NUCLEAR SECURITY SERIES NO. XX

NST056

DRAFT, July 2017

STEP 8: Submission to MS for comment

DEVELOPING A NUCLEAR SECURITY CONTINGENCY PLAN FOR NUCLEAR FACILITIES

DRAFT TECHNICAL GUIDANCE

INTERNATIONAL ATOMIC ENERGY AGENCY

VIENNA, 20XX

FOREWORD

[Standard NSS Foreword to be added]

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 when necessary strengthening this regime. The series also provides guidance for States in fulfilling their obligations and commitments with respect to binding and non-binding international instruments. The Nuclear Security Fundamentals set out the objective of a nuclear security regime and its essential elements [5]. The Nuclear Security Recommendations indicate what a nuclear security regime should address regarding:

(a) Physical Protection of Nuclear Material and Nuclear Facilities [1];

(b) Radioactive Material and Associated Facilities [7]; and

(c) Nuclear and Other Radioactive Material out of Regulatory Control [8].

1.2. This guidance addresses the development of contingency plans by the operator. It is based upon national experience and practices as well as publications in the field of nuclear security. It constitutes a starting point for organizations that have not previously prepared or developed contingency plans for nuclear security events, as well as a reference for organizations that wish to validate or improve their existing contingency plans.

1.3. The Fundamental Principle K of the 2005 Amendment to the Convention on the Physical Protection of Nuclear Material states that "Contingency plans…should be prepared and appropriately exercised by all licence holders and authorities concerned" [10]. The IAEA Nuclear Security Series Recommendations on Physical Protection[1]of Nuclear Material and Nuclear Facilities (NSS-13) recommends the following regarding security contingency plans[2]: "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.". [1]

[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. [1] (which is also Revision 5 of INFCIRC/225) uses the term physical protection throughout (including using the term "physical protection regime" for those aspects of a nuclear security regime related to unauthorized removal and sabotage of nuclear material and nuclear facilities). To aid understanding of this publication as guidance on the implementation of INFCIRC/225 Revision 5, 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. Hence, for example, a State's "physical protection regime" comprises those parts of its nuclear security regime that relate to such measures.

[2] Security contingency plans are referred to as contingency plans throughout this document.

OBJECTIVE

1.4. This publication provides guidance to States, competent authorities and operators on how to develop, enhance and maintain a contingency plan. It is intended for use by senior managers and security specialists in developing a contingency plan for nuclear security events, and by competent authorities to develop programmes for the oversight of the contingency plan.

1.5. This publication also emphasizes the interface between the security contingency plan and the emergency plan to ensure an effective, comprehensive, unified and coordinated response to the three types of nuclear security events [4] should both plans be invoked contemporaneously (e.g. because the nuclear security event triggered a nuclear or radiological emergency). Additionally, this publication assists Member States to ensure that "competent authorities and authorized persons are prepared to respond and respond appropriately" as outlined in IAEA Nuclear Security Fundamentals Essential Element 11.

SCOPE

1.6. This publication provides technical guidance for the operator's contingency planning considerations to effectively respond to nuclear security events, and outlines the relationship and interface with the operator's emergency plan. Although they can be recognized as nuclear security events, this document does not attempt to address computer security events or incidents as these are addressed in IAEA-TDL-005; "*Computer Security Incident Response Planning at Nuclear Facilities.*"

STRUCTURE

1.7. Following this introduction, Section 2 outlines elements of the contingency plan, physical layout of nuclear facility, local environment and targets, overview of the physical protection system, application of the threat assessment or design basis threat, and sections of the contingency plan. Section 3 outlines the objectives of the contingency plan and the goals of the contingency plan. Section 4 outlines rules of engagement, response procedures, recapture and recovery, protocols for off-site response, implementing contingency plans, minimization and mitigation methods, and command, control and communications. Section 5 outlines exercising the contingency plan, Section 6 outlines maintenance of the contingency plan and Section 7 outlines information security. Annexes address interfaces of the contingency and emergency plan and provide examples of a response memorandum of understanding, an implementing procedure and an action matrix.

