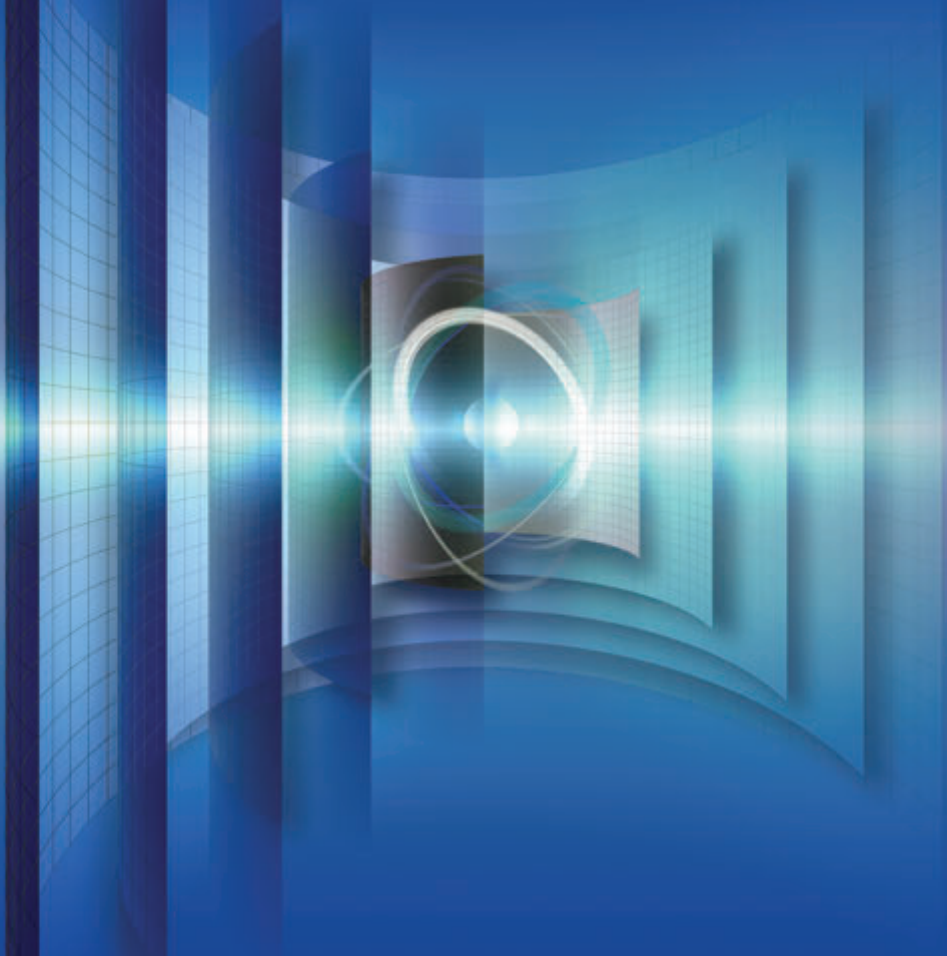
IAEA Nuclear Security Series No. 39-T

Technical Guidance

Developing a Nuclear Security Contingency Plan for Nuclear Facilities



IAEA
International Atomic Energy Agency

IAEA NUCLEAR SECURITY SERIES

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

CATEGORIES IN THE IAEA NUCLEAR SECURITY SERIES

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

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

DRAFTING AND REVIEW

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

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

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

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

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

DEVELOPING A NUCLEAR SECURITY CONTINGENCY PLAN FOR NUCLEAR FACILITIES

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

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

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

IAEA NUCLEAR SECURITY SERIES No. 39-T

DEVELOPING A NUCLEAR SECURITY CONTINGENCY PLAN FOR NUCLEAR FACILITIES

TECHNICAL GUIDANCE

INTERNATIONAL ATOMIC ENERGY AGENCY
VIENNA, 2019

COPYRIGHT NOTICE

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

Printed by the IAEA in Austria
December 2019
STI/PUB/1873

IAEA Library Cataloguing in Publication Data

Names: International Atomic Energy Agency.
Title: Developing a Nuclear Security Contingency Plan for Nuclear Facilities / International Atomic Energy Agency.
Description: Vienna : International Atomic Energy Agency, 2019. | Series: IAEA Nuclear Security Series, ISSN 1816–9317 ; no. 39-T | Includes bibliographical references.
Identifiers: IAEAL 19-01277 | ISBN 978–92–0–105219–3 (paperback : alk. paper)
Subjects: Nuclear facilities. | Nuclear industry — Security measures.
Classification: UDC 341.67 | STI/PUB/1873

FOREWORD

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

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

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

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

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

EDITORIAL NOTE

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

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

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

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

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

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

CONTENTS

1. INTRODUCTION

BACKGROUND

1.1. The IAEA Nuclear Security Series provides guidance for States to assist them in implementing a national nuclear security regime, and in reviewing and strengthening this regime when necessary. The series also provides guidance for States in fulfilling their obligations and commitments with respect to binding and non-binding international instruments.

1.2. The Nuclear Security Fundamentals set out the objective of a nuclear security regime and its essential elements [1]. The Nuclear Security Recommendations indicate what a nuclear security regime should address regarding the following:

(a) Physical protection of nuclear material and nuclear facilities [2];
(b) Radioactive material and associated facilities [3];
(c) Nuclear and other radioactive material out of regulatory control [4].

The Implementing Guide, IAEA Nuclear Security Series No. 27-G, Physical Protection of Nuclear Material and Nuclear Facilities (Implementation of INFCIRC/225/Revision 5) [5] provides more detailed information on the implementation of the recommendations on the physical protection[1] of nuclear material and nuclear facilities [2]. This Technical Guidance publication supplements Ref. [5], and provides more detailed information on the subject of developing and maintaining contingency plans for nuclear facilities.

OBJECTIVE

1.3. This publication provides guidance to States, competent authorities and operators on how to develop and maintain contingency plans for nuclear facilities. It can be used as a starting point for organizations that have not previously

[1] Historically, the term "physical protection" has been used to describe what is now known as the nuclear security of nuclear material and nuclear facilities, and Ref. [2] uses the term physical protection throughout its content (including using the term "physical protection regime" for those aspects of a nuclear security regime relating to unauthorized removal and sabotage of nuclear material and nuclear facilities). The term physical protection is used to refer to those aspects of nuclear security relating to measures against unauthorized removal or sabotage of nuclear material and nuclear facilities. A State's physical protection regime comprises those parts of its nuclear security regime that relate to such measures.

prepared or developed contingency plans, as well as a reference for organizations that wish to validate or improve their existing contingency plans. It is intended for use by senior managers and security specialists charged with developing contingency plans and by competent authorities charged with the oversight of such contingency plans.

