when a specific threat has been detected by information alert or instrument alarm, when an event (such as theft or loss) involving material out of regulatory control has already occurred, or as requested by investigative and special operation units, based on precise information or intelligence.

3.16. When planning targeted or specific detection operations, consideration should be given to the nature of the operation (overt or discreet), the aims of the operation (detection or deterrence), the availability of human and technical resources and the number and level of trained personnel.

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

3.18. Information or intelligence before the initiation of targeted or specific operations will aid competent authorities and other stakeholders in selecting the appropriate detection equipment to be used and determining how standard operating procedures should be adapted.

3.19. These operations should be conducted in connection with emergency management processes and nuclear security arrangements, depending on the severity of the situation (as described in the state's national response framework). References [2] [10] and [11] address the specific nuclear security measures and radiological emergency response actions, including emergency response plans.

3.20. Special considerations and examples of targeted or specific operations include area searches and undercover operations. These examples are elaborated in paras 3.58-3.68.

TABLE 1: COMMON DETECTION OPERATIONS IN A STATE'S INTERIOR BY CATEGORY

Routine Operations	Enhanced Operations	Targeted or Specific Operations
Detection During Routine Patrols Detection During Routine Checkpoints Detection During Routine Operations of Emergency Services Information Alert Obtained from Medical Surveillance Information Alert Obtained from Public Reporting Information Alert Obtained from Law Enforcement Investigations	Detection During a Heightened Security Posture Detection During a High Profile Event	Detection During Targeted Searches Information Alerts Obtained from Undercover Operations

ELEMENTS OF DETECTION OPERATIONS IN THE INTERIOR

3.21. The sub-sections that follow present special considerations and provide detailed examples for the different types of detection operations outlined in table 2. For each type of detection operation guidance is provided on the personnel typically involved in the specified detection activities, the preparatory activities that should be completed prior to conduct of the detection operations, the steps to be followed by the personnel in implementing the detection operation and example fictional scenarios. Where applicable, operational steps and examples are provided for the conduct of detection operations both with and without the use of radiation detection equipment.

3.22. Figures 1-10 provide visual representations of the steps described for each type of detection operation presented in this Section. Boxes depict operational steps and diamonds depict decision points. When a step is optional, dashed lines are used for the arrows and boxes.

3.23. Across all detection operations in the interior of a State, the following elements and activities should be in place to ensure effective conduct of operations and provision of a proper baseline for the personnel:

- Authority to conduct operations: Before the implementation of detection activities, the State should ensure that the personnel conducting these activities has the necessary authorities and jurisdictions. Especially in the case of a targeted search, additional activities might have to be undertaken to ensure that the personnel have the authorization to conduct the search or to proceed with undercover operations.
- Procedures for the detection of criminal or intentional unauthorized acts: The competent authorities and other stakeholders should develop concepts of operations and standard operating procedures for detection, they should establish interagency agreements, as appropriate, and any necessary arrangements for involvement of technical expert support.
- Procedures for information management: Arrangements for information sharing should be established to manage the exchange of information within an organization and between different organizations (see Section 4 for further information).
- Training for the implementation of different types of detection operations: The personnel should have received appropriate training for the detection of criminal or intentional unauthorized acts, as described in paras 2.21-2.28. This includes training on the proper use of any deployed equipment which the personnel are expected to operate in support of those operations.
- Domain awareness: The personnel should have prior knowledge of the area of responsibility and the situational context, including the presence of authorized nuclear and other radioactive

material in the area (e.g. nuclear, medical, research or industrial facilities) and any pre-existing locations with elevated radiation levels.

- Nuclear safety awareness: The IAEA has established requirements for the safety of radioactive material in the IAEA Safety Standards Series. The relevant publications include SF-1, Fundamental Safety Principles and GSR Part 3, Radiation Protection and Safety of Radiation Sources: International Basic Safety Standards.
- Nuclear or radiological emergency response interface: If an information alert or instrument alarm has been confirmed as a non-false alarm, the personnel should determine whether it is safe to proceed. If an actual or potential radiation hazard makes it unsafe to proceed, the appropriate response organization(s) should be notified and appropriate protective actions and other response actions implemented in accordance with Refs [10] and [11].³

SPECIAL CONSIDERATIONS FOR DETECTION DURING ROUTINE OPERATIONS

Detection operations during routine patrols

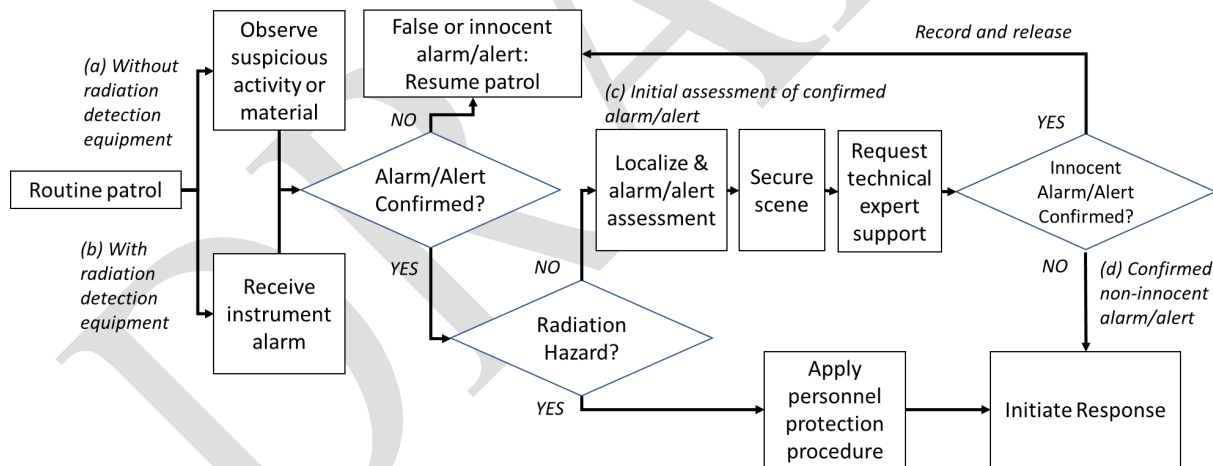


FIG. 1. Example of detection operations for routine patrols.⁴

³ Appropriate response actions include identification whether the operational criteria warranting appropriate protective actions are met, as explained in Refs. [11] and [20].

⁴ The box “apply personnel protection procedure” is an abbreviation for what is referred to in the text as “apply safety standards procedure for your professional area” and it shares the same meaning as “implementing Safety Measures” in Figure 3 of NSS 21 Ref. [3].

3.24. The personnel typically involved in routine patrols belong to the law enforcement, the gendarmerie and other security agencies, or private stakeholders, such as private site security contractors. Patrols of a defined area of operation are regularly carried out by such competent authorities and other stakeholders as part of their normal operations.

3.25. The concept of operations for adding nuclear security detection to existing standard operating procedures of routine patrols should be developed taking into consideration whether the personnel have detention and interdiction authority, whether they use radiation detection equipment themselves and the type of equipment, if available.

3.26. The personnel should have awareness of the domain in which they are designated to patrol, they should have received basic nuclear security awareness training and, if they are provided with detection equipment, then they should also be trained on the use and basic maintenance of such equipment in advance of their deployment patrol.

3.27. Figure 1 shows the actions to be followed during routine patrols by the personnel based on whether or not they have radiation detection equipment as follows:

- (a) If the personnel are on patrol without radiation detection equipment and observe or receive information on any suspicious activities or materials that could indicate the presence of nuclear or other radioactive material out of regulatory control, they should assess the credibility of the information to confirm the alert.
- (b) If the personnel are on patrol with personal radiation detectors and they receive an instrument alarm, they should confirm the validity of the primary detection to determine whether or not it is a false alarm. Applicable radiation detection equipment for use during routine patrols can include personal radiation detectors worn by the operational personnel.
- (c) If the alarm or alert is confirmed and it has been determined that there is no radiation hazard, the personnel proceed to initial assessment of the alarm/alert, including to localize the potential source of radiation and secure the scene. This might include separating or isolating any individuals present at the scene from materials or property, and the detention and interdiction of the suspect material and the individuals. The personnel can then request technical expert support to assist in the assessment of the alarm/alert. Given the limited capabilities of most handheld equipment, even personnel with equipment will likely need to contact technical expert support to complete the alarm assessment and identify the present material.
- (d) If it is determined to be a false or innocent alarm, the personnel may resume their patrol. If a non-innocent alarm is confirmed the appropriate response organization(s) should be notified, personnel protection procedure for professional area applied, and protective actions and other response actions implemented in accordance with Refs [10] and [11].

3.28. Example scenarios for detection during routine law enforcement patrols are the following:

- An officer on patrol discovers a package with the radiation trefoil symbol. The officer does not have radiation detection equipment. The officer secures the area around the package and notifies the shift supervisor to request technical expert support for identification of the package contents.
- An officer on patrol walks past a dumpster and receives an alarm on their personal radiation detector. The officer follows the established procedures to use the detector to confirm a non-innocent alarm. The officer locates the area of elevated radiation, secures the area, and notifies the shift supervisor to request technical expert support to proceed with the identification of the material in order to confirmation a non-innocent alarm.