2. ELEMENTS OF CONTINGENCY PLANS

2.1. The operator should develop written contingency plan(s) to provide a timely and effective response to a nuclear security event, which should then be approved by the competent authority as part of the security plan. 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 there is no conflict of assigned responsibilities during an event.

2.2. In developing a contingency plan, the operator will need to begin by identifying the necessary data, criteria, procedures, resources and logistical support. Following this, the contingency plan can begin to be drafted.

2.3. When developing a contingency plan, a number of specific elements should be specifically addressed to ensure that the contingency plan provides all of the information needed during the response to a nuclear security event:

(a) The physical layout (schematic arrangement of parts and area) of the nuclear facility, local environment, and targets (Note – include this if not part of security plan);

(b) Overview of the physical protection system;

(c) The application of the design basis threat or threat assessment;

(d) Sections of the contingency plan;

(e) Objective;

(f) Incident response procedures;

(g) Minimize and mitigate; and

(h) Command, control and communications.

2.4. In this publication, one method of structuring a contingency plan is elaborated, involving dedicating a section of the plan to each of the elements. Other methods of organization are possible, as long as each area are addressed.

2.5. In the following sections, each of these elements is addressed and guidance is provided on developing the sections of the contingency plan for each element.

PHYSICAL LAYOUT OF NUCLEAR FACILITY, LOCAL ENVIRONMENT AND TARGETS

2.6. The first section of the contingency plan should address the physical layout of the nuclear facility, the local environment and targets within the facility, to enable plan implementers to have ready access to this information for coordination of response activities.

2.7. The contingency plan should also include a description of the facility, including the physical structures located on the site, such as—where applicable—barriers, vital and inner areas, onsite fuel storage facilities, and other possible targets. This information should be provided to only those personnel who require the information to implement their part of the contingency plan.

2.8. The contingency plan should not only include a description of the facility, but also the site and the surrounding area. This description should include a description of the location of the site in relation to nearby towns, transportation routes (e.g. rail, water and roads), staging areas, pipelines, airports, hazardous material facilities, and pertinent environmental features that may have an effect upon coordination of response activities. Main and alternate entry routes for off-site response should also be described in the plans and maps should also be included, as appropriate.

OVERVIEW OF THE PHYSICAL PROTECTION SYSTEM

2.9. In addition to a section describing the physical layout of the facility and its environs, the contingency plan should include a section that contains a visual depiction (e.g. maps, drawings and floor plans) as well as a description of the physical protection systems that support and influence the operator's response to a nuclear security event.

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

2.11. The description should include a specific explanation of 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.

APPLICATION OF THE THREAT ASSESSMENT OR DESIGN BASIS THREAT (DBT)

2.12 According to Ref. [3], "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."

2.13 In order to ensure that an appropriate range of different types of nuclear security events are well-addressed in the contingency plan, a section of the plan should be devoted to possible site-specific scenarios following from possible nuclear security events. Site-specific scenarios should be developed by the operator based on possible nuclear security events. The contingency plan should then outline steps that would be taken by response personnel to respond to the site-specific scenarios.

2.14 Appropriate site-specific scenarios for sabotage and/or unauthorized removal of nuclear material should be identified using the State's Threat Assessment or DBT.

SECTIONS OF THE CONTINGENCY PLAN

2.15. When addressing contingency response planning, roles, responsibilities and priorities for protection to deliver an effective response should be defined in the contingency plan. In addition, the minimum number of response personnel required to implement the contingency plan should be determined, and this number should be documented in the contingency plan, the operators' security plan or as required by the relevant competent authorities. The operator should also identify and document off-site response forces needed to support the response.

2.16. The contingency plan should also be consistent and well-integrated with the State's Contingency Plan and the operator's emergency plan (See Annex I for areas of interfaces between the contingency and emergency plans), nuclear material accounting and control (NMAC) plan and off-site response procedures to ensure a integrated and comprehensive and complmentary response.

3. OBJECTIVES OF THE CONTINGENCY PLAN

3.1. A contingency plan is a predefined set of actions for response to unauthorized acts indicative of attempted unauthorized removal or sabotage, including threats thereof, designed to effectively counter such acts.