SCOPE

1.4. This publication provides guidance on how to develop and maintain contingency plans for nuclear facilities.

1.5. This publication addresses facility level contingency plans and not the State contingency plan, also referred to in some publication as the national response plan.

1.6. Notably, this publication includes guidance on the interface between contingency plans, which focus on nuclear security, and emergency plans, as required in IAEA Safety Standards Series No. GSR Part 7, Preparedness and Response for a Nuclear or Radiological Emergency [6]. This guidance is intended to inform the preparation of an effective, comprehensive, unified and coordinated response in situations where both plans are invoked simultaneously, for example, in cases where a nuclear security event triggers a nuclear or radiological emergency.

1.7. Contingency plans for nuclear security events involving computer security or that occur during transport are not addressed in this publication. These types of nuclear security events are addressed in IAEA Nuclear Security Series Nos 26-G, Security of Nuclear Material in Transport [7]; and 17, Computer Security at Nuclear Facilities [8].

STRUCTURE

1.8. Following this introduction, Section 2 addresses the objectives and goals of developing contingency plans, Section 3 addresses elements of maintaining contingency plans, including contingency plan exercises, contingency plan sustainability and information security. The annexes address interfaces between the contingency plans and the emergency plans (Annex I) and provide examples of a response memorandum of understanding (Annex II), an implementing procedure (Annex III) and an action matrix (Annex IV).

2. DEVELOPING A CONTINGENCY PLAN

2.1. Fundamental Principle K of the 2005 Amendment to the Convention on the Physical Protection of Nuclear Material states that "Contingency (emergency) plans…should be prepared and appropriately exercised by all license holders and authorities concerned" [9].

2.2. According to Ref. [2], contingency plans are "Predefined sets of actions for response to unauthorized acts indicative of attempted *unauthorized removal* or *sabotage*, including *threats* thereof, designed to effectively counter such acts." Reference [2] further recommends in para. 3.58 that (footnote omitted) "The State's *competent authority* should ensure that the *operator* prepares *contingency plans* to effectively counter the *threat assessment* or *design basis threat* taking actions of the *response forces* into consideration."

2.3. The contingency plan should be approved by the competent authority in connection with the security plan as part of licensing. Operators should ensure that the competent authority is provided with sufficient evidence that the contingency plan has been appropriately coordinated with the requirements of the emergency plan to ensure that the plans are integrated and provide for an effective response.

2.4. When developing a contingency plan, the operator should first identify any data, criteria, procedures, resources and logistical support necessary for the contingency plan. After this step is completed, the drafting of the contingency plan should be initiated.

GOALS OF CONTINGENCY PLANNING

2.5. Paragraph 4.19 of Ref. [2] recommends that "*Contingency plans* should be prepared to counter *malicious acts* effectively and to provide for appropriate response by *guards* or *response forces*. Such plans should also provide for the training of facility personnel in their actions."

2.6. Paragraph 3.122 of Ref. [5] states:

> "The goals of contingency planning are to ensure a timely and effective response at all levels to any nuclear security event comprising a malicious act that involves or is directed at a nuclear facility and to maintain physical protection during other events, such as an accident involving a release of

radionuclides, a medical emergency or a natural disaster. The correct actions need to be taken and decisions made at the right time to adequately respond to the event and resolve the situation."

2.7. When developing a contingency plan to meet these goals, the operator should ensure that the contingency plan provides clear guidance for the following:

(a) Identification of the type of nuclear security event that has occurred;
(b) The sequence of actions that would be taken in response to the nuclear security event;
(c) The resources (including number of staff) needed to implement the response to the nuclear security event;
(d) Responsible parties for the implementation of different parts of the contingency plan;
(e) The procedure for informing parties involved in the response that a nuclear security event has occurred.

2.8. In order to ensure an integrated and cohesive response, the contingency plan should be consistent and well integrated with the State contingency plan[2], the operator's overall security plan, the National Radiation Emergency Plan, the operator's emergency plan[3], and nuclear material accounting and control and off-site response procedures.

ELEMENTS OF THE CONTINGENCY PLAN

2.9. The following elements should be specifically addressed as part of the contingency plan:

(a) The objective of the contingency plan;
(b) The physical layout (schematic arrangement of parts and area) of the nuclear facility, the local environment, and potential targets, if not included as part of the security plan;
(c) An overview of the physical protection system, if not included as part of the security plan;

---

[2] Reference [2] refers to the State contingency plan (used throughout this publication for consistency), while Ref. [4] refers to the national response plan for nuclear security events. For the purposes of this publication, these terms are interchangeable.

[3] Annex I provides a discussion of interfaces between contingency and emergency plans.

(d) The application of the design basis threat or threat assessment, if not included as part of the security plan;
(e) A description of roles and responsibilities during response to a nuclear security event;
(f) Criteria for the initiation of the contingency plan;
(g) Rules of engagement;
(h) Response planning;
(i) On-site response forces[4];
(j) Protocols for off-site response to a nuclear security event;
(k) Recapture and recovery of nuclear material;
(l) Minimizing and mitigating the consequences of a nuclear security event;
(m) Command, control and communication during a nuclear security event.

In addition, coordination between physical and computer security response and any interfaces between safety, security and safeguards responsibilities during a nuclear security event should be considered during the drafting of the contingency plan, and addressed as appropriate throughout the plan.

2.10. In the following subsections, guidance is provided on addressing each of these elements in the contingency plan. The guidance provided here assumes that the operator has chosen to develop a separate section of the contingency plan to address each element. Other methods for structuring these plans could also be used,[5] as long as each element is adequately addressed in the plan.

Objective

2.11. The contingency plan should clearly address the objective of the contingency response. Paragraph 3.11 of Ref. [5] states:

> "Each State will define its own response objectives and may have different approaches or strategies for using response forces. These definitions, approaches and strategies may depend on the type of nuclear material and facilities being protected and the potential intentions of adversaries (e.g. theft,

[4] Reference [2] refers to response forces as on-site or off-site persons who are armed and appropriately equipped. For the purposes of this publication, this term also refers to non-armed responders.

