PNRA-RG-926.02 September, 2023

MANAGEMENT OF NUCLEAR SECURITY EVENTS INVOLVING RADIOACTIVE SOURCES

REGULATORY GUIDE

PAKISTAN NUCLEAR REGULATORY AUTHORITY

For Further Details

Directorate of Regulatory Framework

PAKISTAN NUCLEAR REGULATORY AUTHORITY
P.O. Box 1912, Islamabad

www.pnra.org

TABLE OF CONTENTS

1. INTRODUCTION

Radioactive sources are widely used for the benefit of mankind for different applications in medicine, industry, agriculture, research and education. If radiation safety & protection principles and security measures are not adequately considered during use and handling of radioactive sources, these may cause harmful effects to people and the environment due to radiation exposure and radioactive contamination. Effective regulatory oversight is therefore required to ensure safe and secure use of radioactive sources.

Pakistan Nuclear Regulatory Authority (PNRA) has developed a comprehensive regulatory framework to ensure safety and security of radioactive sources throughout their life cycle. Under the regulatory framework, the prime responsibility for safety and security of radioactive sources lies with the licensee. PNRA "Regulations on Security of Radioactive Sources - (PAK/926)" establish requirements for the security of radioactive sources during manufacture, use, storage and transport.

These regulations further specify requirements for managing security events related to radioactive sources. Regulation 7(4) of PAK/926 requires licensees to cooperate and coordinate with relevant organizations having their role in response to contingencies related to security of radioactive sources. Regulation 10 of PAK/926 sets timelines for event notification and reporting mechanism. It also requires licensees to take immediate remedial actions and inform local Law Enforcement Agencies (LEAs). In addition, Regulations 11(3), 12(3), 13(3) and 16(1) of PAK/926 set requirements for responding to security events.

The management of security events is different from events related to radiation safety because of the deliberate, criminal and illegal intent of an adversary which requires different strategies and plans. Managing a security event is complex and may involve various national organizations. Depending on the impact of the security event, the licensee may need to coordinate with PNRA and other relevant organizations.

This Regulatory Guide (RG) describes guidance for licensees in order to develop integrated elements for preparedness and response to security events involving radioactive sources and establish effective mechanism for reporting of security events.

2. OBJECTIVE

This RG provides guidance to licensees for effective management of security events involving radioactive sources.

3. SCOPE

This RG is applicable to management of security events involving radioactive sources. It also covers the interface of security events with radiological emergency, where so applicable.

4. TYPES OF SECURITY EVENTS

The security events have different types based on the nature of threat, potential consequences, handling, response actions, required resources and involvement of response organizations.

The types of security events are as follows:

i. Actual or attempted theft, unauthorized removal or loss of control over radioactive sources;

ii. Actual or attempted sabotage;

iii. Unauthorized transfer or transport of radioactive sources;

iv. Unauthorized access to secured area or source location;

v. Failure of security system that is essential for the security of radioactive sources;

vi. Loss or unauthorized disclosure of sensitive information;

vii. Any adverse condition during transportation that restrict movement of the vehicle carrying radioactive sources (e.g. forceful stopover of vehicle, accident conditions, intentional misrouting, civil disturbance, etc.);

viii. Threat alerts received by the licensee;

ix. Detection and discovery of radioactive sources in scrap or other locations;

x. Other malicious acts related to radioactive source (such as cyber-attack, theft/loss of keys or access control card, suspected tampering with security system, discovery of prohibited items, etc.); and

xi. Any situation that may lead to occurrence of the above events.

5. PREPAREDNESS FOR SECURITY EVENTS

Managing a security event requires pre-defined set of actions during preparedness by the licensee as per its approved Physical Protection Plan for effective response. The goal of preparedness for security events is to ensure that adequate capabilities and arrangements are in place with the licensee for timely, controlled, coordinated and effective response to security event. The licensee should maintain preparedness through identification and maintenance of necessary resources (human,

technical and financial) in order to deal with any kind of security event.

The preparedness for security events is an integrated set of elements which are described in following sub-sections.

5.1. Identification of Roles and Responsibilities

Regulation 15(1) of PAK/926 requires the licensee to ensure that the security related responsibilities and authorities of each individual are identified amongst the defined operating personnel, security personnel and response personnel. The licensee should be aware of responsibilities of these personnel as defined in its Physical Protection Plan. Moreover, the licensee should also ensure that all its individuals are aware of their roles and responsibilities and are regularly trained to perform respective functions.