3.2. Fundamental Principle K states that "[c]ontingency (emergency) plans to respond to unauthorized removal of nuclear material or sabotage of nuclear facilities or nuclear material, or attempts thereof, should be prepared and appropriately exercised by all licence holders and authorities concerned." [10] Further, Ref. [10] adds that "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."

3.3. The contingency plan should be, according to Ref. [1], approved by the competent authority as part of the operator's overall facility security plan, which is prepared by the operator for approval by the competent authority.

3.4. While separate from the emergency plan for the facility, noted in Ref. [2], "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. In Ref. [1], 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 [2], the

emergency plan[3] relates to the response to a nuclear or radiological emergency, whether that emergency is caused by an accident or a malicious act. However, the implementation of the contingency plan and the emergency plan will require coordinated response by physical protection, NMAC and safety personnel." In Ref. [1], the contingency and emergency plans should be comprehensive and complementary.

3.5. The current publication provides detailed information for the operator for drafting, implementing and sustaining a contingency plan.

GOALS OF THE CONTINGENCY PLAN

3.6. According to Ref. [3], "[t]he goals of contingency planning are to ensure a timely and effective response at all levels to any nuclear security event involving a malicious act involving or 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."

3.7. In developing a contingency plan to meet these goals, the operator should ensure that the contingency plan provides clear guidance for the following actions that would need to be undertaken in the case of a nuclear security event:

(a) Determining the credibility of the nuclear security event and the scope of potential consequences for the facility and personnel;

(b) Activating appropriate response plans, personnel and resources to address the nuclear security event;

(c) Taking appropriate actions to protect the facility and personnel and mitigate the consequences of the nuclear security event;

(d) Ensuring that the ability to effectively implement the response plan is maintained throughout the nuclear security event; and

(e) Determining the criteria for the termination of nuclear security events so that operations can be restored.

[3] Emergency plan: 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. [2]

3.8. In addition, contingency plans and emergency plans should be complementary clearly identify the interface between the security contingency plan and the emergency plan to ensure an effective, comprehensive, unified and coordinated response to nuclear security events.

3.9. In addition, contingency plans and emergency plans should be complementary to ensure an effective, comprehensive, unified and coordinated response to nuclear security events.

4. INCIDENT RESPONSE PROCEDURES

RULES OF ENGAGEMENT

4.1. This section of the operator's contingency plan should account for legal aspects or constraints that could affect the contingency response, such as restrictions on the use of force as well as other administrative and logistical requirements for on-site and off-site response personnel, such as those to ensure equipment and other resources are readily available and in working condition.

RESPONSE PROCEDURES

4.2. According to Ref. [1], "the operator should initiate its contingency plans after detection and assessment of any malicious act." However, the criteria by which the operator judges that a malicious act has been detected and assessed should be clearly described in the contingency plan. These criteria should include those that indicate the beginning of a nuclear security event, according to how the situation would be initially perceived by response personnel.

4.3. The criteria for the activation of a response to a nuclear security event could include the identification or notification of certain malicious acts that put the facility at risk in such a way that if unmitigated, would lead to unacceptable radiological consequences or unauthorized removal of material. Some examples could include (but are not limited to):

(a) Armed attack;

(b) Civil disturbance or protest;

(c) Discovery of insider threat;

(d) Loss of off-site power (or station blackout);

(e) Protected area/vital area intrusion; or

(f) Suspected unauthorized removal of nuclear material.

4.4. Member States could also consider identifying and including criteria to activate the contingency plan in situations that do not involve a nuclear security event, but could still require a security response, such as natural disasters, peaceful protest and or a fire. However, the interface with the

emergency response should be carefully considered in this case (more guidance is provided on this topic in Annex I).

4.5. When defining the criteria for activating the contingency plan(s), careful consideration should be given to conditions taken into account in the emergency classification used at activating appropriate level of the emergency response as required in GSR Part 7 [2], so that any coordination with regard to notification and activation should be ensured accordingly.