[5] Another method for structuring contingency plans is provided as an example in appendix II of Ref. [5]. As long as the full scope of information described in this publication is included in the contingency plans, the structure provided there could also be used as a model.

sabotage). Response strategies for nuclear facilities with significant targets for theft and/or sabotage are:

(a) Denial of access, in which the goal is for the response force to prevent adversaries from gaining access to the target area;
(b) Denial of task, in which the goal is for the response force to stop the adversaries (including any insiders involved) before they are able to successfully complete their task;
(c) Containment, in which the goal is for the response force to prevent adversaries from removing material beyond a specific point, such as the boundary of the limited access area, thus preventing it from becoming out of regulatory control."

2.12. Thus, the objective set out in the contingency plan for the response will depend upon the State's response objectives as well as the types of potential targets in the facility.

Physical layout of the nuclear facility, the local environment and potential targets

2.13. The contingency plan should include a description of the physical layout of the nuclear facility and the potential targets within the facility, as well as the local environment. The goal of this section of the contingency plan is to enable staff who use the plan to have ready access to this information for coordination of response activities. Access to the information contained in this section should be provided only to those personnel who require the information to implement their part of the contingency plan.

2.14. The description of the facility and potential targets within it should include physical structures located on the site, as well as, where applicable, barriers, vital and inner areas, on-site fuel or hazardous material storage, critical systems, and components and other possible targets. The description of the local environment of the facility should include both the site and the surrounding area. The location of the site in relation to nearby towns should be described, as well as transportation routes (e.g. rail, water and roads), staging areas, pipelines, airports, hazardous material facilities and pertinent environmental features that might affect coordination of response activities. Main and alternate entry routes for off-site response should also be described in the plan and maps should be included as appropriate.

Overview of the physical protection system

2.15. The contingency plan should include a visual depiction of the physical protection systems that support and influence the operator's response to a nuclear security event, such as maps, drawings and floor plans, as well as a written description of these systems.

2.16. The depiction and description should include all on-site physical protection measures, from those implemented at the outermost facility perimeter to those protecting vital and inner areas as well as other targets.

2.17. The description of the physical protection systems in this section should highlight any physical protection systems and hardware providing defence-in-depth, such as access delays, detection systems, access controls, armaments and communications systems, as identified in the operator's security plan.

The application of the design basis threat or threat assessment

2.18. Paragraph 3.124 of Ref. [5] states "The State, the appropriate competent authorities and the operator should have a comprehensive set of contingency plans that address different types of nuclear security event."

2.19. The operator should develop appropriate site specific scenarios for nuclear security events involving sabotage or unauthorized removal of nuclear material, based on the threats described in the State's design basis threat or threat assessment. A range of these possible site specific scenarios should be described in the contingency plan, as well as steps to be taken by response personnel in responding to these scenarios (see paras 2.28–2.33).

Description of roles and responsibilities during response to a nuclear security event

2.20. Roles, responsibilities and priorities for protection should be set out in the contingency plan. The minimum number of response personnel needed to implement the contingency plan should be determined during the planning process, and this number should be documented either in the contingency plan, the operator's security plan or as required by the relevant competent authorities. The operator should also identify and document any off-site response forces needed to support the response to a nuclear security event.

Criteria for the initiation of the contingency plan

2.21. Paragraph 3.62 of Ref. [2] states, "The *operator* should initiate its *contingency plan* after *detection* and assessment of any *malicious act*."

2.22. The criteria that the operator will use to judge whether a malicious act has been detected should be clearly described in the contingency plan. These criteria should include indicators for whether the cause of the alarm is malicious. If a malicious act is determined to have been detected, a nuclear security event would be considered to be underway. Once it has been determined that a nuclear security event is underway, the competent authority should be notified, as required.

2.23. Criteria for the initiation of the contingency plan should also be included in the contingency plan, and could include the detection of certain malicious acts that put the facility at risk in such a way that could lead to unacceptable radiological consequences or unauthorized removal of material. Examples of such acts include the following:

(a) Armed attack;
(b) Detection of unauthorized intrusion;
(c) Discovery of an insider threat;
(d) Suspicion or detection of unauthorized removal of nuclear material or other radioactive material;
(e) Loss of power for physical protection systems.

2.24. States might also consider requiring the operator to include criteria for initiating the contingency plan in situations that do not involve a malicious act, but for which a security response might still be needed, such as natural disasters, peaceful protest or a fire.

2.25. The contingency plan should also describe criteria for determining when to terminate the response to a nuclear security event after the threat has been neutralized or the facility is no longer considered to be at risk.

2.26. Interfaces with emergency response should be carefully considered (see Annex I for more information on this topic). In particular, when defining the criteria for activating the contingency plan, consideration should be given to the emergency classification used to activate an appropriate level of emergency response as per Refs [6] and [10] such that notifications to the competent authority and the activation of the two plans are coordinated.

Rules of engagement

2.27. The contingency plan should describe any legal or other constraint that could affect the response to a nuclear security event. Such constraints could include restrictions on the use of force or other administrative and logistical requirements for on-site and off-site response personnel, such as requirements to ensure equipment and other resources are readily available and in working condition.

Response planning

2.28. Regardless of whether the response force is based on-site or off-site, the operator should develop implementing procedures for each scenario included in the contingency plan (see paras 2.18, 2.19). The response planning section could include flow diagrams, results from computer modelling or an action matrix to describe these procedures.

2.29. An action matrix is a planning tool that can be used by response personnel to inform timely decision making and specify procedures for response to a specific type of nuclear security event. For each type of nuclear security event addressed in the contingency plan, specific actions, roles and responsibilities, resources and associated timelines would be assigned in the action matrix in a manner that addresses competing priorities and promotes interoperability across the contingency and emergency plans. An example of an action matrix is included as Annex IV.

2.30. The operator's action matrix or a suitable alternative used for response planning should be based on the scenarios outlined in the contingency plan as well as on the criteria for initating the contingency plan (see paras 2.21–2.26), and should include the following information:

(a) A short heading describing the type of nuclear security event (e.g. bomb threat).
(b) A brief narrative of an activity that identifies the beginning of the nuclear security event and provides enough information to allow response personnel to determine whether to initiate the contingency plan.
(c) Responders who would be assigned duties and actions as a result of this nuclear security event.
(d) Specific duties and the steps to be taken by responsible personnel, including provision of initial alerts or event notifications, assessment, communication, activation of response, mitigating actions to be taken and actions to return to normal operations.

(e) Relevant supporting information that will facilitate decision making and necessary actions (e.g. procedures, floor plans, maps, cordon distances, alarm zones and contact lists). This information should not contain an excessive amount of background information or material, as this could hinder navigation by response personnel or their subsequent decision making.