Detection operations during routine checkpoints

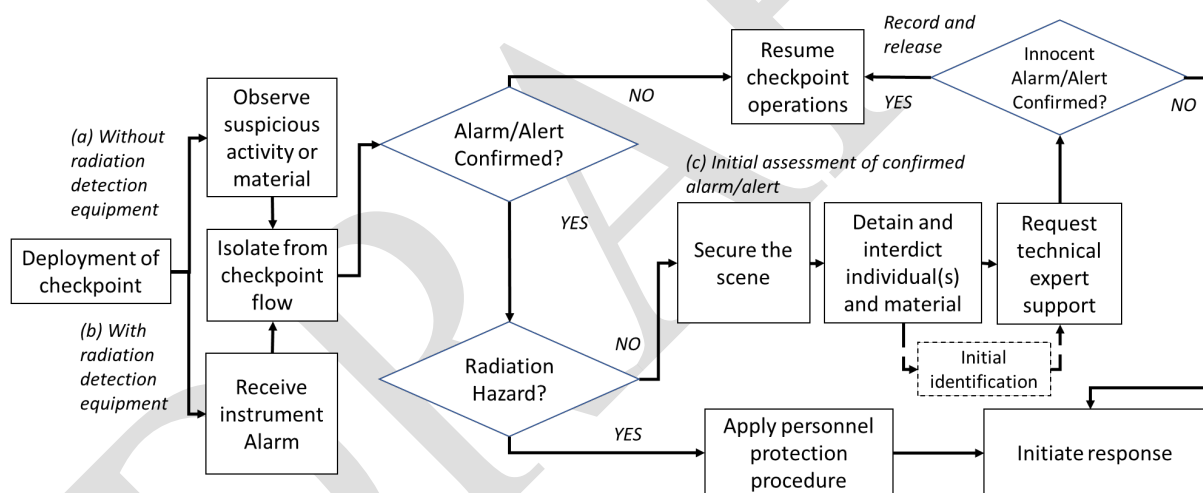


FIG. 2. Example of detection operations for routine checkpoints.

3.29. The personnel typically involved in checkpoints belong to the law enforcement, the gendarmerie and security agencies, or private stakeholders, such as private site security contractors. Checkpoints can be established at traffic chokepoints, regional commercial hubs, inspection stations or transportation hubs, entrances to buildings or facilities.

3.30. The locations of checkpoints are selected as a result of careful planning. Checkpoint planning includes ensuring appropriate human resources will be available, setting up traffic control measures, selecting locations for performing identification of persons and/or vehicle isolation, and locations for conducting secondary inspections.

1 3.31. The personnel should have awareness of the domain in which they are designated to conduct the
2 checks, they should have received basic nuclear security awareness training and, if they are provided
3 with detection equipment, they should also be trained on the use and basic maintenance of such
4 equipment in advance of their deployment. The personnel conducting the checks should have the legal
5 authority and ability to detain and pursue vehicles, and detain suspects.

6 3.32. The personnel should be aware of how time, distance, and shielding affect detection. For
7 example, high activity radiation sources can trigger an alarm from greater distances (e.g., several
8 individuals or cars back). The concept of operations should be designed to ensure the personnel can
9 quickly identify which person or vehicle is the source of the alarm.

10 3.33. Figure 2 shows the actions to be followed by the personnel deployed at a checkpoint conducting
11 their routine duties based on whether they have radiation detection equipment. These actions can be
12 summarized as follows:

- 13 (a) If the personnel are operating a checkpoint without radiation detection equipment and observe
14 any suspicious person or material pass through the checkpoint, they should isolate the suspect
15 individual and/or material from the checkpoint flow and assess the credibility of the information
16 to confirm the alert.
- 17 (b) If the personnel have radiation detection equipment and they receive an instrument alarm, they
18 should isolate the suspect individual and/or material from the checkpoint flow and confirm the
19 validity of the primary detection to determine whether or not it is a false alarm. Applicable
20 radiation detection for use at checkpoints can include personal radiation detectors worn by the
21 operational personnel, vehicle mounted radiation detection systems for use at temporary
22 checkpoints, or radiation conveyor belt monitors for scanning of cargo or other goods. If it is a
23 false alarm, the personnel should resume their operations.
- 24 (c) If the alarm or alert is confirmed and it has been determined there is no radiation hazard, the
25 personnel can proceed with securing the location, separating people from property, detaining
26 and interdicting the material and the individuals involved. If available, trained personnel may
27 use a handheld radionuclide identification device to perform initial identification of the
28 material. Otherwise, they can proceed directly to requesting technical expert support to
29 complete the initial alarm assessment and for identification of the material.
- 30 (d) If it is determined to be an innocent alarm, the personnel may resume their checkpoint activities.
31 If a non-innocent alarm is confirmed the appropriate response organization(s) should be
32 notified, personnel protection procedure for professional area applied, and protective actions
33 and other response actions implemented in accordance with Refs. [10] and [11].

3.34. Radiation detection instruments can be integrated into operations by equipping officers operating the routine checkpoint with personal radiation detectors and/or by diverting traffic (vehicles or pedestrians) past a vehicle mounted detector. For officers conducting routine vehicle checkpoints using a personal radiation detector, in case of an instrument alarm, officers should follow the established procedures to use the detector to search for the source of radiation, secure the area and notify the shift supervisor to request technical expert support for the identification of the material. For officers conducting routine vehicle checkpoints using a vehicle mounted detector, traffic has to be slowed as it passes through the checkpoint. If an alarm is triggered in the vehicle mounted detector, officers should isolate the vehicle and passengers and use personal radiation detectors or handheld radionuclide identification devices to search for the source of radiation.

3.35. Example scenarios for detection at a routine checkpoint are the following:

- An officer is conducting a routine vehicle checkpoint for narcotics interdiction, observes a suspicious package in the vehicle and on further inspection the officer suspects this to be a radiation source. The officer directs the driver to the secondary inspection location as the driver did not acknowledge having authorization to possess nuclear or other radioactive material. The officer isolates the driver from the vehicle and secures the people and vehicle. Technical expert support is notified to assist in confirmation of the alert and identification of the package contents.
- Mail sent to a State's parliament is routed through a specialized screening facility to scan for nuclear and other radioactive material using fixed radiation portal monitors or radiation conveyor belt monitors. A parcel triggers an instrument alarm. The personnel localize the radiation source to a specific package. Technical expert support is requested to assist in confirmation of the alarm and identification of the package contents.

Detection during routine operations of emergency services

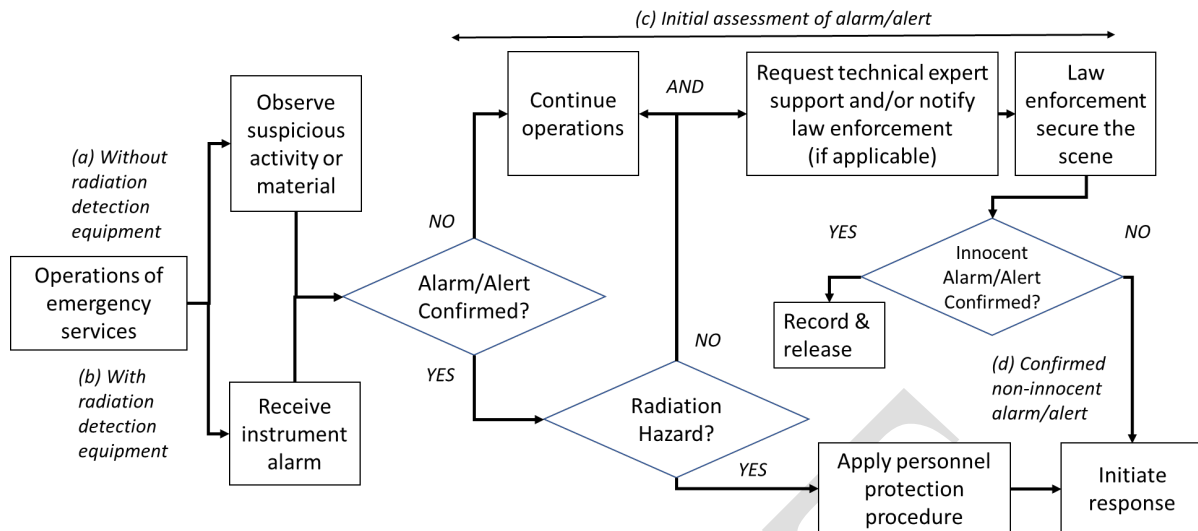


FIG. 3. Example of detection operations during routine operations of emergency services.

3.36. The personnel typically involved in emergency first response operations include law enforcement, fire brigades, specialized response teams and emergency medical services. If personnel are provided with detection equipment, then they should also receive training on the use and basic maintenance of such equipment in advance of deployment with the equipment on patrol.

