DEVELOPING A NUCLEAR SECURITY CONTINGENCY PLAN FOR NUCLEAR FACILITIES

DRAFT TECHNICAL GUIDANCE

INTERNATIONAL ATOMIC ENERGY AGENCY

VIENNA, 20XX
CONTENTS

CONTENTS 3

1. INTRODUCTION 1
   Background 1
   Objective 1
   Scope 2
   Structure 2

2. OBJECTIVES OF CONTINGENCY PLANNING 2
   Goals of the contingency plan 3

3. ELEMENTS OF CONTINGENCY PLANS 4
   Physical layout of nuclear facility, local environment and targets 5
   Overview of the physical protection system 5
   application of the threat assessment or design basis threat 6
   Criteria for a contingency response 6
   Contingency response planning 7
   On-site response forces 8
   Protocols for off-site response forces 8
   Implementing procedures 9

4. ACTION MATRIX 10

5. MAINTAINING THE CONTINGENCY PLANS 10
   Exercising the contingency plans 10
   Sustainability of the contingency plan 12
   Protection of information 12

REFERENCES 13

ANNEX I – INTERFACE OF THE CONTINGENCY AND EMERGENCY PLANS 14

ANNEX II – EXAMPLE OF A RESPONSE MEMORANDUM OF UNDERSTANDING 18

ANNEX III – EXAMPLE OF IMPLEMENTING PROCEDURE 23

ANNEX IV – EXAMPLE OF ACTION MATRIX 26
1. INTRODUCTION

BACKGROUND

1.1. It is possible that sabotage of a nuclear facility could be attempted or that nuclear or other radioactive material could be used for malicious purposes. States have responded to this risk by committing to strengthen the protection and control of such material and to respond effectively to nuclear security events.

1.2. The IAEA Nuclear Security Series Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (NSS-13) recommends the following regarding security contingency plans:

“Contingency (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”. [1]

1.3. Each State is responsible for nuclear security, specifically: to provide for the security of nuclear and other radioactive material and associated facilities and activities; to ensure the security of such material in use, storage or in transport; to combat illicit trafficking and the inadvertent movement of such material; and to be prepared to respond to a nuclear security event.

1.4. This guidance addresses the development of contingency plans. 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.

OBJECTIVE

1.5. This publication provides guidance to States, competent authorities and operators on how to develop, enhance and maintain a contingency plan to achieve the objectives of INFCIRC/225/Rev5.

---

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 plan will be described as a contingency plan throughout this document.
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 plans.

1.6. This publication also emphasizes the interface between the security contingency plan and the emergency plan as required in the IAEA Safety Standards Series No. GSR Part 7 [2] to ensure an effective, comprehensive, unified and coordinated response to nuclear security events should both plans be invoked contemporaneously (e.g. because the nuclear security event triggered a nuclear or radiological emergency).

SCOPE

1.7. This publication provides a framework 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.

STRUCTURE

1.8. Following this introduction, Section 2 outlines: (1) objectives of the contingency plan, (2) operator planning considerations, (3) physical layout of nuclear facility, local environment and targets, (4) overview of the physical protection system, (5) application of the threat assessment/design basis threat, (6) criteria for contingency response, (7) response planning, (8) guard/on-site response force, (9) protocols for off-site response forces, (10) implementing procedures, (11) action matrix, (12) exercising the contingency plan, (13) sustainability of the contingency plan, and (14) protection of information.

1.9. Annexes provide (I) example of a response memorandum of understanding, (II) example of implementing procedure, (III) example of action matrix, (IV) interface of the contingency and emergency plan.

2. OBJECTIVES OF CONTINGENCY PLANNING

2.1. 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.

2.2. Fundamental Principle K in Ref. 1 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.” [1] Further, Ref. [1] 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.”

2.3. 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 as part of its
application to obtain a licence.