2.31. In the response planning section of the contingency plan, the operator should also specify any areas of the facility that need additional protection, such as vital or inner areas. The operator should also include potential adversary routes to those areas in the contingency plan and ensure the timelines provided for the site-specific scenarios are sufficient to allow for response personnel to perform their actions.

2.32. The contingency plan should identify response positions that can provide protection for responders and should include provisions to ensure that response personnel are appropriately equipped for the full range of scenarios outlined in the contingency plan, including weapon systems, protective equipment, communications, transportation and other response equipment.

2.33. This section of the contingency plan should also address ensuring that roles, responsibilities and resources are identified in advance and that the necessary procedures are put in place.

On-site response forces

2.34. The contingency plan should specifically address the on-site response forces. The plan should specify that guards and on-site response forces assigned to implement the contingency plan, which might include on-site military or law enforcement personnel, should be suitably trained and qualified in those duties, should be ready to respond at all times and should not be assigned other duties or responsibilities that could negatively affect the implementation of the contingency response.

2.35. Protocols for response should be established between the operator and any on-site response forces and these protocols should be referenced and described in the contingency plan. These protocols should describe specific actions, areas of responsibility, resources and associated timelines for execution of the contingency plan by on-site response forces.

2.36. In order to facilitate the execution of the contingency plan, the operator could consider integrating information on guards and on-site response forces into an action matrix (see Annex IV and discussion in paras 2.28–2.33).

Protocols for off-site response

2.37. In addition to on-site response forces, arrangements for off-site response forces should be discussed in the contingency plan, including reference to any protocols established between the operator and off-site response force organizations.

2.38. Where possible and consistent with national policing and emergency arrangements, protocols such as a written memorandum of understanding (MOU) should be established between the operator and relevant off-site response force organizations. The purpose of such protocols is to facilitate cooperation and understanding between on-site and off-site response forces and to integrate the off-site response forces into the overall contingency response planning process. Challenges associated with off-site response should be considered in the contingency plan, such as securing resources for the response, potentially long response times depending on the location of the off-site response forces, considerations associated with the sharing of sensitive information and personal data, difficulties with integrated information exchange and collaboration, ensuring secure communications and the need to increase off-site responders' level of familiarity with the facility. An example of an MOU for off-site response is included as Annex II.

2.39. Protocols established between the operator and relevant off-site response force organizations should clearly set out the roles and responsibilities of the operator and the response force organizations during a nuclear security event. Where possible and consistent with national policing and emergency arrangements, protocols should:

(a) Establish incident command structure and specify responsibilities for each organization involved in the response;
(b) Identify the communications methods to be used during the response;
(c) Provide for timely reception and assembly of the off-site responders and coordination of response activities;
(d) Provide an estimate of the number of personnel that will be involved in the response from each organization and the response capabilities available, including weapons and equipment as well as timelines for arrival of both

immediately available personnel and personnel that will arrive at a later time;

(e) Identify suitable secure locations in close proximity to the facility where responders could receive a briefing on the situation during a nuclear security event to enable them to better plan and prepare their response;

(f) Set out the availability of key personnel and any additional information needed to assist in command decisions, briefings, assignment of responders, and situational awareness, such as maps, floor plans and equipment diagrams;

(g) Describe locations that have adequate utilities, such as sanitation, water and electricity, to sustain operations as well as the equipment needed to respond to a nuclear security event (e.g. weapon systems, protective equipment, communications, transportation), and the locations and capabilities of equipment staged on-site and off-site.

2.40. The contents of any MOU or protocols established with off-site response organizations should be included in the contingency plan.

2.41. Provisions should be included in the contingency plan that call for a periodic review of the protocols for off-site response within the framework of the review of the operator's security plan. This periodic review of the protocols for off-site response could include reviewing that the protocols are consistent with and can operate in accordance with the contingency and emergency plans (see Annex I) as well as renegotiating the protocols at the request of either party if changes occur in the governing conditions, such as operating regulations, competent authorities or threat levels, or as necessary.

Recapture and recovery

2.42. In order to support any off-site response undertaken by the operator (e.g. when in pursuit of an adversary), the contingency plan should describe in detail how coordination with State authorities and off-site responders is to be undertaken, in accordance with all applicable laws and regulations.

2.43. The protocols for off-site response described in paras 2.37–2.41 should include provisions establishing the roles and responsibilities of the operator and the off-site response forces with respect to nuclear and other radioactive material that has left the facility in an unauthorized manner during a nuclear security event.

2.44. For on-site recapture and recovery, these protocols should include information on notifications to be sent to the competent authority as well as the

operator's procedures for continuing to search for missing nuclear material and for securing and protecting the area where the nuclear and other radioactive material was stored as a crime scene.

2.45. Recovery actions to be taken by the operator to coordinate the securing and return of nuclear and other radioactive material to the facility should also be described in detail in the contingency plan, including identifying personnel responsible for the transportation and preservation of evidence for any potential criminal proceedings.

Command, control and communication

2.46. Paragraph II.6. of Ref. [5] states:

> "This section describes the arrangements documented in protocols agreed with external response organizations. It details which agency has the operational lead and the circumstances in which this lead may be handed over to another agency. Details are provided of all the communication links to be used and the location of the incident control centres that may be used at different stages of the event, taking into account prevailing circumstances and the centres' strategic and tactical responsibilities."

2.47. Command, control and communication procedures should be documented in the contingency plan, including those for the following:

(a) Coordination of guards and response forces;
(b) Management of response;
(c) Secure communication, if required, and other information security measures;
(d) Chain of command during a nuclear security event;
(e) Handover and delegation of authority during a nuclear security event.

2.48. All communication methods and protocols used during a nuclear security event should be addressed in the contingency plan, and details regarding their interoperability, implementation and maintenance during a nuclear security event should be documented.

2.49. Command, control and communication procedures described in the contingency plan should be integrated with those in the emergency plan in order to allow for effective response in situations where both plans are invoked simultaneously.

DEVELOPING PROCEDURES COMPLEMENTARY TO THE CONTINGENCY PLAN

2.50. In addition to developing the contingency plan as described in the previous sections, operators should establish and maintain procedures detailing actions to be taken in the event that the contingency plan is initiated. These procedures should enable unified command and control by clearly identifing the steps to be taken and decisions to be made by each member of the response organization following the initiation of the contingency plan. An example of such procedures is provided in Annex III.

3. MAINTAINING THE CONTINGENCY PLAN

3.1. Once the contingency plan is in place, it should be regularly exercised, it should be sustained, and sensitive information relevant to it should be protected. The following sections address these three aspects of maintaining the contingency plan.