Following are some functions to be performed by the licensee's personnel for better management of a security event:

i. Identification of sensitive information and its protection according to national regulations;
ii. Prompt identification and correction of problems affecting security in a manner commensurate with their importance;
iii. Management of resources in accordance with Physical Protection Plan;
iv. Development and execution of training program;
v. Conduct of periodic drills and exercises;
vi. Testing and maintenance of security system and radiation detection equipment;
vii. Security event assessment and subsequent communication to on-site response personnel;
viii. Activation of response;
ix. Lodging of First Information Report (FIR) at local police station;
x. Cooperation, coordination and communication of response activities with PNRA and other response organizations;
xi. Arrangement for securing the site;
xii. Execution of directions received from PNRA and other response organizations;
xiii. Taking and recording photographs at the scene, where possible;
xiv. Event analysis (identification of causes, circumstances and consequences of event); and
xv. Identification and execution of corrective actions.

Considerations should also be given at the preparedness stage for any changes in roles and responsibilities of the licensee's personnel in case, a security event escalates to a radiological emergency.

5.2. Capabilities and Resources

PAK/926 requires the licensees to ensure availability of adequate resources (human, technical and financial) and capabilities for effective security of their radioactive sources.

The licensee should identify capabilities and resources that are needed for securing its radioactive sources and to respond to different types of security events as outlined in Section 4. The licensee should ensure that required capabilities and resources are properly maintained. These mainly include:

i. Sufficient, qualified and trained operating, security and response personnel;
ii. Security systems, protective equipment, radiation detection equipment and ancillary equipment;
iii. Documentations including plans, procedures and protocols;
iv. Allocation of funds for security of radioactive sources; and
v. Arrangements for notification, communication, coordination and support needed from other organizations.

These capabilities and resources should be maintained in a manner that allows their effective use in case of a security event. Maintenance of capabilities and resources includes:

(a) Workforce management;
(b) Training and re-training of all personnel;
(c) Financial resources for procurement, maintenance, calibration and replacement of security systems, equipment and tools;
(d) Conducting periodic exercises;
(e) Performance monitoring and assessment;
(f) Promotion of feedback to identify necessary improvements; and
(g) Updating plans, procedures and protocols.

5.3. Systems and Measures for Detection and Response

Detection and response systems are primarily designed to deter, detect and respond to a security event. Detection system is associated with intrusion alarm sensing, access control, monitoring of personnel and radiation detection equipment. Response system is associated with assessment of instrument alarm and information

alerts; intervention and neutralization of adversary's act; communication; assessment and analysis of event happening, recovery and appropriate secure management of radioactive sources in case of a security event.

Regulations 11, 12 and 13 of PAK/926 require the licensee to implement measures to detect and respond to unauthorized removal/access to radioactive sources during manufacture, use, storage and transport.

Detection measures include following, where applicable:

i. Visual observation measures;
ii. Electronic intrusion sensors;
iii. Accountancy records;
iv. Seals and other tamper indicating devices;
v. Process monitoring systems; and
vi. Physical checks.

In order to implement these measures, the licensee should have the following system for detecting a security event:

a) Intrusion Detection System:
   (i) Passive Infrared Sensors;
   (ii) Mono-static Microwave Sensors;
   (iii) Dual Technology Motion Sensors;
   (iv) Balanced Magnetic Switch (BMS);
   (v) Glass Break Sensors; and
   (vi) Tamper Indicating Devices.
b) CCTV Camera System;
c) Electronic Access Control System (such as electronic lock, proximity card or biometric system); and
d) Radiation Detection Equipment (fixed, handheld or portable).

The equipment used for support in responding to a security event mainly include:

a) Radiation Detection Equipment:
   (i) Gamma and neutron dose rate/survey meters (high dose rate measurements may require a telescopic arm type survey meter);
   (ii) Passive dosimeters (TLDs, film badges) and electronic personal dosimeters; and
   (iii) Gamma ray spectrometer.
b) Personal Protective Equipment (PPE):

(i) Respiratory protective equipment;
(ii) Gloves;
(iii) Footwear (can include over boots or shoe covers);
(iv) Undergarments, such as vests; and
(v) Protective suits or other outer clothing (e.g. lead aprons).

c) Ancillary Equipment:
(i) Communication equipment;
(ii) Decontamination equipment;
(iii) Photographic camera;
(iv) Packaging and transport containers; and
(v) Tweezers and tongs.

The security system should be integrated in the facility security control room (also called as Central Alarm Station).