4.6. The contingency plan should also describe criteria used to determine when to terminate the response to a nuclear security event. These criteria would determine when to return the facility to secure security posture once the threat has been neutralized or the facility is no longer at risk.

4.7. In this section of the operator's contingency plan, the operator should specify areas, such as the target set equipment, control room, which require additional protection as well as potential adversary routes and timelines to those areas and ensure timelines are appropriate for response personnel to implement their actions in each scenario. The plans should also include response positions that provide protection for responders and will enable response personnel to appropriately respond to the nuclear security event. In addition, provisions should be included in the plan to provide response personnel with the appropriate equipment needed to respond to the nuclear security event, such as weapon systems, protective equipment, communications, transportation and other response equipment.

4.8. This section of the contingency plans should also address ensuring that procedures, roles and responsibilities, and resources are identified and in place in advance. In developing an effective plan, regardless whether the response force is based on-site or off-site, the operator should develop site-specific implementing procedures for each site-specific scenario included in the contingency plan. The ultimate aim of the contingency response planning is to return the facility to a secure security posture.

4.9. A section of the contingency plan should specifically address the on-site response forces. Notably, the plan should specify that guards and on-site response forces assigned to implement the contingency plan—which may include on-site military and or law enforcement personnel—should be suitably trained and qualified in those duties, available to respond at all times and should not be assigned other duties or responsibilities that could negatively impact the implementation of the contingency response.

4.10. In order to aid execution of the contingency plan, the operator would consider capturing this information within an action matrix. (see Annex IV).

4.11. 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 would describe the specific actions, areas of responsibility, resources and associated timelines for implementation of the operators contingency response by on-site response forces.

PROTOCOLS FOR OFF-SITE RESPONSE

4.12. In addition to the section of the contingency plan referring to the on-site response forces, arrangements for off-site response forces should be discussed in a separate section, including a reference to a description of any protocols established between the operator and the off-site response force organization.

4.13. Protocols such as written Memoranda of Understanding (MOU) should be be established between the operator and relevant off-site response force organizations. The purpose of such protocols is to facilitate cooperation, understanding and arrangements between on-site and off-site response forces and to integrate the off-site response forces into the overall contingency response planning process. Challenges may occur in relation to delivering off-site response protocols, such as securing resources, response times, sensitive information considerations, integrated secure communications and facility familiarity, and should be considered in the contingency plan. An example of a response memorandum of understanding is included as Annex II.

4.14. Protocols should outline the roles and responsibilities of the operator and the response force organization in the case of a nuclear security event. More specifically, protocols should: establish incident command structure to eliviate the potential for confusion by any responding agencies, specify responsibilities for each agency and identify the communications methods required at all levels of response; provide a general description of the number of personnel for each agency responding, the response capabilities; i.e., weapons, equipment, etc., and timelines for personnel immediately available and those personnel that will be arriving at a later time ; and provide timely reception, marshalling and coordination of response activities. This would include the identification of suitable secure locations, in close proximity to the facility, where responders could receive a situational brief to enable them to plan and prepare their response.

4.15. In addition, the protocols should specify: the availability of key personnel and any additional information (i.e, maps, floor plans, equipment diagrams) necessary to assist in command decisions, briefings, assignment of responders, and situational awareness; locations that have adequate utilities, such as sanitation, water and electricity to sustain operations; and equipment needed to respond to the nuclear security event, such as weapon systems, protective equipment, communications, transportation, locations and capabilities of equipment staged on-site and off-site.

4.16. Provisions for a periodic review of the protocols for off-site response in concert with the review of the operator’s security plan should be made. This could include reviewing that the protocols are consistent with and can operate in conjunction with the contingency and emergency plans (see Annex

I) and reviewing and renegotiating as necessary at the request of either party if changes occur to the governing conditions such as operating regulations, competent authorities or threat levels (DBT).