EXERCISING THE CONTINGENCY PLAN

3.2. Training and exercises should be used to evaluate and improve the ability of response personnel to implement the contingency plan. Paragraph 3.60 of Ref. [2] states:

> "The coordination between the *guards* and *response forces* during a *nuclear security event* should be regularly exercised. In addition, other facility personnel should be trained and prepared to act in full coordination with the *guards*, *response forces* and other response teams for implementation of the plans."

3.3. The operator should ensure that all personnel involved in the response to a nuclear security event receive initial as well as periodic training relating to the contingency plan and participate in exercises of the contingency plan and emergency plan, commensurate with their roles and responsibilities during a nuclear security event.

3.4. Training and exercises relating to the contingency plan could include tabletop exercises, limited scope testing, classroom lectures, walking tours to familiarize personnel with the facility and force on force exercises or other activities during which responders will need to demonstrate their responsibilities during a nuclear security event in order to validate the effectiveness of the various components of the contingency plan. The ability of personnel to implement the contingency plan could be evaluated based on their knowledge of topics such as the following:

(a) Implementing procedures;
(b) The facility, targets, physical protection systems and defence-in-depth measures;
(c) Threats to the facility;
(d) Response equipment;
(e) Response positions and timelines;
(f) Steps to be taken by individuals or groups in particular situations.

3.5. The operator should develop an evaluation process to identify lessons from training and exercises that could be incorporated into a corrective action programme to further improve and refine the contingency plan. For example, operators might document all drills and exercises, including a post-exercise critique in which participants identify good practices, areas for improvement, deficiencies or other findings in relation to performance, plans, equipment or strategies. If a concern is identified during this critique, it should be incorporated into the operator's corrective action programme for timely correction. Issues incorporated into the corrective action programme should be protected and communicated only on a need-to-know basis, consistent with information security requirements imposed by the competent authority.

3.6. The operator should also conduct joint contingency plan exercises involving coordinated response by safety, nuclear materials accounting and control, and security personnel, in order to evaluate and improve the effectiveness of unified communication, command and control, and handover. In particular, exercises should be used to ensure interoperability between the contingency plan and the emergency plan. Joint security exercises involving off-site organizations should also be undertaken in order to evaluate and improve implementation of the contingency plan as well as coordination between the contingency and emergency plans.

SUSTAINABILITY OF THE CONTINGENCY PLAN

3.7. According to Ref. [11], contingency planning should be considered at each stage of the life cycle of a facility. Each of these stages will have actions associated with them that will need to be addressed in the contingency plan, as detailed in Ref. [11].

3.8. Operators should ensure that the contingency plan continues to guide a systematic, coordinated and effective response to malicious acts at all stages of the life cycle of a facility. This can be accomplished through periodic and independent review, evaluation, audit and maintenance of the contingency plan in accordance with the requirements of the competent authority.

3.9. The contingency plan should be updated as soon as reasonable after any change in personnel, procedures, equipment or facilities that may affect the plan. Revisions to the contingency plan should be submitted to and approved by the relevant competent authorities, as required, and their interoperability with the emergency plan, as well as with any procedures followed by the organizations responsible for implementing the contingency plan (such as the nuclear material accounting and control organization), should be regularly reviewed.

3.10. Protocols that are relevant to the contingency plan, such as an MOU agreed between the operator and off-site response forces, should also be reviewed at regular intervals or as necessary in order to ensure compliance with performance requirements.

3.11. The results of the reviews of the contingency plan should be analysed as part of the operator's lessons identified and corrective action programme. The results should be available to the operator's management so that they are able to assess the findings, recommendations and implement corrective actions when needed.

3.12. All records relating to reviews of the contingency plan should be retained in accordance with the requirements of the competent authority.

INFORMATION SECURITY

3.13. The contingency plan may contain sensitive information that should be protected properly according to the information security requirements of the competent authority. More information on securing sensitive information can be found in Ref. [12].

3.14. Consistent with the guidance provided in Ref. [12], information on the contingency plan should be treated as sensitive and should be provided to only those personnel who need the information in order to implement their roles with respect to the contingency plan. Controls applied to the plan could include records of its receipt, location, transfer and destruction. Where necessary, encryption or other secure means should be used to convey sensitive information relating to or extracted from the contingency plan to external parties. The external parties should provide assurance that the sensitive information relating to or extracted from the contingency plan will be stored in secure (access controlled) systems. There should also be procedures to ensure the integrity and availability of any information critical to the appropriate response to a nuclear security event. This includes information systems such as detection and assessment systems, and communication 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] INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5), IAEA Nuclear Security Series No. 13, IAEA, Vienna (2011).

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

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

[5] INTERNATIONAL ATOMIC ENERGY AGENCY, Physical Protection of Nuclear Material and Nuclear Facilities (Implementation of INFCIRC/225/Revision 5), IAEA Nuclear Security Series No. 27-G, IAEA, Vienna (2018).

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

[7] INTERNATIONAL ATOMIC ENERGY AGENCY, Security of Nuclear Material in Transport, IAEA Nuclear Security Series No. 26-G, IAEA, Vienna (2015).

[8] INTERNATIONAL ATOMIC ENERGY AGENCY, Computer Security at Nuclear Facilities, IAEA Nuclear Security Series No. 17, IAEA, Vienna (2011).

[9] Amendment to the Convention on the Physical Protection of Nuclear Material, GOV/INF/2005/10–GC(49)/INF/6, IAEA, Vienna (2005).

[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 (in preparation).

[11] INTERNATIONAL ATOMIC ENERGY AGENCY, Security during the Lifetime of a Nuclear Facility, IAEA Nuclear Security Series No. 35-G, IAEA, Vienna (2019).

[12] INTERNATIONAL ATOMIC ENERGY AGENCY, Security of Nuclear Information, IAEA Nuclear Security Series No. 23-G, IAEA, Vienna (2015).

Annex I

INTERFACE OF THE CONTINGENCY PLANS AND EMERGENCY PLANS

I–1. Each State independently determines the relationship between nuclear and radiation safety, and nuclear security.

I–2. While separate from the emergency plan for the facility, as stated in Ref. [I–1], Fundamental Principle K "may imply that contingency plans are the same as emergency plans. In practice there are differences among States in the definition and use of these terms." Paragraph 3.120 of Ref. [I–1] continues by noting that in Ref. [I–2] (reference omitted):

> "the contingency plan is part of the overall nuclear security plan and relates to the response of physical protection personnel to nuclear security events involving malicious acts. In IAEA Safety Standards Series No. GSR Part 7, Preparedness and Response for a Nuclear or Radiological Emergency, the emergency plan relates to the response to a nuclear or radiological emergency, whether that emergency is caused by an accident or by a malicious act. However, the implementation of the contingency plan and the emergency plan will require a coordinated response of physical protection, nuclear material accounting and control, and safety personnel."