The licensee should also introduce sufficient 'Delay' measures after the 'Detection' in order to interrupt and neutralize the adversary by response personnel. Delay measures include security fences, structural barriers, doors, locking mechanism, etc.

5.4. Implementing Procedures

Regulation 15(5) of PAK/926 requires the licensee to submit a Physical Protection Plan for radioactive sources to PNRA for approval. Subsequently, Regulation 15(6) of PAK/926 requires the licensee to identify, prepare and maintain necessary procedures for implementation of its Physical Protection Plan.

To comply with requirements of PAK/926, the applicable procedures to be used in case of a security event should be identified, prepared, reviewed and approved by the licensee and, as appropriate, should be tested as a part of evaluation of the security system on periodic basis.

Procedures for managing a security event should address instructions for personnel to assess, coordinate and respond to a security event. Examples of such procedures include:

i. Information gathering and analysis (collect information on alerts);
ii. Assessment of security event;
iii. Response activation;
iv. Notification and reporting to PNRA;
v. Dissemination of information to other relevant response organizations;

vi. Safety and security arrangements at scene;
vii. Regaining control operations;
viii. Coordination and communication; and
ix. Management and retention of records and evidences.

5.5. Testing and Evaluation of Physical Protection Plan and Security System

Regulation 5 of PAK/926 requires the licensee to conduct assessment/ evaluation of the security system on periodic basis to ensure the effectiveness of the security system. Regulation 15(5) of PAK/926 requires the licensee to test and evaluate its physical protection plan at approved intervals and revise, if needed.

The licensee should test, evaluate and improve the arrangements for preparedness and response to security events through performance testing, vulnerability assessment, tabletop exercises, drills and force on force exercises. The licensee should ensure participation of its relevant personnel in such testing and evaluation.

The licensee should develop testing and evaluation process to continually improve the effectiveness of capabilities of its personnel for responding to security events. This process may include:

i. Identify the test type;
ii. Define test purpose, objectives, standards and responsibilities;
iii. Create a test plan;
iv. Identify and develop scenarios;
v. Identify elements and locations to be tested;
vi. Define testing methodology and evaluation criteria;
vii. Identify resource requirements;
viii. Coordinate and obtain necessary approvals for the test;
ix. Conduct the test;
x. Identify compensatory measures;
xi. Collect data during testing;
xii. Analyze the data; and
xiii. Document the results.

The conduct of periodic drills and exercises should imitate a real situation as closely as possible. For this purpose, the licensee should develop security scenarios against possible security events. Guidance for development of exercise scenarios is provided in Annexure-I.

The licensee should also conduct exercises in order to evaluate and improve the effectiveness of security system, response arrangements and interface with other plans such as radiation emergency plan. Such exercises may also be conducted for better management of interfaces such as:

(a) Establishment and implementation of a unified command and control system;

(b) Identification of dual assignments and priorities of response personnel;

(c) Familiarization of response forces with facility secured areas, safety terminologies and radiation protection principles;

(d) Coordination for safe movement of first responders and law enforcement agencies necessary to perform required actions;

(e) Coordination for rapid and safe evacuation of facility personnel to designated assembly areas;

(f) Coordination for protection against potential threats and possible rapid ingress/egress (subject to search before leaving the facility); and

(g) Coordination to address the post-event recovery operations.

6. NOTIFICATION AND REPORTING OF SECURITY EVENTS

As soon as a security event (as identified under Section 4 of this RG) involving radioactive source during manufacturing, use, storage and transport is detected, the licensee should immediately notify the event to National Radiation Emergency Coordination Center (NRECC) of PNRA and inform other response organizations (if necessary) for recovery and mitigation actions.

6.1. Notification to Local Law Enforcement Agencies (LEAs)

Generally, security events with malicious and criminal intent require response from local Law Enforcement Agencies (LEAs). In case of such events, Regulation 10(1)(a) of PAK/926 requires the licensee to inform local LEAs. The licensee should also lodge First Information Report (FIR) in local Police Station and submit copy of FIR to PNRA.

The FIR generally specifies the following details:

i. Date, time and place of occurrence of event;

ii. Name and address of the licensee (complainant);

iii. Name and address of suspected persons involved in the event (accused); and

iv. Brief about causes and circumstances of the event.

However, the licensee should also provide the specific information related to

the radioactive sources or devices for inclusion in FIR, such as:

(a) Description of the radioactive source involved (name, identification number, activity when imported, type of equipment/device, purpose); and

(b) PNRA license (authorization) number.