IMPLEMENTING CONTINGENCY PLANS

4.17. A section of the contingency plan should also address the implementation of the contingency plan. Operators should establish and maintain procedures containing predetermined actions to be taken in the event that the contingency plan is initiated. To enable immediate response, these procedures would be developed to enable unified command and control through provision of specific guidance that identify the steps to be taken and decisions to be made by each member of the response organization. An example implementing procedure is provided to demonstrate how to develop written procedures that implement the requirements of the contingency plan in Annex III.

RECAPTURE AND RECOVERY

4.18. Protocols should be established to outline the roles and responsibilities of the operator and with off-site response forces for material that has left the facility. For on-site, as suggested in Ref. [3] these will include notifications, the operator processes to continue to look for missing material, securing the area where the material was stored and protecting as a crime scene.

4.19. For off-site response by the operator; i.e., “hot pursuit” ensure all coordinations with State authorities and off-site responders are detailed and in accordance with all applicable laws and regulations.

4.20 Recovery actions taken by the operator to coordinate securing and return of material to the facility would be described in detail to include who will be responsible for transport and preservation of evidence for potential criminal proceedings.

MINIMIZE AND MITIGATE

4.21. This section could be populated by way of flow diagrams, computer modelling or an action matrix.

4.22. An action matrix is a planning tool that can be used by response personnel to inform timely decision making and specify procedures for the steps to respond to a specific type of nuclear security event. For each type of nuclear security event, specific actions, roles and responsibilities, resources and associated timelines would be assigned in the action matrix in a manner that prevents conflict in duties and promotes interoperability across the contingency and emergency response plans.

4.23. The operator’s action matrix, or suitable alternative, would be based on the scenarios outlined in the contingency plan as well as the criteria for contingency response, and should include the following information:

(a) A short heading describing the type of event (i.e. Event 1: Bomb Threat);

(b) A brief narrative of an activity that identifies the beginning of an initiating event, which provides enough information to allow response personnel to establish initiation of the contingency plan;

(c) Responders who could be assigned duties and actions as a result of an initiating event;

(d) Specific duties and the steps to be taken by responsible personnel, including initial alerts or event notifications, assessment, communication, activation of response, mitigating actions (denial, containment, recapture, recovery, forensics), and return to normal operations; and

(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 to the extent that it could hinder navigation by response personnel or their subsequent decision making.

COMMAND, CONTROL AND COMMUNICATION

4.24. Command, control, and communication—including coordination, management, chain of command, handover and delegation of authority during a contingency response—should be documented in the contingency plan. These aspects should be integratable to those in the emergency plan to allow for effective response if both plans are invoked contemporaneously. All communication methods and protocols would need to be accounted for, including their interoperability and how they would be implemented and maintained during the event.

5. EXERCISING THE CONTINGENCY PLAN

5.1. Once the contingency plan is in place, they need to be regularly exercised and reviewed in order to maintain their usefulness and to contribute to continuous improvement. In addition, sensitive information relevant to the contingency plans needs to be protected. The following sections address these three aspects of maintaining the contingency plan.

5.2. As part of the discussion of contingency plans, Ref. [1] recommends that "[t]he 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."

5.3. Specifically, the operator should ensure that all personnel involved in contingency response undertake initial training as well as periodic training and participate in exercises of the contingency plan and emergency response plan to the appropriate level commensurate with their roles and responsibilities. The operator should also conduct joint exercises between safety, NMAC and security to demonstrate unified communication, command and control, handover, interfacing and the interoperability between contingency and emergency planning. Joint security exercises with the facility and off-site organizations should also be undertaken to test and practise implementation of the contingency plan as well as the coordination between the contingency and emergency plans.

5.4. Training and exercises could include table top exercises, limited scope testing, classroom lectures, familiarization walk downs, force on force and/or performance based activities to validate the components of the contingency plan. Training and exercises should evaluate the ability of response personnel to implement of the contingency plan. The ability of personnel to implement the plan could be evaluated based on knowledge of topics such as:

(a) Implementing procedures;

(b) Facility, targets, physical protection systems and defense-in-depth measures;

(c) DBT to the facility;

(d) Response equipment;

(e) Response positions and timelines; and

(f) Steps to be taken by individual and or groups in particular situations.