According to Ref. [I–1], the contingency plans and emergency plans[1] should be comprehensive and complementary.

I–3. This annex lists areas of interfaces between the contingency plans and emergency plans. Each section highlights the main areas of interface and includes supporting examples within these areas.

[1] Reference [I–3] defines emergency plan as "A description of the objectives, policy and *concept of operations* for the response to an *emergency* and of the structure, authorities and responsibilities for a systematic, coordinated and effective response. The *emergency plan* serves as the basis for the development of other plans, *procedures* and checklists."

FACILITY DESIGN FEATURES

I–4. Consideration of physical protection during the facility design and site selection phases is important to ensure that safety and security functions are mutually supportive and are not in conflict with each other to the extent possible. As the contingency plan is a predefined set of actions for response to unauthorized acts, the following are examples of where an interface may exist between emergency planning and contingency planning:

(a) Physical layout of nuclear facility and local environment (e.g. demographics and topography);
(b) Safety related equipment and radioactive material requiring protection against unauthorized removal or sabotage based on a graded approach;
(c) Location and protection of control rooms, emergency response facilities and alarm stations;
(d) Design of fire safety features (fire doors, suppression systems);
(e) Emergency evacuation routes, access routes and muster points (including physical barriers along these routes);
(f) Coordination of changes to the layout or design of a nuclear facility that may impact security or emergency response.

PLANS AND PROCEDURES

I–5. Contingency plans and emergency plans need to take into account the respective security and safety requirements.

I–6. The following lists the consistencies needed between contingency plans and emergency plans:

(a) Plans need to be implemented with the appropriate level of response;
(b) Plans need to be comprehensive and complementary;
(c) Off-site emergency plans, procedures and assets need to be coordinated, and interact with on-site security forces (e.g. access control, on-site protection);
(d) Sufficient numbers of security personnel need to be available to support an emergency response while maintaining adequate security;
(e) An MOU with any single off-site response organization needs to be consistent with both the emergency plans and contingency plans.

ORGANIZATION STRUCTURE

I–7. The roles and responsibilities are identified between the emergency plan and the contingency plan in order to do the following:

(a) Define a coordinated response, including decision making;
(b) Respond with an appropriate number of qualified personnel, with appropriate and sufficient equipment, and within required timelines;
(c) Identify competing priorities (dual assignments, unavailability) for security personnel during an emergency response.

I–8. Establishment and use of a unified command and control system for emergency and contingency response provides for effective coordination of on-site and off-site response. Some characteristics of the unified command and control mechanism may include the following:

(a) Location of a unified command and control facility that may evolve with progression of the event;
(b) On-site and off-site authority and responsibility.

IMPLEMENTATION OF THE CONTINGENCY PLAN

Initiating event[2]

I–9. Assessment of an event involves the following:

(a) Identification of initiating events that require coordination between emergency and contingency plan.
(b) Coordinated activation of both internal emergency and security personnel, which may include the following:
    (i) Arranging access to vital areas;
    (ii) Moving physical barriers;
    (iii) Relocating security personnel based on a nuclear or radiological emergency;
    (iv) Establishing a timeline and criteria for activation that may be different for contingency plan versus the emergency plan.

[2] This section is based on Ref. [I–4].

Coordination of response actions

I–10. Coordination between the emergency plan and the contingency plan with respect to on-site activities to ensure protection from all hazards, including radiological hazards, involves the following:

(a) Coordination between the emergency plan and the contingency plan to ensure safe movement of emergency workers necessary to perform required actions;
(b) Coordination of security measures for all personnel;
(c) Emergency evacuation of personnel, as prescribed in the emergency plan, for rapid and safe egress to designated emergency planning zones;
(d) Coordination in relation to accountability of personnel and nuclear or radiological material following an emergency evacuation;
(e) Identification of safety related equipment and devices, equipment within vital areas, and hazardous materials that may be adversely affected by the security response actions;
(f) Coordination of safety and security response as event progresses;
(g) Re-evaluation of target(s) as event progresses;
(h) Adaptation of protective strategies against threat as event progresses;
(i) Coordination between the emergency and contingency plan to ensure protection from all hazards, including radiological hazards, of off-site security response assets, and the potential need for rapid ingress/egress of response personnel.

COMMUNICATIONS

I–11. Coordination between contingency and emergency response actions needs to include communication systems and procedures addressing the following:

(a) Secure internal communication systems between contingency response personnel and emergency response personnel;
(b) Awareness and understanding of contingency and emergency response actions and terminology;
(c) Diverse and redundant methods of communication for both contingency and emergency response;
(d) Communication processes established between the contingency and emergency response in order to ensure a coordinated response;
(e) Coordination of notification to appropriate levels of contingency and emergency response consistent with the potential consequences of the event;

(f) Coordinated notification to off-site response agencies;
(g) Coordination of the established public communication strategy on contingency and emergency response that provides for transparency while maintaining the appropriate level of confidentiality (e.g. not disclosing security or safety related sensitive information) based on the audience (e.g. media, local population, other nuclear facilities, other stakeholders) and timing of information release.

RECOVERY

I–12. Coordination of contingency and emergency responses needs to address the post-event recovery considerations including the following:

(a) Prioritized and coordinated recovery team efforts (all hazards, medical, security);
(b) Clearing of areas and site equipment (e.g. searching for additional or residual security concerns) prior to resuming operations;
(c) Preservation of forensic evidence (e.g. prevention of unnecessary interference with collection or preservation of evidence).

TRAINING AND EXERCISES

I–13. Coordinated contingency and emergency response actions need to be trained and exercised to include initial and periodic training, commensurate with the prescribed actions of the contingency and emergency personnel.

REFERENCES TO ANNEX 1

[I–1] INTERNATIONAL ATOMIC ENERGY AGENCY, Physical Protection of Nuclear Material and Nuclear Facilities (Implementation of INFCIRC/225/Revision 5), IAEA Nuclear Security Series No. 27-G, IAEA, Vienna (2018).
[I–2] INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5), IAEA Nuclear Security Series No. 13, IAEA, Vienna (2011).
[I–3] INTERNATIONAL ATOMIC ENERGY AGENCY, IAEA Safety Glossary: Terminology Used in Nuclear Safety and Radiation Protection, 2018 Edition, IAEA, Vienna (2019).

[I–4] 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 (in preparation).