6.2. Notification and Reporting to PNRA

Regulation 10(1)(b) of PAK/926 requires the licensee to notify PNRA within twenty-four (24) hours after a security event is detected. The licensee should establish a continuous communication channel with PNRA, after initial notification, for required assistance.

The licensee should make the required notifications to NRECC through available means (such as cell phone/telephone, fax service, email). The licensee should notify NRECC as per Notification Form attached at Annexure-II. The contact details of NRECC are given in the Notification Form. The licensee should ensure confidentiality and protection of information while making security event notifications. Such information should not be disclosed to unauthorized individuals and only authorized and official communication channels should be used.

The licensee should update PNRA about substantive changes, additions or modifications to the initial notification in a timely manner in accordance with the prevailing situation.

In case of confusion, misinterpretation, speculations or false result, the licensee may withdraw the initial notification of security event upon providing justification and conclusive results of investigation to PNRA.

Regulations 10(1)(c) and 10(1)(d) of PAK/926 require the licensee to submit a preliminary report within seventy-two (72) hours and a detailed report within sixty (60) days to PNRA, once security event has occurred. Such events include the following:

i. Actual or attempted theft, unauthorized removal or loss of control over radioactive sources;

ii. Actual or attempted sabotage;

iii. Unauthorized transfer or transport of radioactive sources;

iv. Unauthorized access to secured area or source location;

v. Any adverse condition during transportation that restrict movement of the vehicle carrying radioactive sources (e.g. forceful stopover of vehicle, accident conditions, intentional misrouting, civil disturbance, etc.); and

vi. Any situation that may lead to occurrence of the above events.

These reports should contain sufficient details and information to describe what occurred during the event, vulnerabilities identified and corrective actions to prevent recurrence were taken by the licensee. Relevant documents, data and photographs, where possible should be attached with these reports. The licensee should ensure confidentiality of sensitive information while processing these reports.

The "Preliminary report" should contain at least the following contents:

(a) Brief description of radiation facility or location where the event occurred;

(b) Brief description of the event and its causes;

(c) Immediate actions taken in response to the event and compensatory measures taken or planned including dates of completion;

(d) Brief summary of ongoing investigations, assessment or evaluation; and

(e) Current situation of the event including way forward.

The "Detailed report" should contain at least the following contents:

(a) Description of radiation facility or location where the event occurred;

(b) Detailed description of the event including means of detection;

(c) Description of actions taken in response to the event and compensatory measures taken or planned including dates of completion;

(d) Causes of the security event (including security system failures that contributed to the event);

(e) Security event circumstances and consequences;

(f) Description of investigations, assessment or evaluation;

(g) Corrective actions taken or planned including dates of completion to address the causes; and

(h) Significance for safety and any lessons learned.

If significant additional information is identified or received after submission of detailed report, the licensee should share such information with PNRA.

6.3. Security Event Logs and Records

The licensee should maintain a log to record all types of security events. Maintaining record of events in a log may identify system vulnerabilities, or actions to be taken by licensee for improvement.

7. RESPONSE AND REMEDIAL ACTIONS

Regulations 11(3), 12(3), 13(3) & 16(1) of PAK/926 require licensee to take response actions in case when security event is detected for radioactive sources of different categories. Similarly, as per Regulation 17 of PAK/926, the licensee should take appropriate measures against increased security threat. The licensee should describe the mechanism and process to return the radioactive source to its secured storage location if it is in use.

Regulation 10(1)(a) of PAK/926 also requires licensee to take immediate remedial actions whenever a security event occurs.

As soon as the security event is occurred, the licensee should take the required actions that include but not limited to:

i. Initiate response measures appropriate to the security event and assess the validity and potential consequences of security event;

ii. Establish coordination and communication with response organizations, where needed (such as Police, SPD, PNRA, NDMA, Fire Brigade, Rescue 1122, Civil Defense, etc.);

iii. Establish and maintain interface with emergency plan; and

iv. Locate, identify, recover and secure radioactive source involved in the event.

The goals for the response to security events are to:

(a) Save life of public and affected workers;

(b) Render first aid and ensure the health and safety of responders;

(c) Prevent, deter and detect criminal or intentional unauthorized acts;

(d) Establish coordination and cooperation with response organizations;

(e) Protect, to the extent practicable, property and the environment;

(f) Regain control over the situation and mitigate the consequences; and

(g) Facilitate legal proceedings.