2.4. While separate from the emergency plan for the facility, noted in Ref. [3], “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 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 contingency
plans and the emergency plan will require coordinated response by physical protection, NMAC and
safety personnel.”

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

GOALS OF THE CONTINGENCY PLAN

2.6. 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.”

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

— Determining the credibility of the nuclear security event and the scope of potential
  consequences for the facility and personnel;

— Activating appropriate response plans, personnel and resources to address the nuclear security
  event;

---

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]
— Taking appropriate actions to protect the facility and personnel and mitigate the consequences of the nuclear security event;
— Ensuring that the ability to effectively implement the response plan is maintained throughout the nuclear security event; and
— Determining the criteria for the termination of nuclear security events so that operations can be restored.

2.8. In addition, contingency plans should 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. ELEMENTS OF CONTINGENCY PLANS

3.1. As noted in the previous section, 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.

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

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

(a) The physical layout of the nuclear facility, local environment, and targets;
(b) The physical protection system;
(c) The application of the design basis threat or threat assessment;
(d) The criteria for a contingency response;
(e) Contingency response planning;
(f) On-site response forces;
(g) Protocols for off-site response forces; and
(h) Implementing procedures.
3.4. In this publication, one method of structuring contingency plans is detailed, involving dedicating a section of the plans to each of the elements. Other methods of organization are possible, as long as each area are addressed.

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

PHYSICAL LAYOUT OF NUCLEAR FACILITY, LOCAL ENVIRONMENT AND TARGETS

3.6. 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.

3.7. The contingency plans 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.

3.8. The contingency plans 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

3.9. In addition to a section describing the physical layout of the facility and its environs, the contingency plans 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.

3.10. 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.

3.11. 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

3.12 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.”

3.13 In order to ensure that an appropriate range of different types of nuclear security events are well-addressed in the contingency plans, a section of the plans 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 plans should then outline steps that would be taken by response personnel to respond to the site-specific scenarios.

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

CRITERIA FOR A CONTINGENCY RESPONSE

3.15 A section of the contingency plans should explicitly outline the criteria for initiating the contingency plans.

3.16 According to Ref. [1], “the operator should initiate its contingency plan 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 plans. 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.

3.17 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):

- Armed attack;
- Civil disturbance or protest;
- Discovery of insider threat;
- Loss of off-site power (or station blackout);
- Protected area/vital area intrusion; or
- Suspected unauthorized removal of nuclear material.

3.18 Member States could also consider identifying and including criteria to activate the contingency plans 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).

3.19. 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.

3.20. The contingency plans 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.

CONTINGENCY RESPONSE PLANNING

3.21. A section of the contingency plans should be explicitly devoted to response planning. 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.

3.22. When addressing response planning, roles, responsibilities and priorities for protection to deliver an effective response should be defined in the contingency plans. 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.

3.23. 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 plans. 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.

3.24. In the contingency plans, 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.

3.25. The contingency plans should also 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.

3.26. The contingency plans should also be consistent and well-integrated with the 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 cohesive response.

ON-SITE RESPONSE FORCES

3.27. A section of the contingency plans should specifically address the on-site response forces. Notably, the plans should specify that guards and on-site response forces assigned to implement the contingency plans—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.

3.28. Protocols for response should be established between the operator and any on-site military and or law enforcement response personnel, and these protocols should be referenced and described in the contingency plans. 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 FORCES

3.29. In addition to the section of the contingency plans 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.

3.30. 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 plans. An example of a response memorandum of understanding is included as Annex II.

3.31. 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 eliminate 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.

3.32. 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.

3.33. 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, statutory authorities or threat levels (DBT).

IMPLEMENTING PROCEDURES

3.34. A section of the contingency plans should also address the implementation of the contingency plans. Operators should establish and maintain procedures containing predetermined actions to be taken in the event that the contingency plans are 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.

3.35. In order to aid execution of the contingency plan, the operator would consider capturing this information within an action matrix, as described in the next section of this publication (see Annex IV).
4. ACTION MATRIX

4.1. 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.