3.37. Figure 3 shows the actions to be followed during the conduct of their routine duties by the personnel based on whether they have radiation detection equipment as follows:

- (a) If the personnel do not have radiation detection equipment, and they observe suspicious materials or activities that might indicate the presence of nuclear or other radioactive material out of regulatory control, then based on the information available, they should attempt to localize the potential source of the radiation and assess the credibility of the information to confirm the alert.
- (b) If equipped with a personal radiation detector, and the personnel receive an instrument alarm they should confirm the validity of the primary detection to determine whether or not it is a false alarm. They can use the detector to search for the radiation source that caused the alarm.
- (c) If the alarm or alert is confirmed and it is safe to proceed based on all present hazards, the personnel continue their operations while also notifying technical expert support to perform initial assessment of the alarm/alert and law enforcement to secure the scene.
- (d) If it is determined to be a false or innocent alarm, the personnel may record and release the material. If a non-innocent alarm is confirmed the appropriate response organization(s) should be notified, personnel protection for professional area applied, and protective actions and other response actions implemented in accordance with Refs [10] and [11].

3.38. Example scenarios for detection during the routine operations of emergency services are the following:

- A fire brigade inspection team performing a walk-through at a nightclub observes a package with a radiation trefoil. The fire brigade inspection team isolates the package, requests technical expert support and notifies law enforcement using established protocols.
- Fire brigade responds to a fire alarm at a private residence. An instrument alarm is triggered on a firefighter's personal radiation detector indicating the presence of radiation. The firefighter follows the established procedures to use the detector to search for the source of radiation. The firefighters request technical expert support and notify law enforcement.

Detection by information alert obtained from medical surveillance

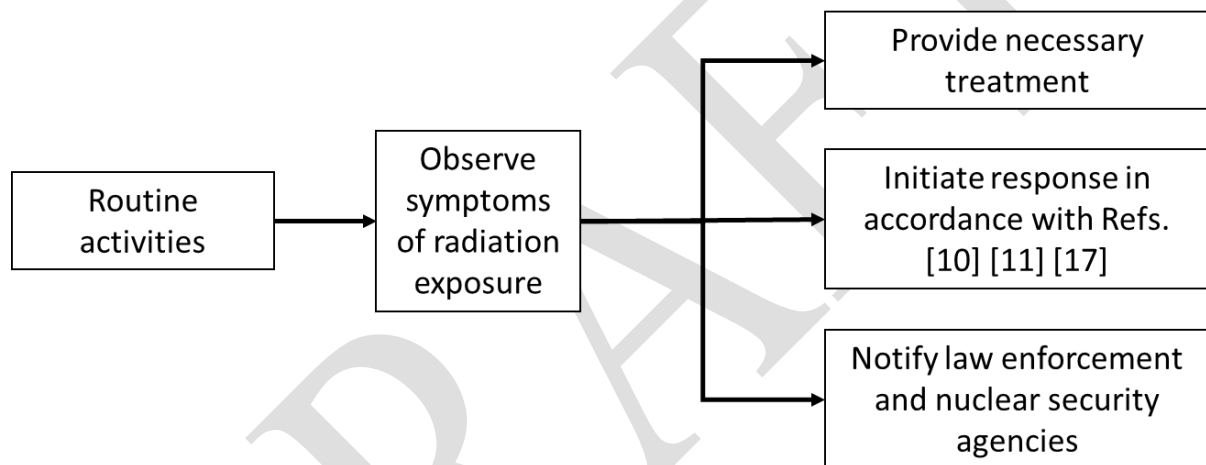


FIG. 4. Example of detection by information alert obtained from medical surveillance.

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

3.40. To generate information alerts and achieve detection of criminal or intentional unauthorized acts involving material out of regulatory control during medical surveillance, the State should ensure that the medical personnel has received appropriate training to identify radiation injuries or illness as outlined in the IAEA Emergency Preparedness and Response (EPR) Series, Generic Procedures for Medical Response During a Nuclear or Radiological Emergency [17] and Ref. [11]. In case the origin of the radiation cannot be identified or is suspicious, then law enforcement should be informed in addition to other appropriate competent authorities as defined in Ref. [17]. In this circumstance hospitals, clinics or other health authorities should establish a process for additionally notifying nuclear security agencies. States may decide to use existing notification mechanisms, including as outlined Ref.

[17], or create a dedicated communication channel and standard operating procedures specific to notification directly to law enforcement of a potential nuclear security event. Nuclear security agencies, based on the information received, may inform medical personnel about the need to consider further steps as new information is gleaned. Further details on information sharing with regard to information alerts obtained from medical surveillance is provided in Annex III.

3.41. Figure 4 shows the actions to be followed by the medical personnel if during the conduct of their routine duties, they observe symptoms of acute radiation exposure or become aware of suspicious activity that might may be linked to the exposure of the patient to nuclear or other radioactive material. The medical personnel should use established procedures to notify law enforcement, while also providing necessary treatment in line with Ref. [17].

3.42. An example scenario for detection by information alert obtained from medical surveillance is the following: The medical team identifies a patient with symptoms consistent with radiation exposure but the patient has no reason for contact with nuclear or other radioactive material and exhibits suspicious behaviour when asked about potential exposure. The medical team isolates the patient and checks for potential radioactive contamination. The patient is put under medical control for receiving medical treatment. The doctors follow the established notification procedures, including to inform law enforcement.

Detection by information alert obtained from public reporting

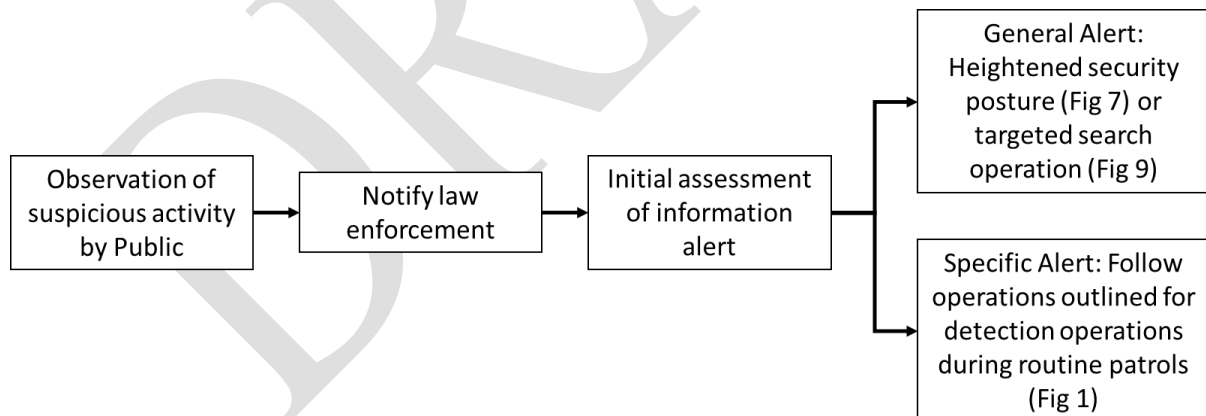


FIG. 5. Example of detection by information alert obtained from public reporting.

3.43. The typical personnel involved in detection by information alert obtained from public reporting include law enforcement or private stakeholders, such as private site security contractors.

3.44. To generate information alerts and achieve detection of criminal or intentional unauthorized acts involving material out of regulatory control from public reporting, the State should establish a process

for the authorities to receive notifications from members of the public, such as a reporting hotline. Established public security awareness raising channels can be leveraged.

3.45. Figure 5 shows the actions to be followed if the public observes or becomes aware of any suspicious activity that might indicate the presence of nuclear or other radioactive material out of regulatory control. The public should notify law enforcement using established procedures. Law enforcement then initiates existing procedures for initial assessment of an information alert. Depending on the initial assessment of the information, this could result in a heightened security posture (paras. 3.50-53), targeted search operations (paras. 3.58-63), or if potential radioactive or nuclear material out of regulatory control is present follow detection operations during routine patrols for initial assessment of the alert (paras. 3.24-28).

3.46. An example scenario for detection by information alert from public reporting would be: A commuter observes a suspicious package on the train platform and reports this to the local transport police. The transport police arrive to inspect the package and observe radiation symbols on the packaging, or if equipped with personal radiation detectors receive an instrument alarm. The officer secures the package and requests technical expert support.

Detection by information alert obtained during law enforcement investigation

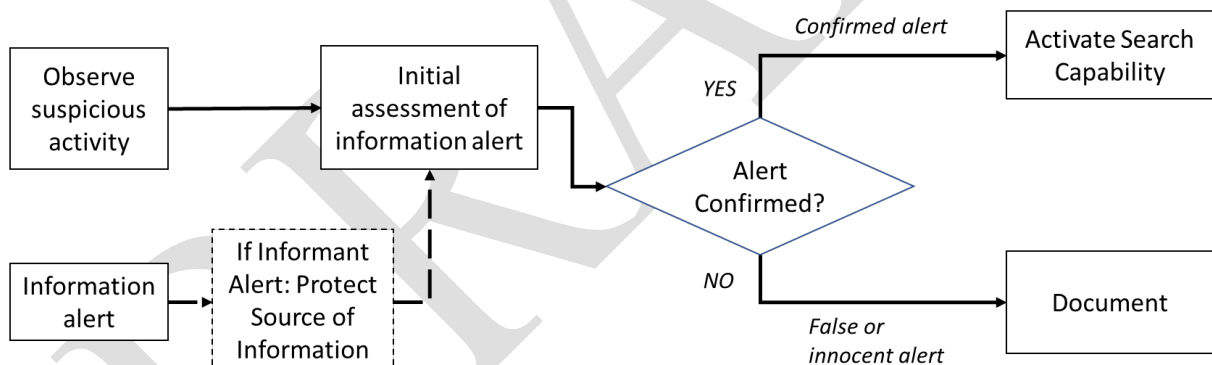


FIG. 6. Example of detection by information alert obtained from law enforcement investigation.