7.1. Initiation of Response

The response to security events starts with the initial assessment of an alarm from security system or information alert at the security control room or Central Alarm Station (CAS) of the facility. An alarm or alert should be assessed to determine whether or not a security event has occurred. If the initial assessment is inconclusive, then a detailed assessment should be carried out to arrive at a definite conclusion. Alarm assessment requires human observation and judgment, through deployment of response personnel to investigate the cause of the alarm or through use of remote video

systems. In general, the licensee should be able to provide necessary information for assessment.

If the outcome of the assessment process is confirmation of a security event, the licensee should declare the occurrence of the security event and activate appropriate response as per approved Physical Protection Plan. An example of steps for response to a security event is given at Annexure-III and an example of an administrative worksheet to gather initial information on scene of security event is given at Annexure-IV.

7.2. Coordination and Communication

The response to security event normally involves different response organizations for which effective and efficient coordination and communication is essential. Regulation 7(4) of PAK/926 requires licensee to cooperate and coordinate with relevant organizations having their role in response to contingencies related to security of radioactive sources. The licensee should coordinate, to the extent practicable, with response organizations including law enforcement agencies for responding to security events. The licensee should develop a procedure to address identification of coordination activities, communication arrangements, resources and related documentation.

The security event may likely lead to a radiological emergency that requires effective coordination and communication to manage interface between security response and emergency response. In such situation, interface of response measures for security event and the radiological emergency to be taken during preparedness, response and post event evaluation may be identified.

The licensee should use the identified primary and secondary reliable communication means during response to security event preferably landline numbers. Regular meetings with response organizations should be conducted during response to security event. List of response personnel should be updated and made available at all times.

7.3. Recovery and Secure Management

If a radioactive source is lost, stolen or misplaced, it can pose significant hazard to the public. Information on the type of source, its activity and other physical and chemical characteristics will be essential in assessing its potential hazard for the public. The licensee should initiate the efforts to track the source from the last known location and the person who handled the source through physical and administrative searches.

Investigative work should be conducted to retrace the sequence of events in order to collect the information regarding the persons who may have handled

the radioactive source intentionally or unintentionally. Other possible sources of information may include reports from the medical community on possible contaminated or overexposed victims and investigation by law enforcement agencies.

The licensee should develop a procedure to address arrangements for physical searches for missing sources and related coordination with the law enforcement agencies. The search team should include personnel trained in identification and handling of radioactive sources and packages. Following information should be considered while performing physical searches:

i. At all times, be mindful of safety and security precautions. Do not ignore 'situational awareness' while performing searches;
ii. Suspicious persons and packages should be safely handled and examined by non-intrusive means whenever possible;
iii. Look for objects bearing the radiation symbol. Do not attempt to open suspicious packages with labels indicating radioactive sources;
iv. Properly use hand-held search equipment over the surface of person(s), package, and vehicle to assess;
v. Look for the information about the name of the source owner or manufacturer;
vi. Look for lead or other heavy shielding containers;
vii. Survey sanitary disposal sites and recycling facilities;
viii. Ensure the security of other sources.

After source recovery, the licensee should establish its control and bring it back into the premises. In addition, the licensee should ensure that all persons who may have been exposed are identified and assessed.

8. TERMINATION OF SECURITY EVENT RESPONSE

The licensee should develop a procedure for establishing process and criteria for termination of a security event including information to PNRA and other relevant organizations. All relevant records/data generated during the event should be gathered and secured before the termination of event.

Once the event is terminated, all operating and security personnel involved in search, recovery, decontamination of area, monitoring of personnel and environment etc. should pass through health surveillance and their personal dosimeters should be immediately sent for dose assessment.

9. EVENT ANALYSIS

Documentation and records are very important for analysis of an event. The analysis provides insight to the sequence of occurrence of events, effectiveness of

security systems and response measures etc. Arrangements should be made to acquire the expertise necessary to conduct analysis of an event.

The analysis of an event should give due consideration to the following:

i. The root causes of an event;
ii. Verification of adherence of administrative and technical procedures;
iii. Recorded interviews/investigations;
iv. Records of inventory of radioactive sources, area survey, work orders, source movement, access control, etc.;
v. Identification of any violation of regulatory requirements;
vi. Identification of any vulnerability of security system; and
vii. Identification of improvements in decision making, trainings, equipment and procedures.

The licensee should carry out event analysis as soon as possible and take actions promptly on the basis of an analysis to avoid recurrence of such events. The licensee should use outcome of event analysis in the development of preliminary and detailed reports.