4.2. The operator’s action matrix, or suitable alternative, would be based on the scenarios outlined in the contingency plans 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.

5. MAINTAINING THE CONTINGENCY PLANS

5.1. Once the contingency plans are 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 plans.

EXERCISING THE CONTINGENCY PLANS

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.” [1]

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 plans and emergency response plans 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 plans 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 plans. 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:

- Implementing procedures;
- Facility, targets, physical protection systems and defense-in-depth measures;
- DBT to the facility;
- Response equipment;
- Response positions and timelines; and
- 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.
SUSTAINABILITY OF THE CONTINGENCY PLAN

5.6. 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, and testing of the contingency plan in accordance with the requirements of the competent authority.

5.7. 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 plans 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.

5.8. Protocols that are relevant to the contingency plans, 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.

5.9. 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.

5.10. 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.

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

PROTECTION OF INFORMATION

5.12. The contingency plan could contain sensitive information that would need to 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.
REFERENCES


ANNEX I – INTERFACE OF THE CONTINGENCY AND EMERGENCY PLANS

1. 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.

2. Plans and Procedures

a. In the case of separate regulations for security and safety, contingency and emergency planning takes 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.
- 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.

3. 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

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.

4. Implementation of the Contingency Plan

Initiating Event

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 activation of contingency plans 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 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.
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
1 Off-Site

2 a. Coordination between the emergency and contingency plan to ensure protection from all
3 hazards, including radiological hazards, of off-site security response assets, and the potential
4 need for rapid ingress/egress of response personnel.

5 5. Communications

6 a. Secure internal communication systems between contingency and emergency response
7 personnel.
8 b. Awareness and understanding of contingency and emergency response actions and
9 terminology.
10 c. Redundant methods of communication for both contingency and emergency response.
11 d. Communication processes established between the contingency and emergency response in
12 order to ensure a coordinated response.
13 e. Coordination of notification to appropriate levels of contingency and emergency response
14 consistent with the potential severity of the event.
15 f. Coordinated notification to off-site agencies.
16 g. Coordination of the public communication strategy established regarding contingency and
17 emergency response that provides for transparency while maintaining the appropriate level of
18 confidentiality (e.g. not disclosing security or safety related sensitive information) based upon
19 the audience (e.g. media, local population, other nuclear facilities, other stakeholders) and
20 timing of information release.

21 6. Recovery

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

27 7. Training and Exercises

28 a. Initial and periodic training, commensurate with the job and tasks of the contingency and
29 emergency personnel.
30 b. Exercises are undertaken to test and practise implementation of the contingency plan and joint
31 exercises test and practice coordination between the contingency and emergency plans.
32 Lessons learnt from contingency and emergency, and joint exercises are captured and used to
33 further refine the plans.

34 8. Sustainability Programme

35 a. An effective change control process exists to ensure that any proposed changes of design,
36 layout or procedures are thoroughly evaluated to verify that they do not jeopardize
37 contingency or emergency plans.
38 b. Periodic review of the contingency and emergency plans.
18

ANNEX II – EXAMPLE OF A RESPONSE MEMORANDUM OF UNDERSTANDING

(Note: This is an example of a MOU that may 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 (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 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:

(i) Information regarding any radiological and technical issues;

(ii) On-site protection of workers;
(iii) Site maps and facility floor plans;
(iv) Escorts;
(v) Compatible communications; and
(vi) Logistical support, such as marshalling areas, briefing areas, power supplies,
(vii) 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):

(i) Tactical response units;
(ii) Crisis negotiator;
(iii) Canine team;
(iv) Explosive disposal;
(v) Emergency services (e.g. local law enforcement, medical services, hazmat teams);
(vi) Forensic identifications services;
(vii) Technical traffic collision investigation;
(viii) Dangerous goods coordinator;
(ix) Underwater search and recovery;
(x) 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:

(i) Direct phone line between the command and control elements;
(ii) Compatible Command centre radios and frequencies;
(iii) Compatible portable security radios and frequencies; and
(iv) Other compatible communication devices.