3.47. Law enforcement should establish procedures for initiating the search for nuclear and other radioactive material out of regulatory control and requesting technical expert support based on information alerts, investigative leads or other information gained during the course of regular law enforcement investigation activities. The law enforcement personnel should be able to assess the credibility and source of this information in a timely manner.

3.48. Figure 6 shows the actions to be followed by the personnel if during a routine investigation, they observe or become aware of suspicious activity that might indicate nuclear or other radioactive material are out of regulatory control. The personnel should perform an initial assessment of the credibility of

the information alert to confirm the alert. If the alert is deemed credible and confirmed, personnel should initiate the established procedures to search for nuclear or other radioactive material. It is important that personnel protect the source of information that generates the information alert in accordance with established procedures. This information can be obtained through sensitive means, such as an informant or as part of activities gathering evidence for use in criminal proceedings. The steps to be followed during a targeted search are described in paras 3.58-3.63.

3.49. Example scenarios for detection by information alert during a law enforcement investigation are the following:

- A confidential source provides information related to the location of a stolen ⁶⁰Co source. The law enforcement officer assesses this information to be credible. Law enforcement initiates the search for the radioactive material.
- Law enforcement officers are surveilling a tobacco smuggling operation. During the course of the investigation, the officers set up a telephone intercept operation. While monitoring, the officers hear a discussion on planning for an attack using a radiological dispersal device. The officers assess this information to be credible and notify the specialized operational unit of the need for a targeted search operation.

SPECIAL CONSIDERATIONS FOR DETECTION DURING ENHANCED OPERATIONS

Detection operations during a heightened security posture



FIG. 7. Example of detection operations during a heightened security posture.

3.50. The personnel typically involved in detection operations during heightened security posture include law enforcement, security agencies, defence forces, and technical expert support.

3.51. Operational plans for enhanced operations should be developed in advance based on risk-informed scenarios and should be adapted to the actual situation leading to the heightened security posture. The planners of the detection operations should consider the advantages and disadvantages of overt and covert operations for the detection of nuclear or other radioactive material out of regulatory control and the scope of the heightened security posture, including defining the location and timeframe. The planners should take into consideration that States do not generally want to remain in a heightened security posture for an extended period of time due to the increased resource demand for sustaining such operations.

3.52. Figure 7 shows the actions to be followed for detection during a heightened security posture as the result of a general alert. The authorities tailor pre-existing operational plans for enhanced operations and deploy additional resources as dictated by the plan. These resources could include deployment of additional patrols and/or checkpoints where the personnel conduct operations according to their assigned duties (see paras 3.24-3.35) and/or deployment of roving patrols of specially trained teams with backpack-based radiation detection systems or vehicle mounted or airborne radiation detection systems.

3.53. An example scenario for enhanced detection operations during a heightened security posture is the following: After credible but unspecific threat information of illicit use of radioactive or nuclear material is made against a country, the national threat level is raised. No specific material or suspect is identified, but security organizations are instructed to heighten the security posture around potential targets, transit pathways, and locations with radioactive and nuclear material for a defined time period. Security organizations develop an operational plan in cooperation with technical experts to deploy additional radiation detection capabilities.

Enhanced detection operations during a high profile event

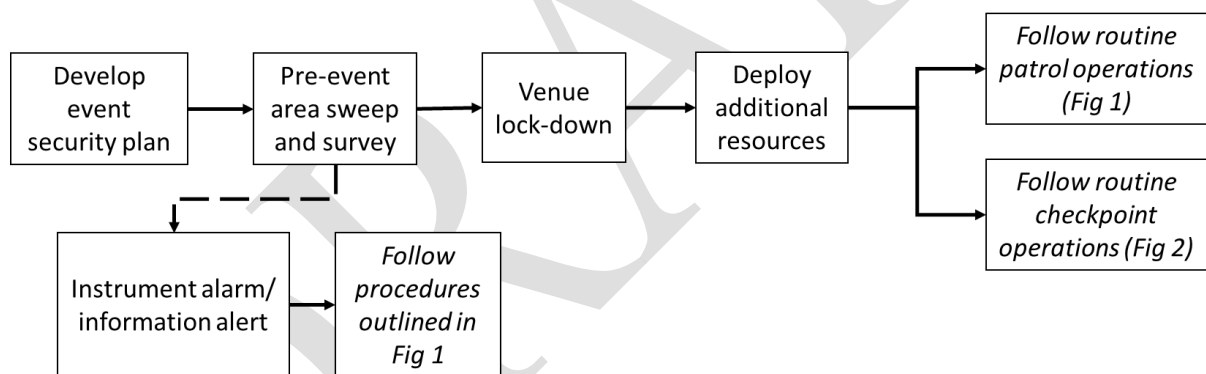


FIG. 8. Example of enhanced detection operations during a high-profile event.

3.54. The personnel typically involved in securing a high profile event could include law enforcement, the gendarmerie, security agencies, explosive ordnance disposal teams, defence forces and private stakeholders, such as private site security contractors for venue security or VIP protection.

3.55. The detection plan for a high profile event should be developed in advance of the event in consultation with all relevant stakeholders and should be integrated into the overall security plan. Planners should consider utilization of both overt and discreet detection operations to develop a defence in depth strategy. They should also consider the scope of the event, the location and timeframe.

3.56. Figure 8 shows the steps to be followed to secure the event and enable the implementation of radiation detection measures. The personnel should conduct an area sweep and a radiation survey before

the commencement of the event in conjunction with other security sweeps (i.e. explosives sweeps). This helps determine the background, any locations with elevated radiation levels, or any existing threats in the area where the event is scheduled to take place and can be done using backpack-based detectors, handheld gamma and/or neutron survey meters, or handheld radionuclide identification devices. After the sweeps and surveys have been concluded, the personnel should secure the venue and establish perimeter security (venue lock-down). The responsible authorities should deploy additional resources, such as routine patrols (Fig. 1) and checkpoints (Fig. 2), for the detection of nuclear and other radioactive material out of regulatory control, in accordance with pre-established processes. The authorities might also choose to raise the security posture (Fig. 7) for the duration of the event in a specified area. If during the pre-event area sweep, or at any other time during the public event, the personnel receive an instrument alarm or information alert then they should follow pre-established procedures for the timely adjudication and confirmation of that alarm or alert (in accordance with Figs. 1 and 2).

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

SPECIAL CONSIDERATIONS FOR DETECTION DURING TARGETED OR SPECIFIC OPERATIONS

Targeted search operations

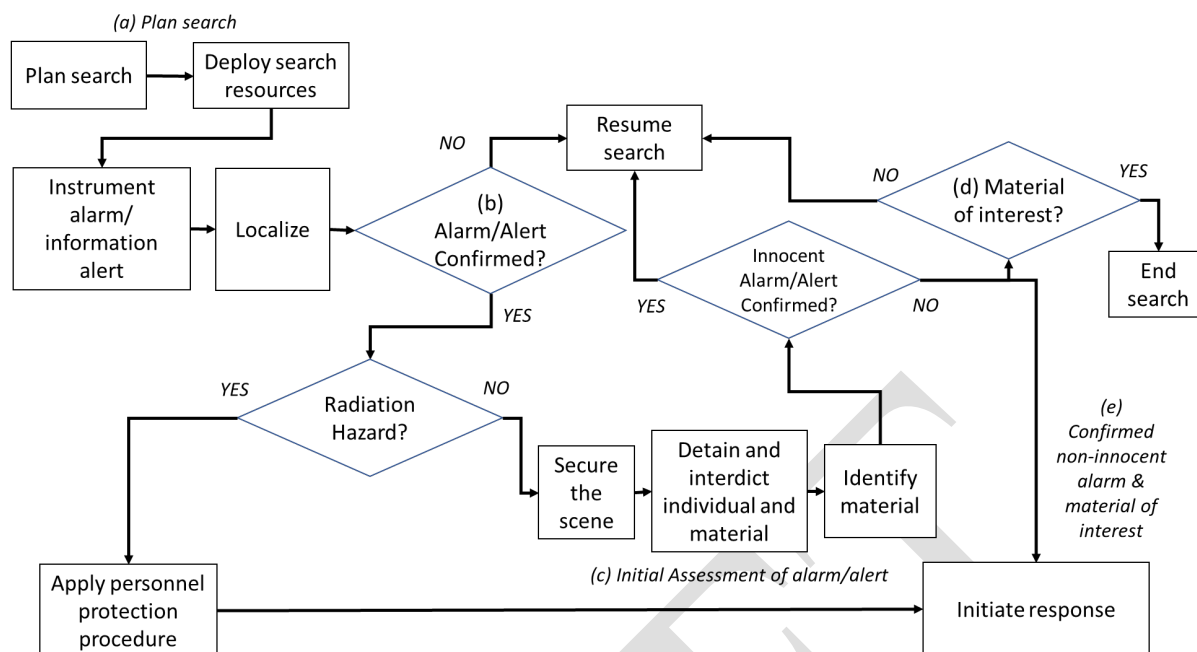


FIG. 9. Example of detection operations during targeted search.