10. PROVISIONS TO MAINTAIN AND ENHANCE ARRANGEMENTS FOR MANAGING NUCLEAR SECURITY EVENTS

The licensee should take measures to maintain and enhance arrangements for preparedness and response to security events. The arrangements are to maintain, review and update plans and procedures, to establish mechanism to incorporate lessons learned from experience feedback and make the availability of human, technical and financial resources.

Arrangements should be made to ensure that security systems and measures are continuously available and functional for the detection and response to security event.

The licensee should consider the following for maintenance and enhancement of preparedness and response to security events:

i. Strong leadership and management support;
ii. Establish strong safety and security cultures;
iii. Periodic exercises and evaluation of capabilities;
iv. Establish reliable Points of Contact with relevant organizations; and
v. Addressing issues and resolving conflicts.

The licensee should also perform self-assessment and audit at regular intervals and the identified gaps should be included in the corrective action plan.

11. RECORD KEEPING

The licensee should make arrangements to protect and maintain, to the extent practicable data and information generated in case of security event for pre-defined time period. The licensee should protect record as per pre-defined classification (e.g. secret, confidential and restricted). The record associated with security events should be made available to PNRA during inspections. The licensee should have safe and secure record keeping arrangements related to management of security events.

12. REFERENCES

[1]. Regulations on Security of Radioactive Sources - (PAK/926), Pakistan Nuclear Regulatory Authority, Islamabad (2018).

[2]. Regulations on Management of a Nuclear or Radiological Emergency - (PAK/914) (Rev.1), Pakistan Nuclear Regulatory Authority, Islamabad (2022).

[3]. Regulations on Radiation Protection - (PAK/904) (Rev.1), Pakistan Nuclear Regulatory Authority, Islamabad (2020).

[4]. Security of Radioactive Material in Use and Storage and of Associated Facilities, IAEA Nuclear Security Series No. 11-G (Rev.1), International Atomic Energy Agency, Vienna (2019).

[5]. Security of Radioactive Material in Transport, IAEA Nuclear Security Series No. 9-G (Rev.1), International Atomic Energy Agency, Vienna (2020).

[6]. Developing a National Framework for Managing the Response to Nuclear Security Events, IAEA Nuclear Security Series No. 37-G, International Atomic Energy Agency, Vienna (2019).

[7]. Security of Nuclear Information - IAEA Nuclear Security Series No. 23-G, International Atomic Energy Agency, Vienna (2015).

13. GLOSSARY

i. "Delay" means a function of security system, occurring between detection and response, designed to increase adversary's penetration time towards the radioactive source locations.

ii. "Detection" means a function of security system that begins with sensing a potentially malicious or otherwise unauthorized act and that is completed with the assessment of the cause of the alarm.

iii. "Deter" means a function of security system, to dissuade adversary from undertaking the attempt or malicious act.

iv. "Licensee" means the holder of a valid license issued by the Authority.

v. "Operating Personnel" means individual workers engaged in the operation of a licensed radiation facility.

vi. "Physical Protection Plan" means a document prepared by the licensee and required to be reviewed by the Authority that presents a detailed description of the security arrangements in place at a facility.

vii. "Radiation Facility" means any premises where radiation source (radioactive material or radiation generator) is acquired, produced, manufactured, processed, reprocessed, repaired, used, handled, extracted, imported, exported, stored, installed, operated, maintained and converted.

viii. "Radioactive Source" (also called as sealed radioactive source) means radioactive material that is permanently sealed in a capsule or closely bonded, in a solid form.

ix. "Remedial action" means the removal of a source or the reduction of its magnitude (in terms of activity or amount) for the purposes of preventing or reducing exposures that might otherwise occur in an emergency or in an existing exposure situation.

x. "Response" in nuclear security refers to measures that include activities for the identification, collection, packaging and transport of evidence contaminated with radionuclides, nuclear forensics and related actions in the context of investigation into the circumstances surrounding a nuclear security event.

xi. "Response Organization" means an organization designated or otherwise recognized as being responsible for managing or implementing any aspect of response to security event.

xii. "Response Personnel" means persons, on-site or off-site, who are appropriately equipped and trained to counter an attempted unauthorized removal of radioactive sources or an act of sabotage.

xiii. "Sabotage" means a deliberate act directed against a radioactive source in use, storage or transport that could directly or indirectly endanger

the health and safety of personnel, the public or the environment by exposure to radiation or release of radioactive material.

xiv. "Secured Area" means designated area containing radioactive source to which access is limited to authorized personnel only and controlled for security purposes.

xv. "Security Culture" means the assembly of characteristics, attitudes and behaviors of individuals, organization and institutions that serve as a means to support and enhance the security.