5.5. Alongside the training and exercises, the operator should develop an evaluation process to identify lessons learned from the training and exercises that could be incorporated into a corrective action programme to further improve and refine the plans. For example, operators could document scenarios and participants for all drills and exercises. This could include a documented post-exercise critique in which participants identify best practices, areas for improvement deficiencies or other findings in relation to performance, plans, equipment or strategies. Issues identified that decrease the effectiveness of the physical protection regime would then be recorded in the operator's corrective action programme for timely corrections to the appropriate programme area. Issues recorded into the corrective action programme should be protected properly, and communicated on a need-to-know basis, according to information security requirements of the competent authority.

6. MAINTENANCE OF THE CONTINGENCY PLAN

6.1. In Ref. [1], it is recommended that operators establish a process to monitor and manage physical protection elements. Accordingly, operators should ensure that the contingency plan continues to

meet risk mitigation requirements over the long term. This can be accomplished by periodic and independent reviews, audits, testing, and maintenance of the contingency plan in accordance with the requirements of the competent authority.

6.2. Such a process should include updating the contingency plan as soon as reasonably practicable after any changes occur in personnel, procedures, equipment, or facilities that may have an adverse affect on the plan; ensuring revisions to the contingency plan are submitted to and approved by the relevant competent authorities; and regularly reviewing interoperability with emergency plans, NMAC and all organizations involved in the contingency plan.

6.3. Protocols that are relevant to the contingency plan, such as an MOU's made between the operator and local, state, and national agencies, should also be reviewed. They should be conducted at required intervals or as necessary, in order to ensure expected performance requirements are being met.

6.4. Impartial and unbiased assessments of the contingency plan should also be performed at intervals determined by the competent authority. These assessments should be audited by competent personnel, independent of the security programme.

6.5. The results of the reviews, audits, and performance evaluations of the contingency plan should constitute part of the operator's lessons learned and corrective action process. They should be available to the operator's management to enable management to assess the findings, recommendations and implement corrective actions when needed.

6.6. All records related to reviews and audits as well as other documentation should be retained in accordance with the requirements of the competent authority.

7. INFORMATION SECURITY

7.1. The contingency plan could contain sensitive information that would need to be be protected properly according to information security requirements of the competent authority. Information management procedures should define that distribution of sensitive information is limited to appropriate individuals, including off-site agencies and external stakeholders, whose trustworthiness has been appropriately determined, on a need-to-know basis. Controls applied to sensitive information could include records of its receipt, location, dispatch and destruction. There should also be procedures to ensure the integrity and availability (on a need-to-know basis) of the information critical to appropriate response. This includes information systems (such as detection/assessment systems and communication systems.)

REFERENCES

[1] 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 (January 2011).

[2] INTERNATIONAL ATOMIC ENERGY AGENCY, Preparedness and Response for a Nuclear or Radiological Emergency, IAEA General Safety Requirements No. GSR Part 7, IAEA, Vienna (2015)

[3] INTERNATIONAL ATOMIC ENERGY AGENCY, Physical Protection of Nuclear Material and Nuclear Facilities (Implementation of INFCIRC/225/Revision 5) Draft Implementing Guide, NST 023 (2015). [TO BE PUBLISHED]

[4] INTERNATIONAL ATOMIC ENERGY AGENCY, Developing a National Framework for Managing the Response to Nuclear Security Events, Draft Implementing Guide, NST 004 (December 2016). [TO BE PUBLISHED]

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

[6] INTERNATIONAL ATOMIC ENERGY AGENCY, Amendment to the Convention on the Physical Protection of Nuclear Material Amendment (8 May 2016)

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

[8] INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Recommendations on Nuclear and Other Radioactive Material out of Regulatory Control, IAEA Nuclear Security Series No. 15, IAEA, Vienna (January 2011).