3.58. The personnel typically involved in targeted search operations include law enforcement, security agencies, defence forces, and technical support organizations.

3.59. The personnel should obtain legal authority to conduct a search for nuclear or other radioactive material out of regulatory control in accordance with national legislation and regulations.

3.60. The plan for the search should take into consideration the advantages and disadvantages of overt and discreet detection methods, and which entity has the authority and the jurisdiction to conduct the search at a given location within the State. The plan should include provisions for selecting the appropriate type of equipment for the detection of the material at the given location.

3.61. Personnel should have access to, and training on the use of, equipment and resources used during the search, such as handheld or backpack detectors, radionuclide identification devices, vehicle mounted radiation detection systems. Planners and personnel should understand the functions and limitations of each type of equipment. Pre-established processes for initiating, as appropriate, the local or national response plans, which would cover nuclear security measures and emergency response actions, should be in place.

3.62. Figure 9 shows the actions to be followed to implement detection operations for targeted search as follows:

- (a) The planning process begins with determination of the search scope, discrete reconnaissance and surveillance of the intended search location, coordination with other competent authorities, and identification of necessary resources specific to the material for which they are searching.

1 Planners can request consultation with technical experts to determine optimal search techniques
2 and equipment selection. The personnel should then deploy resources in accordance with the
3 search plan and use the available equipment to detect the nuclear or other radioactive material
4 out of regulatory control. Depending on the material of interest and area to be searched radiation
5 detection equipment of use in conducting a search can include: personal radiation detectors;
6 handheld gamma and/or neutron survey meters; backpack-based radiation detection systems;
7 and vehicle mounted, airborne or maritime radiation detection systems.

8 (b) If during the course of the search an instrument alarm or information alert indicates the potential
9 presence of radiation, the personnel should follow the operating procedures for initial
10 alarm/alert assessment, including to localize the source of radiation and confirm the validity of
11 the information alert or primary detection to determine whether or not it is a false alarm.

12 (c) If the alarm or alert is confirmed and it has been determined that there is no radiation hazard,
13 the personnel should proceed to initial assessment of the alarm/alert, including to secure the
14 scene. This might include separating or isolating any individuals present at the scene from
15 materials or property, and the detention and interdiction of the suspect material and the
16 individuals. Initial identification can be performed using handheld radionuclide identification
17 devices.

18 (d) Technical expert support should be activated to identify if the material found matches the
19 description of the material of interest. If not, the found material should be securely stored, the
20 incident documented, and the search continued.

21 (e) If it is determined to be a false or innocent alarm, the personnel may record and release any
22 present material. If a non-innocent alarm is confirmed the appropriate response organization(s)
23 should be notified, personnel protection for professional area applied, and protective actions
24 and other response actions implemented in accordance with Refs [10] and [11].

25 3.63. An example scenario for search operations is the following: The authorized carrier for the
26 transport of a disused ⁶⁰Co radioactive source reports the theft of the source to the regulatory body.
27 Based on law enforcement information, a likely area for the missing source is identified. A search team
28 is assembled and deployed with radiation detection equipment. The search team locates and identifies
29 the radioactive source. The scene is secured and processed as a radiological crime scene. The radioactive
30 material is recovered and transported to a secure storage location.

31 **Detection by information alert obtained from undercover operations**

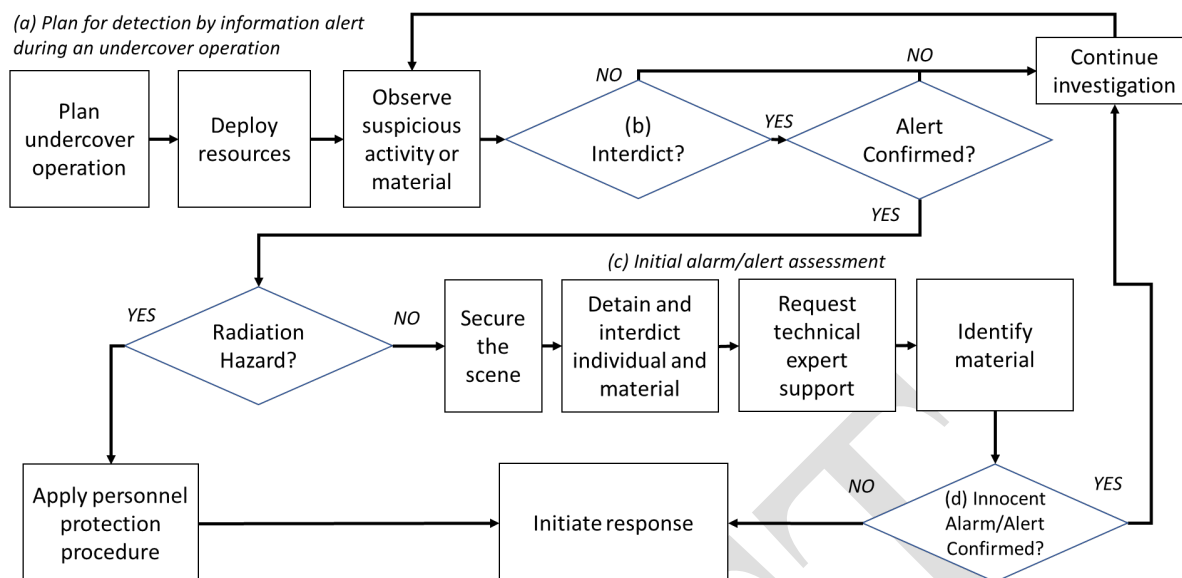


FIG. 10. Example of detection by information alert obtained from undercover operations.

3.64. The typical personnel involved in detection by information alert obtained from undercover operations include law enforcement, security agencies, and technical expert support.

3.65. Planners should be aware of which competent authority is allowed to conduct an undercover operation. Before engaging in undercover detection operations, the personnel should obtain the authority to conduct an undercover operation in accordance with existing legal procedures.

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

3.67. Fig. 10 shows the actions to be followed for detection by information alert obtained during the conduct of the undercover operations.

(a) The plan should include determination of the scope of the operations, reconnaissance of the location, coordination with other competent authorities, and identification of necessary resources. The personnel should deploy resources in accordance with the operational plan.

(b) If suspicious activity or material is observed, the personnel should use techniques and information available to confirm the presence of nuclear or other radioactive material. This can be a visual confirmation as radiation detection equipment might not be viable for the operations. The personnel should decide to either interdict the suspicious material or continue with the investigation until more evidence can be collected and alarm/alert confirmed.

(c) If the material is interdicted and the alarm or alert is confirmed, and it has been determined that there is no radiation hazard, the personnel proceed to initial assessment of the alarm/alert, including to secure the scene. The personnel then contact technical expert support for radionuclide identification and to confirm whether it is a non-innocent alarm.

(d) If it is determined to be a false or innocent alarm, the personnel may resume their patrol. If a non-innocent alarm is confirmed the appropriate response organization(s) should be notified, personnel protection procedure for professional area applied, and protective actions and other response actions implemented in accordance with Refs [10] and [11].

3.68. Common undercover operations that can be used for the detection of nuclear and other radioactive material out of regulatory control include sting operations⁵, buy-bust⁶ and controlled delivery⁷.

4. ROLE OF INFORMATION FOR DETECTION OPERATIONS IN THE INTERIOR

4.1. Information has an essential role in the planning and conduct of detection operations in the interior. Ref. [3] states that “An information alert, possibly indicating a nuclear security event, may come from a variety of sources, including operational information, medical surveillance and border monitoring and with a follow-up assessment may lead to detection.”

4.2. Effective information collection, analysis, and dissemination processes should be used to determine the most effective manner of deploying detection resources. Effective information management systems can address the challenge presented by covering a vast interior area with numerous potential targets by informing the prioritization of where, when, and how to conduct detection operations in the interior.

4.3. According to Security of Nuclear Information (NSS No. 23-G) [18], “State policy on the security of information should define which type of information the State wishes to be secured and indicate how that security is to be applied.” These information security policies and protocols should be incorporated

⁵ Sting operations are deceptive actions designed to catch a person committing a crime. A typical sting operation will have an undercover law enforcement officer play a role as a criminal partner or potential victim and go along with a suspect's actions to gather evidence of the perpetrator's illegal activity.

⁶ Buy-bust is a type of undercover operation including the controlled purchase of illicit material by undercover law enforcement officers from the perpetrator. After the controlled purchase the perpetrator is detained, and the material is confiscated.