xvi. "Security Event" means an event that has potential or actual implications for security that must be addressed.

xvii. "Security Personnel" means authorized and security cleared persons who are responsible for security related to patrolling, monitoring, assessing or escorting any individuals or transport or controlling access and providing initial response.

xviii. "Security System" means an integrated set of security measures.

xix. "Sensitive Information" means information, in whatever form, including software, the unauthorized disclosure, modification, alteration, destruction, or denial of use of which could compromise security.

xx. "Source Location" means a position of radioactive source inside the secured area.

xxi. "Storage" means the holding of radioactive sources in a facility that provides for their containment with the intention of retrieval.

xxii. "Transport" means carriage of radioactive sources by any means of transportation, beginning with the departure from a facility of the shipper and ending with the arrival at a facility of the receiver.

xxiii. "Unauthorized Removal" means theft or other unlawful taking of radioactive sources.

ANNEXURE-I

GUIDELINES FOR DEVELOPING EXERCISE SCENARIOS

Drills and exercises are conducted to assess and validate the security systems and measures in order to deter, detect and timely respond to the security event involving radioactive sources. For the conduct of exercise, a scenario may be developed based on the reasonably foreseeable information. The exercise information may include briefings, exercise injects, messages, maps etc.

Participants for the execution of exercise scenarios may take the roles of players, controllers or evaluators (as necessary). Guidelines for developing exercise scenarios are given below:

1. Defining the Exercise Scenario

The licensee should define a broad scenario that outlines the various objectives of the exercise. Depending on the exercise scope, the scenario may be divided into several phases, each focused on a particular aspect of prevention, detection and response to a security event. The scenario may include the security events described under Section 4 of this RG and have following description:

i. Define the roles and responsibilities of the operating, security and response personnel, associated law enforcement and support agencies to deter and prevent the adversary act;

ii. Replicate the malicious act i.e. theft, sabotage, loss or misplace and unauthorized removal of radioactive sources;

iii. Visualize the detection of security event involving radioactive sources;

iv. Test and evaluate the sequences of actions to be taken.

2. Components of Exercise Scenario

a) Exercise Narrative

The exercise narrative of the scenario is a brief overview to describe the security event. It is a description that contains all the information to drive the exercise. The narrative of the scenario is provided mainly for the exercise personnel and organizers to understand the scenario. The exercise planning team should ensure that the scenario should be realistic and developed in such a way to avoid any sensitivity that may arise due to the use of real names or sensitive venues. The exercise narrative should include three basic elements:

i. General context and comprehensive description including type of event (e.g. unauthorized access, unauthorized removal, theft or loss of radioactive sources, illicit trafficking, hostile action etc.);

ii. Sequence of actions that allow players to demonstrate proficiency and competency in order to meet the exercise objectives;

iii. Technical details necessary to depict scenarios accurately by all exercise personnel.

b) Key Security Events and Adversary Timeline

The adversary timeline is the time that adversary takes to accomplish its tasks. The occurrence of the events allows the players to take appropriate actions. The exercise planning team should describe the timeline of adversary attack and subsequent actions taken by exercise players, for example:

i. Attempted theft of radioactive sources during use, storage or transport;

ii. Illicit trafficking or unauthorized shipment involving radioactive sources/materials. This may lead to detection, interdiction and subsequent management of such trafficking or unauthorized movement;

iii. Sabotage of radiation facility or radioactive source during transportation.

These scenarios may lead to define exercise objectives to prevent theft, unauthorized movement or sabotage and strengthen the coordination of licensee with other organization to prevent the use of radioactive sources for malicious purposes.

c) Detailed Sequence of Events

The detailed sequence of events may be described by using various event logs like player event log (e.g. adversary, operator, response personnel etc.) and controller event log for successful planning and implementing the drills.