[9] INTERNATIONAL ATOMIC ENERGY AGENCY, Use of Nuclear Material Accounting and Control for Nuclear Security Purposes at Facilities, Implementing Guide, IAEA Nuclear Security Series No. 25-G, IAEA, Vienna (May 2015)

[10] INTERNATIONAL ATOMIC ENERGY AGENCY, Convention on the Physical Protection of Nuclear Material, INFCIRC/274/Rev.1, IAEA, Vienna (February 1987); Amendment to the Convention on the Physical Protection of Nuclear Material, GOV/INF/2005/10–GC(49)INF/6, IAEA, Vienna (2005).

ANNEX I – INTERFACE OF THE CONTINGENCY AND EMERGENCY PLANS

This annex lists areas of interfaces between the contingency and emergency plans. Each section highlight the main areas of interface and are supported with examples within these areas.

FACILITY DESIGN FEATURES

a. Initial site selection and design takes physical protection into account as early as possible and that safety and security functions are mutually supportive and avoid conflicts 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 and contingency planning:

- Physical layout of nuclear facility and local environment (e.g. demographics and topography)
- Safety related equipment and radioactive material requiring protection against unauthorized removal /sabotage based upon a graded approach
- Location and protection of control rooms, emergency response facilities and alarm stations
- Design of fire safety features (fire doors, suppression systems, etc.)
- Emergency evacuation/access routes (including physical barriers along these routes)

b. Coordination of changes to the layout or design of a nuclear facility that may impact security and/or emergency response.

PLANS AND PROCEDURES

a. Contingency and emergency plans should take into account the respective security and safety requirements.

b. Consistency between contingency plans and emergency plans

- The contingency and emergency plans are implemented with the appropriate level of response.
- The contingency and emergency plans should be comprehensive and complementary.
- Alignment of off-site emergency plans, procedures and assets, and interaction with on-site security forces (for example, access control; on-site protection).
- Sufficient numbers of security personnel to support an emergency response while maintaining adequate security.

c. Memoranda of Understanding (MOU) with any single off-site response organization are consistent with both the emergency and contingency plans.

ORGANIZATION STRUCTURE

a. The roles and responsibilities are identified between the emergency plan and the contingency plan in order to:

— Define the coordinated response, including decision making

— Respond with appropriate number of qualified personnel, with appropriate and sufficient equipment, and within required timelines

— Competing priorities (dual assignments; unavailability) for security personnel during an emergency response

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

— Location of unified command and control facility may evolve with progression of the event

— On site and off site authority and responsibility

IMPLEMENTATION OF THE CONTINGENCY PLAN

Initiating event[4]

a. Assessment of an event:

— Identification of initiating events that require coordination between emergency and contingency plans

— Coordinated activation of both internal emergency and security personnel, which may include but is not limited to

— Arranging access to vital areas

— Moving physical barriers

— Relocation of security personnel based upon a radiological event

— Time line and criteria for activation may be different for contingency plans versus emergency plans. Of note would be site Emergency Action Levels that may call for the

[4] IAEA, Developing a National Framework for Managing the Response to Nuclear Security Events, Draft Implementing Guide NST004 [TO BE PUBLISHED]

activation of the contingency plan for other than a security initiated event or for activation of the emergency plan in case of a nuclear or radiological emergency triggered by a nuclear security event.

On-site

a. Coordination between the emergency plan and the contingency plan to ensure protection from all hazards, including radiological hazards.

b. Coordination between the emergency plan and the contingency plan to ensure safe movement of emergency workers necessary to perform required actions.

c. Coordination of security measures for all personnel.

d. Emergency evacuation of personnel, as prescribed in the emergency plan, for rapid and safe egress to designated emergency planning zones

e. Coordination in relation to accountability of personnel and nuclear/radiological material following an emergency evacuation.

f. Identification of safety-related equipment and devices, equipment within vital areas, and hazardous materials that may be adversely affected by the security response actions.

g. Coordination of safety and security response as event progresses and adaptation of protective strategies against threat.

— Re-evaluation of target(s) as event progresses

— Adapting protective strategies as event progresses

Off-site

a. 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

a. Secure internal communication systems between contingency and emergency response personnel.

b. Awareness and understanding of contingency and emergency response actions and terminology.

c. 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 severity of the event.

f. Coordinated notification to off-site agencies.

g. Coordination of the public communication strategy established regarding 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 upon the audience (e.g. media, local population, other nuclear facilities, other stakeholders) and timing of information release.