⁷ Controlled delivery is used when a consignment of illicit radioactive material is detected and allowed to go forward under the control and surveillance of law enforcement officers in order to secure evidence against the organizers of the criminal activity.

into the organizational level processes and joint agency detection operations plan for nuclear and other radioactive material out of regulatory control (Annex 1).

4.4. The general process for collecting, processing, disseminating, and using information to inform nuclear security detection operations is outlined in paras 4.5-4.18 and depicted in Fig. 12. Competent authorities and other stakeholders in the interior collect information from all available open and closed sources of information. This raw data should then be analysed, which includes sorting, evaluating and interpreting the information to produce an analytical report of key findings relevant to detection operations in the interior. These analytical reports should be disseminated to relevant competent authorities and other stakeholders to inform the planning, implementation, and evaluation of detection operations in the interior.

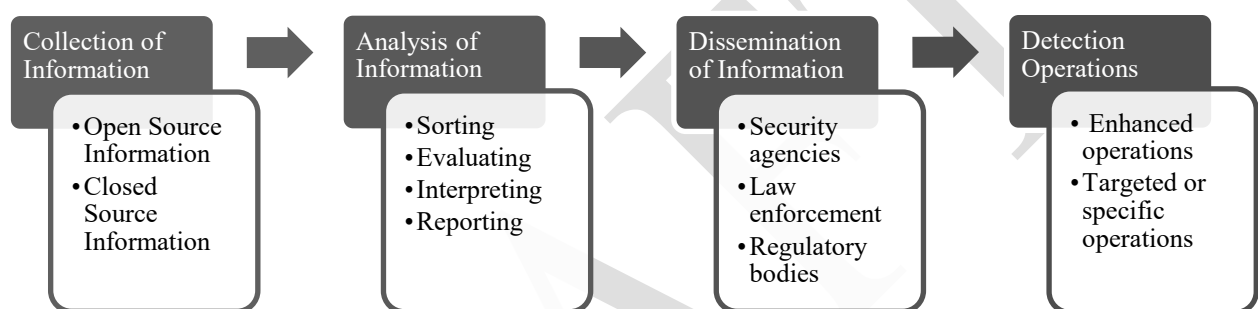


Fig. 12. Process for handling information related to the detection of criminal or intentional unauthorized acts involving nuclear and other radioactive material out of regulatory control in the State's interior.

COLLECTION OF INFORMATION

4.5. Competent authorities can choose to collect or receive information from 'open sources' and from 'closed sources.' Open sources contain publicly available information, (e.g. media, published materials). Closed sources refer to information that is not publicly available and is generated by the authorities. These can include criminal records, reports of loss of regulatory control, analytical reports and intelligence gathering activities.

4.6. Information sources can be both national and international. National information sources include interagency working groups (at both the strategic level and operational levels), formal reporting procedures and existing cooperation mechanisms between different competent authorities. International information sources include any source of information received from an entity located outside of a State, such as: the IAEA's Incident and Trafficking Database (ITDB), IAEA's Unified System for Information Exchange in Incidents and Emergencies (USIE), information from the International Criminal Police

Organization (INTERPOL), regional information exchange networks, and information exchange with neighbouring countries on a bilateral basis according to cooperation agreements.

4.7. The types of information of interest for collection to assist competent authorities to design, implement, and conduct effective detection operations in the interior include: operational information, medical surveillance, reports of regulatory non-compliances and reports of loss of regulatory control, information from the public and other external sources that can also lead to the decision to raise the security posture or heighten alert

4.8. Operational information providing awareness of the presence of authorized nuclear or other radioactive material in the area of responsibility of a competent authority or other stakeholder can inform the planning and implementation of detection operations in a State's interior. Competent authorities should share with authorized personnel in security organizations relevant information, on a need to know basis, from the national radioactive source inventory as this will assist in developing a common operating picture. Information on the types and locations of nuclear and other radioactive material present in a State's interior can assist in selecting the equipment and tactics to be used in detection operations. This information can include the types of radionuclide, activity, expected dose rates, physical characteristics, or additional information about the radioactive source, such as the type, model, packaging, and labelling.

4.9. Operational information on potential adversaries in a State's interior can also inform the planning and implementation of detection operations in the interior. Investigative leads or information from other law enforcement activities could result in information alerts or to the conduct of detection operations for material out of regulatory control. Information related to other hazards relevant in planning and conducting detection operations in a State's interior might include the presence of armed adversaries, explosives, or flammable chemicals.

4.10. Prompt notification of missing, lost, or stolen nuclear or other radioactive material by licensees can inform targeted search operations. Often the regulatory body might be the first organization to receive such information, but should have protocols in place to quickly notify relevant security organizations who can implement the dictated search operations (see Ref. [2] for more information on reports of regulatory non-compliances and reports of loss of regulatory control).

4.11. Information from medical services and health authorities on any suspected radiation injuries or casualties might indicate the occurrence of a nuclear security event. For information alerts obtained from medical surveillance a State should define the procedures between the law enforcement and public health authorities on how to share sensitive information on medical data in a protected way. More information on the management of information alerts obtained from medical surveillance is presented in Annex III.

4.12. Competent authorities might receive information from the public indicating a threat, suspicious activity or abnormal situation involving nuclear or other radioactive material. The law enforcement and security agencies should establish an outreach programme with industry, academia, or other licensees of nuclear or other radioactive material to promote working relationships and situational awareness among the authorities and other stakeholders. A potential threat perceived and communicated by the industry or the academia could enable law enforcement to tailor detection operations and to address the threat. The monitoring of all source information, including open sources such as social networks, dark web and encrypted mails can also provide information to inform the planning and targeting of detection operations in the interior.

ANALYSIS OF INFORMATION AND DATA

4.13. The analysis of information is a key step in making it useful to direct planning and implementation of detection operations in the interior. Many competent authorities and stakeholders with traditional security mandates have their own internal information collection and analysis processes that encompass the four steps in the analysis of information: sorting, evaluating, interpreting and reporting. The information analysis process for nuclear security detection in a State's interior demands multi-agency cooperation as it relies on the information collection capability, expertise and experience from a wide variety of State organizations, including law enforcement, intelligence agencies, regulatory bodies and technical support organizations. Subject matter experts on nuclear and other radioactive material should be involved or consulted as part of the information analysis process because law enforcement and national security organizations might lack technical knowledge on nuclear and other radioactive material.

4.14. The analysis process compiles the collected raw information into an analytic report that can be used by relevant competent authorities and stakeholders to plan and implement detection operations in a State's interior. Although the quantity of available information might be vast and continually updated, personnel who perform this analysis often face time restrictions in delivering the relevant outcome of the analysis to operational organizations.

DISSEMINATION OF INFORMATION

4.15. Analytic reports on nuclear security should be disseminated to relevant stakeholders on a need-to-know basis. Through information exchange among relevant competent authorities and other stakeholders the multi-agency information analysis process can build on, and be made complementary to, existing information collection and analysis processes. Secure dissemination of the analytical report should be done in accordance with existing policies and procedures. Information sharing can also extend to competent authorities and other stakeholders operating at different pathway layers of the detection

architecture, including the State's borders and the exterior of the State, as a nuclear security event can move through several pathway layers.

4.16. The collection, analysis and distribution of information enables competent authorities to identify and prioritize strategic locations and pathways for the conduct of detection operations in the interior.

4.17. Detection operations in the interior should be implemented using a graded approach based on updates to the threat and risk assessment driven by the analysis of information relevant to nuclear security. More specifically, when no specific threat has been identified, routine operations can be implemented; when the information analysis results in the identification of elevated risk, enhanced operations can be planned and implemented; when a specific threat has been detected by information alert or instrument alarm, targeted or specific operations can be planned and implemented.

5. ROLE OF EQUIPMENT FOR DETECTION IN THE INTERIOR

5.1. The detection of a potential nuclear security event in the interior can occur by an information alert or an instrument alarm. Radiation detection instruments should be used to confirm the presence of nuclear or other radioactive material out of regulatory control. This confirmation can be conducted using a single type of radiation detection equipment or a combination of different types, especially for performing initial assessment, alarm adjudication and identification.

5.2. Instrument alarms can come from a wide variety of radiation detection instruments. Annex I presents some types of equipment that are typically used for radiation detection in the interior of a State. Some are small enough to be worn (personal radiation detectors), some are handheld or worn as a backpack, and some are vehicle-based. They also differ by function: some are used to detect radiation from radioactive material, some are used to locate the material more precisely after detection of the radiation, and some are used to identify radionuclides.

5.3. According to *Functional Specifications for Nuclear Security Detection Equipment and Systems* (IAEA Nuclear Security Series No. 1) [19], the choice of the most appropriate type of detection instruments for any given operation should be determined by environmental conditions and the likely scenarios identified through the threat and risks assessment, including the type of material of concern, the material's signature and likely adversary tactics. Ref. [19] further indicates that detection instruments can be used to survey, generate instrument alarms, search and localize (i.e. initial alarm assessment), or identify radionuclides.