ANNEXURE-II

SECURITY EVENT NOTIFICATION FORM

Event Date:	Event Time:
Facility Type: ☐ Irradiators ☐ Teletherapy ☐ Brachytherapy ☐ Industrial Radiography ☐ Industrial Gauges ☐ Oil Well Logging ☐ Calibration Sources ☐ Other_____ (Please specify)	**Nature of Event:** ☐ Source lost or stolen ☐ Attempted or actual sabotage ☐ Unauthorized transfer or transport ☐ Unauthorized access to secured area ☐ Failure of essential security systems ☐ Loss of sensitive information ☐ Other_____ (Please specify)
Name and location of facility/site where incident occurred: _____ _____ _____	
City: _____	Contact No. _____
Incident Summary: (Brief description of event) (Use another sheet, if required)	
Sender details: Name: _____ Designation: _____Contact No. _____ Reporting Time: _____ Signature with Date: _____	

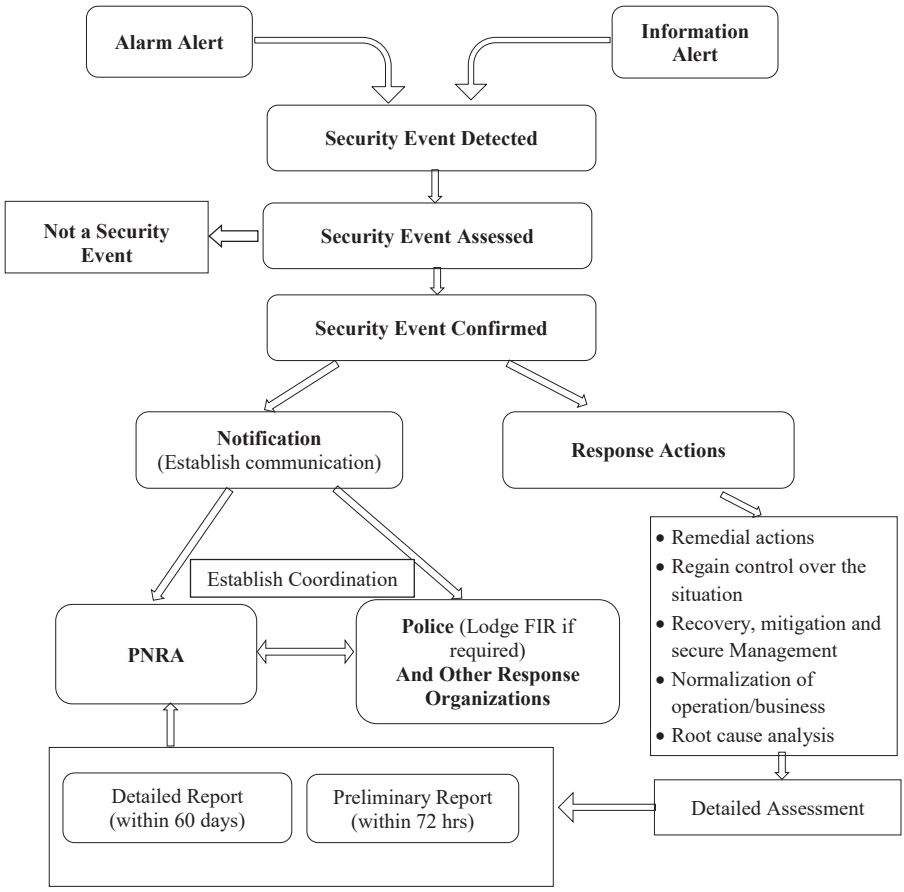
Please send filled form to:

National Radiation Emergency Coordination Center (NRECC)
PNRA HQs, Mauve Area, G-8/1, Islamabad.

Telephone	Fax	Email
Primary: 051-9262019 Backup: 051-2289210 Toll Free: 0800-77766 Officer In-charge: 0300-8540319 Alternate Officer In-charge: 0334-5131978	Primary: 051-9260201 Backup: 051-2289233	nrecc@pnra.org

ANNEXURE-III

EXAMPLE OF SEQUENCE FOR RESPONSE TO A SECURITY EVENT



ANNEXURE-IV

ADMINISTRATIVE WORKSHEET FOR GATHERING INITIAL INFORMATION

This Annexure provides sample of an administrative worksheet to be used to record important information regarding security event and observations at the scene/site. The worksheet once used, will help to develop security event report. This worksheet is generic in nature and may be revised as necessary for the situation encountered at the scene.

Operational Data	Notes/Observations
Location of the scene	
Time and date	
Person(s) present at the scene	
Weather condition	
Main cause of security event	
Situation observed at the scene	
Information of suspected culprit involved	
Information of the radioactive source involved	
Description of useful evidences found at the scene	
Description of any hazardous material found at the scene	
Description of any contaminated item found at the scene	
Radiation detector used for survey (Name/Model/Sr. No.)	
Background dose rate	
Assessment and evaluation of radiation hazards	

Signature (Name and designation of facility personnel): _____
Date: _____

PAKISTAN NUCLEAR REGULATORY AUTHORITY
P.O. Box 1912, Islamabad
www.pnra.org