RECOVERY

a. Prioritized and coordinated recovery team efforts (all hazards, medical, security, etc.)

— Clearing of areas and site equipment (e.g. searching for additional or residual security concerns) prior to resuming operations.

b. Preservation of forensic evidence (e.g. unnecessary interference with collection or preservation of evidence)

TRAINING AND EXERCISES

a. Initial and periodic training, commensurate with the job and tasks of the contingency and emergency personnel.

b. Exercises are undertaken to test and practise implementation of the contingency plan and joint exercises test and practice coordination between the contingency and emergency plans. Lessons learnt from contingency and emergency, and joint exercises are captured and used to further refine the plans.

SUSTAINABILITY PROGRAMME

a. An effective change control process exists to ensure that any proposed changes of design, layout or procedures are thoroughly evaluated to verify that they do not jeopardize contingency or emergency plans.

b. Periodic review of the contingency and emergency plans.

ANNEX II – EXAMPLE OF A RESPONSE MEMORANDUM OF UNDERSTANDING

This is an example of an MOU. It might not apply to Member States where the response forces are government agencies that are mandated under law to provide response to the facility.

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) agrees to provide an adequate, appropriate and effective response to calls for assistance as a result of a nuclear security event.

— The (Response Forces) agrees 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 threat levels (DBT).

2. Points of Contact

The (Operators designee) will be the primary facility site contact for security and issues with the (Response Forces 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 (Operators 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 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, but not limited to:

(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; and

(f) Logistical support, such as marshalling areas, briefing areas, power supplies,

(g) Accountability of personnel arriving and working on the site at all times,etc.

4.2. Response Forces

The (Response Forces) agrees to provide 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 numbers and estimated time of arrival of each Response Force's primary response and supporting response elements would be specified in an Annex to the MOU and may include the following (but not limited to these):

(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 identifications services;

(g) Technical traffic collision investigation;

(h) Dangerous goods coordinator;

(i) Any other service provided by the Response Forces and/or supporting units deemed necessary by the Incident Commander.

4.2. First Response Forces at the facility

Upon arrival the first Response Forces would receive a reception brief 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 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

The (Operator) and Response Forces agree to have interoperable equipment to facilitate effective communications during security events at the facility, such as:

(a) Direct phone line between the command and control elements;

(b) Compatible command centre radios and frequencies;

(c) Compatible portable security radios and frequencies; and

(d) Other compatible communication devices.

6.2. Maintenance of communications equipment

The following off-site communication resources will be maintained by 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.

9. Limitations of Liability, Indemnification and Insurance

9.1. Response Forces

The Response Forces shall not be liable in any manner whatsoever to the facility, which includes all of its respective staff, servants and agents or their successors and assign 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 .

9.2. 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 related 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.

10. 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 obligations between the parties.

11. Agreement

This MOU constitutes the entire agreement between the parties. There are no other agreements, undertakings, representatives or warranties, collateral, oral or otherwise, related 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

This example, of a bomb warning procedures, is provided as an example of how to use this planning tool to develop written procedures that implement the requirements of the contingency plan.)

Bomb Warning Procedure

1. Purpose

This 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**).

2. 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' offsite, or other third parties who would notify security.

3. Objectives of the Contingency Response

— Validate the warning

— Mitigate the warning

— Minimize potential consequences of the warning

— Inform all decision makers of the event

4. Decisions/Actions

— 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.

5. Responsible Personnel

- **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.

6. Termination of Event

— 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

7. 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 ACTION MATRIX

This is provided as an example of an action matrix to identify the steps to be taken for responding to initiating events. The action matrix could also be represented by way of flow diagrams, computer modelling, or equivalent process.

Initiating 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' offsite, or other third parties who would notify security.				
Responsible Personnel	**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 CAS, and await directions Execute ongoing tactical operations If a bomb is not discovered, communicate to CAS, and await directions	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	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.
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