Annex II

EXAMPLE OF A MEMORANDUM OF UNDERSTANDING FOR OFF-SITE RESPONSE

II–1. This annex gives an example of an MOU (Box II–1). This MOU outlines the agreement between the [name of the facility] (the operator) and the [name of the response force organization] (the response forces). It might not apply to States where the response forces are government agencies that are mandated under law to provide response to the facility.

BOX II–1. EXAMPLE MEMORANDUM OF UNDERSTANDING FOR OFF-SITE RESPONSE

1. Introduction

This MOU outlines the agreement between the operator and the response forces for terms and conditions of both parties in relation to the following:

— The response forces agree to provide an adequate, appropriate and effective response to calls for assistance as a result of a nuclear security event.
— The response forces agree to participate in familiarity, preparedness activities and security exercises and training.
— The operator agrees to provide facilities, technical support, logistics, expertise and resources to support the response forces.

This MOU is subject to review at the request of either party (annually or otherwise) if changes occur to the governing conditions such as operating regulations, statutory authorities or security threats (design basis threat).

2. Points of contact

The operator's designee will be the primary facility site contact for security and issues with the response force's designee. Additional points of contact would be identified between the operator and response forces.

3. Initial notification

3.1. Initial notification

When a security event occurs at the operator's facility, the central alarm station (CAS) will follow the contingency plan to contact the response forces by the agreed upon communication arrangements.

3.2. Response forces arrival

Following communication from the CAS, the response forces will deploy, in a timely manner, appropriate and adequate response personnel to the facility to assist the operator's facility response personnel with the security event.

4. Responsibilities

4.1. Operators

The operator agrees to provide facilities, technical support, logistics, expertise and resources to support the response forces. This may include the following:

(a) Information regarding any radiological and technical issues;
(b) On-site protection of workers;
(c) Site maps and facility floor plans;
(d) Escorts;
(e) Compatible communications;
(f) Logistical support, such as marshalling areas, briefing areas, power supplies;
(g) Accountability of personnel arriving and working on the site at all times.

4.2. Response forces

The response forces agree to provide a minimum of [X] personnel and equipment at the request of the operator to assist the facility during a nuclear security event. Agreements on the expected number and estimated time of arrival of each response forces' primary response and supporting response elements would be specified in an annex to the MOU and may include the following:

(a) Tactical response units;
(b) Crisis negotiator;
(c) Canine team;
(d) Explosive disposal;
(e) Emergency services (e.g. local law enforcement, medical services, hazmat teams);
(f) Forensic identification services;
(g) Technical traffic collision investigation;
(h) Dangerous goods coordinator;
(i) Any other service provided by the response forces or supporting units deemed necessary by the incident commander.

4.3. First response forces at the facility

Upon arrival, the first response forces would receive a reception briefing and determine the appropriate response actions in coordination with the incident commander.

5. Security exercises

5.1. Exercises

The operator would invite the response forces to participate in security exercises and drills as part of their exercise programme, at a frequency of [X] every [X] years. The response forces would continue, as agreed upon, to practice command and control of the response.

The operator would be responsible for planning security exercises, developing the exercise scenarios and coordinating the exercise. The response forces would appoint a liaison officer to assist in the development and coordination of response forces involvement in the exercises.

5.2. Facility visits by response forces

The operator would invite response forces personnel to conduct visits of the facility to establish and maintain a level of familiarity with respect to response logistics, plant layout, operations and equipment.

6. Communications

6.1. Communication resources

During security events at the facility, the operator and response forces agree to have interoperable equipment to facilitate effective communications capable of providing information that is secure and authenticated, such as the following:

(a) A direct phone line between the command and control elements;
(b) Compatible command centre radios and frequencies;
(c) Compatible portable security radios and frequencies;
(d) Other compatible communication devices.

6.2. Maintenance of communications equipment

The following off-site communication resources will be maintained by the facility:

(a) Dedicated direct telephone link between the CAS and response forces;
(b) Radio communication between the facility CAS and response forces.

6.3. Communications testing

The operator would test communications with the response forces on a regular basis. If a test is not initiated by the operator, the response forces would contact the operator and request that the test be conducted.

7. Limitations of liability, indemnification and insurance

7.1. Response forces

The response forces shall not be liable in any manner whatsoever to the facility, which includes all of its respective staff, and agents or their successors and assign responsibility for any claim, including a claim by any third party

against the facility, its staff or agents, unless it was caused by negligence of an employee or agent of the response forces.

7.2. Facility

The facility does hereby indemnify the response forces, its staff and agents, including their successors and assign against all costs, losses, expenses or liabilities incurred as a result of a claim or proceeding relating to or arising from response forces' performance of this agreement unless it was caused by negligence or wilful misconduct of an employee or agent of the response forces. Notwithstanding the foregoing, in no event shall the facility be liable for indirect or consequential damages.

The facility and the response forces would ensure that they have appropriate general liability insurance.

8. Termination

Either party may terminate this MOU at any time, without fault and without liability, upon [X] weeks written notice of termination.

Termination of this MOU does not affect any other relationship or obligation between the parties.

9. Agreement

This MOU constitutes the entire agreement between the parties. There are no other agreements, undertakings, representatives or warranties (collateral, oral or otherwise) relating to the subject matter herein.

IN THE WITNESS WHEREOF the parties have executed this agreement.

DATED AT_____, this_____day of_____, year_____

Signature:_____

Name:_____

Chief of response forces

(Response forces pursuant to delegated authority)

DATED AT_____, this_____day of_____, year_____

Signature:_____

Name:_____

Facility operator

Note: The MOU would include an appendix detailing the relevant definitions used in the MOU.

Annex III

EXAMPLE OF IMPLEMENTING PROCEDURE

III–1. The bomb warning procedure detailed in paras III–3 to III–8 is provided as an example of how to develop written procedures that implement the requirements of the contingency plan.

III–2. Purpose: The purpose of this procedure is to establish and maintain predetermined actions that implement the requirements of contingency plan response personnel during a nuclear security event for a (bomb warning).

III–3. Event description: Bomb warnings may be expressed by telephone, by mail (letter or email), by a hand delivered message, or by some other means. Warnings may be given directly or indirectly through a law enforcement agency, mass media organization, or some other third party. Warnings also may be received and communicated by plant personnel, authorities off-site, or other third parties who would notify security.

III–4. Objectives of the contingency response to a bomb warning include the following:

— Validate the warning;
— Mitigate the warning;
— Minimize potential consequences of the warning;
— Inform all decision makers of the event.