INSTRUMENT DEPLOYMENT PLAN FOR DETECTION IN THE INTERIOR AND EQUIPMENT SELECTION

5.4. Ref. [3] states that “Based on the detection strategy and within the framework of the national nuclear security detection architecture, the competent authorities could prepare an instrument deployment plan(s) based upon the assessed threat of criminal or intentional unauthorized acts involving nuclear or other radioactive material out of regulatory control.” The plan should specify the number and type of instruments to be deployed, location of instruments to be deployed while considering the instruments life cycle across acquisition, maintenance calibration replacement, including the personnel and resources needed to operate the instruments alarm assessment and adjudication procedures SOPs.

5.5. The instrument deployment plan should be developed under a holistic approach encompassing both detection at State borders and in a State’s interior to ensure the equipment needs of all the competent authorities are met and to support a functional nuclear security detection architecture. Developing the instrument deployment plan should be a multi-agency activity involving all relevant competent authorities and other stakeholders involved in the national nuclear security detection architecture. This multi-agency activity should account for the individual organizational and collective needs that best meet the goals of the detection strategy at the national and operational levels. A coordinated plan for selecting and deploying equipment allows States to avoid wasting resources by procuring redundant or non-applicable equipment and carefully weighing trade-offs between cost and desired capabilities to best counter identified risks.

5.6. Ref. [3] recommends that consideration should be given in the instrument deployment plan to “Monitoring for radiation inside the country and searching for nuclear and other radioactive material out of regulatory control.” Monitoring can include results from recent background radiation surveys accumulated through interior detection operations. The identification of locations with elevated radiation hotspots levels can help operational teams in the interpretation of field measurements and in alarm adjudication. Section 3 outlines the types of equipment that may be of use in supporting each type of detection operation in the interior, including targeted search operations. The interior component of the instrument deployment plan should include radiation detection instruments, complementary detection technology, any other supporting capabilities and infrastructure to support all the operations outlined in section 3. For further information on the components of a detection instrument deployment plan see Ref. [3].

5.7. Ref. [7] outlines the following equipment procurement considerations related to equipment functionality that are applicable both to detection at State Borders as well as in a State’s interior: “ability of the equipment (including associated computer hardware and software) to support the concept of operations and the design; ability to detect and measure radiation levels associated with materials of

1 concern for nuclear security; ability to identify such materials; reliability (ability to consistently perform
2 adequately) under expected environmental conditions at the detection location; compatibility with
3 existing equipment; ability to meet the specifications for the display, storage and retention of data; ease
4 and reliability of calibration; certification as qualified equipment for the intended purpose; training
5 needs for operator; and general ease of use.”

6 5.8. The choice of radiation detection equipment for deployment in a State’s interior should
7 additionally address the specific interior challenges outlined in paras 2.11-2.20. Performing detection
8 to cover the potential adversary pathways that have the highest risk across a large area or types of
9 domains can be best achieved by using mobile and/or portable, durable and versatile equipment.
10 Consideration of these factors in the planning and acquisition phase will help to optimize performance
11 of detection equipment during operations.

12 5.9. Planners should know the capabilities and limitations of chosen equipment, including its
13 sensitivity, size and durability, to understand how to most effectively incorporate the detection
14 instruments into operational plans and procedures.

15 5.10. The deployment plan should consider the appropriate combination of detection equipment to
16 meet operational needs.

17 OPERATION OF RADIATION DETECTION EQUIPMENT

18 5.11. Ref. [3] states that “Technical support should be available for assessing alarms and assisting in
19 the initial assessment activities. Technical support in the form of expert support teams should include
20 persons equipped and trained to use basic radiation monitoring instruments for categorization of
21 radioactive material and to perform radiation protection tasks.”

22 5.12. During the initial assessment of an instrument alarm or an information alert, it is crucial to
23 conduct measurements with radiation detection equipment to decide whether the alert or alarm is
24 innocent (in which case the incident should be recorded and the material released) or whether the
25 presence of material out of regulatory control is confirmed, that might lead to the declaration of a
26 nuclear security event.

27 5.13. The State should consider the response times needed by technical expert support teams to be
28 deployed in the field to support various types of detection operations. States should take into
29 consideration that these operations could be taking place at any location within the State’s interior.
30 These team(s) should have adequate training and equipment to identify the suspect material within the
31 timeframe that personnel may legally detain suspects and material.

32 **Complementary technology**

1 5.14. In addition to radiation detection instruments, the detection of criminal or intentional
2 unauthorized acts involving nuclear or other radioactive material out of regulatory control in a State's
3 interior can be complemented by other security technologies. Competent authorities and other
4 stakeholders operating in the State's interior often deploy or have access to the following technologies:

- 5 • Equipment for detection of explosives (trace or volume): This is a classical tool for examination
6 of suspicious content and in combination with radiation detection equipment can confirm the
7 presence or absence of a radiological dispersal device;
- 8 • Classic security monitoring equipment (surveillance cameras, closed-circuit television): This
9 equipment provides real time information that can support detection operations in the interior
10 and can serve for automatic license plate recognition, face recognition, perimeter security, and
11 tracking adversary movement;
- 12 • Metal detectors: These detectors can detect the presence of shielding or suspicious metal
13 objects;
- 14 • Non-intrusive equipment: This equipment can be used for the inspection of people or goods.
- 15 • Global Positioning System (GPS) equipment and software: This can help map areas that have
16 been surveyed and record background radiation measurements.

17 5.15. The interaction and interoperability of radiation detection equipment with other security
18 technologies should be considered when implementing detection operations in a State's interior. They
19 should consider integrating the information generated by these complementary technologies into their
20 detection strategy. Competent authorities and other stakeholders should consider methods or processes
21 for cross-referencing and/or processing data coming from different systems.

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] 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 AND WORLD CUSTOMS ORGANIZATION, Nuclear Security Recommendations on Nuclear and Other Radioactive Material out of Regulatory Control, IAEA Nuclear Security Series No. 15, IAEA, Vienna (2011).
- [3] INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Systems and Measures for Detection of Nuclear and other Radioactive Material out of Regulatory Control, IAEA Nuclear Security Series No. 21, IAEA, Vienna (2012).
- [4] INTERNATIONAL ATOMIC ENERGY AGENCY, Risk Informed Approach for Nuclear Security Measures for Nuclear and Other Radioactive Material out of Regulatory Control, IAEA Nuclear Security Series No. 24-G, IAEA, Vienna (2015).
- [5] INTERNATIONAL ATOMIC ENERGY AGENCY, Planning and Organizing Nuclear Security Systems and Measures for Nuclear and Other Radioactive Material out of Regulatory Control, IAEA Nuclear Security Series No. 34-T, IAEA, Vienna (2019).
- [6] INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Systems and Measures for Major Public Events, IAEA Nuclear Security Series No. 18, IAEA, Vienna (2012).
- [7] INTERNATIONAL ATOMIC ENERGY AGENCY, Detection at a State's Border of Nuclear and Other Radioactive Material out of Regulatory Control, Technical Guidance to be published (NST016).
- [8] INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5), IAEA Nuclear Security Series No. 13, IAEA, Vienna (2011).

- [9] INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Recommendations on Radioactive Material and Associated Facilities, IAEA Nuclear Security Series No. 14, IAEA, Vienna (2011).
- [10] INTERNATIONAL ATOMIC ENERGY AGENCY, Developing a National Framework for Managing the Response to Nuclear Security Events, IAEA Nuclear Security Series No. 37-G, IAEA, Vienna (2020).
- [11] FOOD AND AGRICULTURE ORGANIZATION OF THE UNITED NATIONS, INTERNATIONAL ATOMIC ENERGY AGENCY, INTERNATIONAL CIVIL AVIATION ORGANIZATION, INTERNATIONAL LABOUR ORGANIZATION, INTERNATIONAL MARITIME ORGANIZATION, INTERPOL, OECD NUCLEAR ENERGY AGENCY, PAN AMERICAN HEALTH ORGANIZATION, PREPARATORY COMMISSION FOR THE COMPREHENSIVE NUCLEAR-TEST-BAN TREATY ORGANIZATION, UNITED NATIONS ENVIRONMENT PROGRAMME, UNITED NATIONS OFFICE FOR THE COORDINATION OF HUMANITARIAN AFFAIRS, WORLD HEALTH ORGANIZATION, WORLD METEOROLOGICAL ORGANIZATION, Preparedness and Response for a Nuclear or Radiological Emergency, IAEA Safety Standards Series No. GSR Part 7, IAEA, Vienna (2015).
- [12] INTERNATIONAL ATOMIC ENERGY AGENCY, Manual for First Responders to a Radiological Emergency, IAEA Emergency Preparedness and Response Series EPR-First Responders, IAEA, Vienna (2006).
- [13] INTERNATIONAL ATOMIC ENERGY AGENCY, Developing Regulations and Associated Administrative Measures for Nuclear Security, IAEA Nuclear Security Series No. 29-G, IAEA, Vienna (2018).
- [14] INTERNATIONAL ATOMIC ENERGY AGENCY, Sustaining a Nuclear Security Regime, IAEA Nuclear Security Series No. 30-G, IAEA, Vienna (2018).
- [15] INTERNATIONAL ATOMIC ENERGY AGENCY, Building Capacity for Nuclear Security, IAEA Nuclear Security Series No. 31-G, Vienna (2018)