6.2. Maintenance of communications equipment

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

(i) Dedicated direct telephone link between the CAS and Response Forces;
(ii) 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

Bomb Threat Procedure

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

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 Threat).

2. Event Description
Bomb threats may be expressed by telephone, by mail (letter or email), by a hand delivered message, or by some other means. Threats may be given directly or indirectly through a law enforcement agency, mass media organization, or some other third party. Threats 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 threat
- Mitigate the threat
- Minimize potential consequences of the threat
- Inform all decision makers of the event

4. Decisions/Actions
- Gather and evaluate information from the bomb threat 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 threat
  - 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 threat, 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.

5. **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

6. **Data and Supporting Guidance**

   - Bomb Threat Checklist
   - “Discovery of explosives” nuclear security event procedure
   - Emergency evacuation plan for bomb threat
• 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 how to develop 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 Threat

Event Description: Bomb threats may be expressed by telephone, by mail (letter or email), by a hand delivered message, or by some other means. Threats may be given directly or indirectly through a law enforcement agency, mass media organization, or some other third party. Threats also may be received and communicated by plant personnel, authorities’ offsite, or other third parties who would notify security.

<table>
<thead>
<tr>
<th>Responsible Personnel</th>
<th>CAS</th>
<th>Guards/ Response Forces</th>
<th>Security Management</th>
<th>Facility Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Actions</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Initial receipt or notification of bomb threat</td>
<td>- Upon request, conduct search for suspected bomb(s)</td>
<td>- Assess threat, and if required direct CAS to deploy guards to conduct search.</td>
<td>- Receive briefing from security management or CAS</td>
<td></td>
</tr>
<tr>
<td>- Notify security management</td>
<td>- If a bomb is confirmed, cordon, communicate location and details to CAS, and await directions</td>
<td>- Direct CAS to notify facilities operations</td>
<td>- If a bomb is not discovered, await recommendations from security management.</td>
<td></td>
</tr>
<tr>
<td>- Notify facilities operations</td>
<td>- Execute ongoing tactical operations</td>
<td>- Receive search results.</td>
<td>- If a bomb is confirmed, await recommendations from security management.</td>
<td></td>
</tr>
<tr>
<td>- Deploy response personnel</td>
<td>- If a bomb is not discovered, communicate to CAS, and await directions</td>
<td>- Report results to facility operations.</td>
<td>- If a bomb is confirmed, consider secondary hazards (e.g., effects to safety equipment or personnel).</td>
<td></td>
</tr>
<tr>
<td>- If a bomb is discovered, transition to the “Discovery of explosives” procedure</td>
<td>- If a bomb is confirmed, cordon, communicate location and details to CAS, and await directions</td>
<td>- Advise facility operation on recommendations.</td>
<td>- Activate emergency plan.</td>
<td></td>
</tr>
</tbody>
</table>

Supporting Guidance

- Bomb Threat Checklist
- “Discovery of explosives” nuclear security event procedure
- Emergency evacuation plan for bomb threat
- Facility maps and floor plans
- Specific guard response procedures

- “Discovery of explosives” nuclear security event procedure
- Emergency evacuation plan for bomb threat
- Facility maps and floor plans
- Off-site response contact list
- On-site response contact list

- Bomb Threat Checklist
- “Discovery of explosives” nuclear security event procedure
- Emergency evacuation plan for bomb threat
- Facility maps and floor plans
- Off-site response contact list
- On-site response contact list

- On-site emergency plan
- Emergency evacuation plan for bomb threat
- Facility maps and floor plans
- Off-site response contact list
- On-site response contact list
<table>
<thead>
<tr>
<th>list</th>
</tr>
</thead>
<tbody>
<tr>
<td>- On-site response contact list</td>
</tr>
</tbody>
</table>