III–5. Decisions and actions in response to a bomb warning include the following:

— Gather and evaluate information from the bomb warning communication;
— Notify appropriate entities;
— Attempt to locate suspected bomb(s);
— If bomb is confirmed, take action to mitigate potential consequences;
— If bomb is not confirmed, begin taking actions to return to normal operations;
— Terminate event once the facility is determined to be safe.

III–6. Responsible response personnel and their associated actions in response to a bomb warning include the following:

- Central alarm station (CAS) operator:
  - — Initial receipt or notification of bomb warning;
  - — Notify security management;
  - — Notify facilities operations;
  - — Deploy response personnel;
  - — If a bomb is discovered, transition to the discovery of explosives procedure.
- Guards/response forces:
  - — Upon request, conduct search for suspected bomb(s);
  - — If a bomb is confirmed, cordon, communicate location and details to CAS, and await directions;
  - — Execute ongoing tactical operations;
  - — If a bomb is not discovered, communicate to CAS, and await directions.
- Security management:
  - — Assess warning and if required direct CAS to deploy guards to conduct search;
  - — Direct CAS to notify facilities operations;
  - — Receive search results;
  - — Report results to facility operations;
  - — Advise facility operation on recommendations;
  - — Advise on ongoing tactical operations;
  - — If a bomb is discovered, transition to the discovery of explosives procedure.
- Facility operations:
  - — Receive briefing from security management or CAS;
  - — If a bomb is not discovered, await recommendations from security management;
  - — If a bomb is confirmed, await recommendations from security management;
  - — If a bomb is confirmed, consider secondary hazards (e.g. effects to safety equipment or personnel);
  - — Activate emergency plan.

III–7. Termination of a bomb warning event involves the following decisions and actions:

- — Security management will make recommendations to facility operations to terminate event if no bomb was discovered.

— Facility operations will deliver a strategy to return to normal operations.

III–8. The bomb warning implementing procedure contains the following data and supporting guidance:

— Bomb warning checklist;
— Discovery of explosives nuclear security event procedure;
— Emergency evacuation plan for bomb warning;
— Facility maps and floor plans;
— Off-site response contact list;
— On-site response contact list;
— On-site emergency plan.

Annex IV

EXAMPLE OF AN ACTION MATRIX

IV–1. Table IV–1 is provided as an example of an action matrix to identify the steps to be taken for responding to nuclear security events. The action matrix could also be represented by way of flow diagrams, computer modelling, or a comparable process.

TABLE IV–1. EXAMPLE MATRIX WITH STEPS FOR RESPONSE TO A NUCLEAR SECURITY EVENT

Nuclear security event No. 1: Bomb warning				
Event description: Bomb warnings may be expressed by telephone, by mail (letter or email), by a hand delivered message, or by some other means. Warnings may be given directly or indirectly through a law enforcement agency, mass media organization, or some other third party. Warnings also may be received and communicated by plant personnel, authorities off-site, or other third parties who would notify security.				
Responsible personnel	Central alarm station (CAS)	Guards/response forces	Security management	Facility operations
Actions	Initial receipt or notification of bomb warning Notify security management Notify facilities operations Deploy response personnel If a bomb is discovered, transition to the discovery of explosives procedure	Upon request, conduct search for suspected bomb(s) If a bomb is confirmed, cordon, communicate location and details to the CAS, and await directions Execute ongoing tactical operations If a bomb is not discovered, communicate to the CAS, and	Assess warning, and if required direct the CAS to deploy guards to conduct search Direct the CAS to notify facilities operations Receive search results Report results to facility operations Advise facility operation on recommendations Advise on	Receive briefing from security management or the CAS If a bomb is not discovered, await recommendations from security management If a bomb is confirmed, await recommendations from security management If a bomb is confirmed, consider secondary hazards (e.g.

TABLE IV–1. EXAMPLE MATRIX WITH STEPS FOR RESPONSE TO A NUCLEAR SECURITY EVENT (cont.)

Nuclear security event No. 1: Bomb warning				
Event description: Bomb warnings may be expressed by telephone, by mail (letter or email), by a hand delivered message, or by some other means. Warnings may be given directly or indirectly through a law enforcement agency, mass media organization, or some other third party. Warnings also may be received and communicated by plant personnel, authorities off-site, or other third parties who would notify security.				
Responsible personnel	Central alarm station (CAS)	Guards/response forces	Security management	Facility operations
Actions		await directions	ongoing tactical operations If a bomb is discovered, transition to the discovery of explosives procedure	effects to safety equipment or personnel) Activate emergency plan
Supporting guidance	Bomb warning checklist Discovery of explosives nuclear security event procedure Emergency evacuation plan for bomb warning Facility maps and floor plans Off-site response contact list On-site response contact list	Discovery of explosives nuclear security event procedure Emergency evacuation plan for bomb warning Facility maps and floor plans Specific guard response procedures	Bomb warning checklist Discovery of explosives nuclear security event procedure Emergency evacuation plan for bomb warning Facility maps and floor plans Off-site response contact list On-site response contact list	On-site emergency plan Emergency evacuation plan for bomb warning Facility maps and floor plans Off-site response contact list On-site response contact list

IAEA
International Atomic Energy Agency

No. 26

ORDERING LOCALLY

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

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

NORTH AMERICA

Bernan / Rowman & Littlefield
15250 NBN Way, Blue Ridge Summit, PA 17214, USA
Telephone: +1 800 462 6420 • Fax: +1 800 338 4550
Email: orders@rowman.com • Web site: www.rowman.com/bernan

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

REST OF WORLD

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

Eurospan Group
Gray's Inn House
127 Clerkenwell Road
London EC1R 5DB
United Kingdom

Trade orders and enquiries:
Telephone: +44 (0)176 760 4972 • Fax: +44 (0)176 760 1640
Email: eurospan@turpin-distribution.com

Individual orders:
www.eurospanbookstore.com/iaea

For further information:
Telephone: +44 (0)207 240 0856 • Fax: +44 (0)207 379 0609
Email: info@eurospangroup.com • Web site: www.eurospangroup.com

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

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

A security contingency plan describes the predefined actions for a security response to actual or suspected sabotage or unauthorized removal of nuclear material. This publication provides guidance to States, competent authorities and operators on how to develop and maintain contingency plans for nuclear facilities. It is intended for use by facility personnel responsible for the development of security and contingency plans, and by competent authority personnel responsible for the oversight of security systems and programmes at nuclear facilities.

INTERNATIONAL ATOMIC ENERGY AGENCY
VIENNA
ISBN 978–92–0–105219–3
ISSN 1816–9317