- [16] INTERNATIONAL ATOMIC ENERGY AGENCY, Preparation, Conduct and Evaluation of Exercises for Detection of and Response to Acts Involving Nuclear and Other Radioactive Materials out of Regulatory Control, Nuclear Security Series No. 41-T, Vienna (2020).
- [17] INTERNATIONAL ATOMIC ENERGY AGENCY, WORLD HEALTH ORGANIZATION, Generic Procedures for Medical Response During a Nuclear or Radiological Emergency, IAEA Emergency Preparedness and Response Series EPR-Medical, IAEA, Vienna (2005).
- [18] INTERNATIONAL ATOMIC ENERGY AGENCY, Security of Nuclear Information, IAEA Nuclear Security Series No. 23-G, IAEA, Vienna (2015).
- [19] INTERNATIONAL ATOMIC ENERGY AGENCY, Technical and Functional Specifications for Border Monitoring Equipment, IAEA Nuclear Security Series No. 1, IAEA, Vienna (2006).
- [20] FOOD AND AGRICULTURE ORGANIZATION OF THE UNITED NATIONS, INTERNATIONAL ATOMIC ENERGY AGENCY, INTERNATIONAL CIVIL AVIATION ORGANIZATION, INTERNATIONAL LABOUR ORGANIZATION, PAN AMERICAN HEALTH ORGANIZATION, WORLD HEALTH ORGANIZATION, Criteria for Use in Preparedness and Response for a Nuclear or Radiological Emergency, IAEA Safety Standards Series No. GSG-2, IAEA, Vienna (2011).

ANNEX I – EQUIPMENT FOR RADIATION DETECTION

I-1. **Personal radiation detectors** are pocket-sized, lightweight radiation detectors, which can be worn on the body for rapid detection of gamma and sometimes neutron radiation. These instruments give an alarm (audible, visual or vibrating) if the measured radiation level exceeds a pre-set threshold, and are generally intended to provide notification of potentially unsafe conditions. They are used to ensure personal safety with little or no intrusion or disruption of activities. They are used primarily by front line officers (e.g. border guards, coastguards, customs officers, law enforcement teams) as they are small, compact, can be operated at extreme and hard environmental conditions, are user friendly, and require minimal training. The wearer should be able to use the detector effectively while performing other tasks. They are the least expensive type of radiation detection equipment but have limited sensitivity.

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

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

I-4. **Backpack-based radiation detection systems** are instruments where the detector (gamma and/or neutron, with/without identification capabilities) and associated electronics are contained in a backpack, in order to be worn by the user for executing discreet searches in public areas. They are particularly useful for radiation surveys of large areas before or during major public events, or for detecting radiation in close proximity, for example while walking down the centre of a passenger train or bus. They may also be used temporarily for area monitoring or may be mounted on a small vehicle. The systems may be equipped with a global positioning system for mapping purposes. Important considerations for their use are weight, ergonomics, battery life and charge time, training time and ease of use and capability for data transmission.

I-5. **Vehicle mounted radiation detection systems** are mobile radiation detection systems that are mounted to or inside a vehicle, and may also be referred to as mobile detection systems. They may be able to measure gamma and/or neutron radiation, and may incorporate identification of gamma-radiation-emitting radionuclides. They may be equipped with a global positioning system and provide search and localization capabilities. Operationally, they may be used in motion or as stationary equipment and they offer increased flexibility.

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

I-7. **Radiation conveyor belt monitors** are portal monitors where the material is put through the detectors in a continuous flow by means of a conveyor drive and are suitable for monitoring large quantities of items. a specific application can be found in monitoring public mail, as parcels and letters are placed on a conveyor belt to detect the presence of gamma and neutron radiation with high sensitivity and may be combined with x ray screening systems.

I-8. **Airborne radiation detection systems** can be mounted inside or outside aircraft, including unmanned aerial vehicles, during operation. They may be used for measurement, detection, and localization of radioactive materials, and data obtained by these systems are typically used for area mapping. They may be able to measure gamma and/or neutron radiation and may incorporate identification of gamma-radiation-emitting radionuclides.

I-9. **Maritime radiation detection systems** can be mounted to or placed inside a maritime vessel. they may be operated in motion or in stationary mode. they may be able to measure gamma and/or neutron radiation, may incorporate identification of gamma-radiation-emitting radionuclides and may be equipped with a global positioning system. they are manufactured for operation in marine environments.

ANNEX II - JOINT AGENCY DETECTION OPERATIONS PLAN FOR MATERIAL OUT OF REGULATORY CONTROL

I-1. To organize nuclear security detection operations across multiple competent authorities in a State's interior, the joint agency detection operations plan for nuclear and other radioactive material out of regulatory control will formalize coordination of agency roles, responsibilities, authorities, and concept of operations. Table I-1 below provides an example of the structure and the main components of a joint agency detection operations plan.

TABLE I-1. EXAMPLE COMPONENTS OF A JOINT AGENCY DETECTION OPERATIONS PLAN FOR MATERIAL OUT OF REGULATORY CONTROL

Section	Purpose
Title Page	Provides title of document, approval date, version number and is signed by representatives of the participating authorities.
Table of Contents	Shows the structure of the plan and provides a quick overview of the plan.
Introduction	Provides the purpose and scope of the plan including the mandate for developing the plan, the participating entities, relevant definitions of terms used in the plan, a list of the associated plans of the participating entities.
Planning Considerations	Describes preparatory activities and the process for assessing priorities for managing potential incidents and nuclear security events. This section also includes: - Identification of potential scenarios for detection in the interior that necessitate joint agency operations, including identification of likely adversaries, tactics, and materials of concern; - Description of resources to be deployed to implement joint operations including number of personnel, equipment, and training requirements; - Identification of legal authority under which joint operations may be conducted; - Identification of funding sources for joint operations.
Coordination and Communication	Describes the chain of command, coordination and communication mechanisms between all participating authorities, including: - Interface with national regulatory body and operators of facilities where nuclear or other radioactive material is used, processed or stored; - Interface with national response agencies to locate and recover nuclear or other radioactive material out of regulatory control; - Interface with competent authorities responsible for nuclear forensics examination;

	iv. Description of information security policies and protocols; v. Public and media communications strategy.
Concept of Operations	Provides a description of the concept of operations and standard operating procedures for potential types of joint operations. The concept of operations generally includes: i. Goals and functional outcomes of the detection process; ii. Existing policies and constraints affecting the operations; iii. Activities and interactions between stakeholders for alarm processing.
Roles and Responsibilities	Describes the roles, responsibilities and areas of jurisdiction for each competent authority involved in each operation. Defines lead agency for each type of joint operation.
Operational Needs	Clarifies the needs for the conduct of operations for detection in the interior and includes: i. Dispute resolution; ii. Joint command structure; iii. Transfer of command; iv. Intelligence activities; v. Detection; vi. Request for response; vii. Information release.
Plan Review and Sustainability	Provides details of mechanism for plan review, maintenance, and sustainability, including: i. Regular time period for conduct of review ii. Regular review and update of risk and threat assessment; iii. Process for agreeing to, documenting and disseminating changes or amendment in the operational needs; iv. Assessment of training and resource requirements, including human and financial; v. Maintenance of equipment; vi. Evaluation of the plan, including joint exercises.
Appendices	Includes relevant items to support the plan including: i. Coordinating or subordinate plans or protocols.

ANNEX III – INFORMATION ALERTS OBTAINED FROM MEDICAL SURVEILLANCE

II-1. Law enforcement and health professionals have access to information that could be shared to prevent or detect criminal or other unauthorized acts with the use of nuclear or other radioactive material out of regulatory control.

II-2. Law enforcement has information about potential incidents involving nuclear or other radioactive material out of regulatory control and should notify hospitals and health emergency services. Raising threat awareness among health professionals will increase the likelihood that they identify signs of suspicious injuries or activity related to a potential nuclear security event.

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

II-4. To allow effective communication of information between law enforcement and health professionals, communication protocols should be developed and communicated to all parties. The establishment of these protocols is essential for the timely exchange of information. The aim is to communicate information at an early stage, if possible before it is established whether an intentional or criminal unauthorized act has taken place. The communication process includes an understanding on both sides of each other's information needs and who receives what kind of information and why.

II-5. Authorities should establish the communication process into a written document enabling information exchange among all entities or parties and ensuring that the process is aligned with national legislation. Information has to be shared on a need to know basis via the predefined and protected communication channels to the recognized points of contact.

II-6. An important consideration when establishing the communication protocols is that medical data is often protected by national legislation as part of patient confidentiality and therefore it constitutes sensitive information. The legislation might include provisions for exemptions allowing law enforcement, prosecutors or security agencies to gain access to the medical data for specific reasons, such as an on-going investigation of a potential nuclear security event, or the protection of the health and safety of the public. However, the legal liability for the release of medical data or patient information without the patient's consent might still be a concern for health professionals.

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