Published in Volume 118, No. 21 of the Official Gazette dated 23 May 2022

Republic of the Philippines
Department of Science and Technology
PHILIPPINE NUCLEAR RESEARCH INSTITUTE
Commonwealth Avenue, Diliman, Quezon City

CPR PART 10

REQUIREMENTS FOR THE PHYSICAL PROTECTION OF NUCLEAR MATERIALS AND NUCLEAR INSTALLATIONS

TABLE OF CONTENTS

Published in Volume 118, No. 21 of the Official Gazette dated 23 May 2022

Republic of the Philippines
Department of Science and Technology
PHILIPPINE NUCLEAR RESEARCH INSTITUTE
Commonwealth Avenue, Diliman, Quezon City

CPR PART 10

REQUIREMENTS FOR THE PHYSICAL PROTECTION OF NUCLEAR MATERIALS AND NUCLEAR INSTALLATIONS

I. GENERAL PROVISIONS

Section 1. *Purpose*

(a) This Part is promulgated pursuant to Republic Act No. 5207, as amended, "An Act Providing for the Licensing and Regulation of Atomic Energy Facilities and Materials, Establishing the Rules on Liability for Nuclear Damage and for Other Purposes", to establish the regulatory requirements for the protection of the health and safety of the workers and the general public.

(b) This Part prescribes requirements for the establishment and maintenance of a physical protection measures and systems against:

(1) Unauthorized removal of nuclear material; and

(2) Sabotage of nuclear material and nuclear installations.

Section 2. *Scope*

(a) The requirements established in this Part are applicable to the physical protection of nuclear installations licensed pursuant to CPR Part 7, including nuclear material stored thereat.

(b) The requirements in this Part are applicable to all aspects of physical protection of nuclear installations and nuclear material in use, storage and during transport.

Section 3. *Definitions*

As used in this Part:

(a) ***"Adversary"*** means an individual, group or organization that conducts or intends to conduct detrimental activities and against which physical protection system is designed. An adversary may be an insider, outsider or collusion of both;

(b) ***"Assessment"*** means the determination by a guard or an electronic system of the cause of the alarm and extent of the threat;

(c) ***"Authorized person"*** means any individual, including an employee, consultant or an agent of the nuclear installation operator who has been designated in writing by the said installation operator to have responsibility for visual surveillance of or control over special fissionable material is used or stored;

(d) ***"Bullet-resisting"*** means protection against complete penetration, passage of fragments of projectiles and spalling of the protective material that could cause injury to a person standing directly behind the bullet-resisting barrier.

(e) ***"Central Alarm Station"*** means an installation which provides for the complete and continuous alarm monitoring, assessment and communication with guards, facility management and response forces;

(f) ***"Configuration Management"*** means the process of identifying and documenting the characteristics of a facility's physical protection system, including computer systems and software, and of ensuring that changes to these characteristics are properly developed, assessed, approved, issued, implemented, verified, recorded and incorporated into the facility documentation;

(g) ***"Contingency Plan"*** means predefined set of actions for responses to unauthorized acts indicative of attempted unauthorized removal or sabotage, including threats thereof, designed to effectively counter such acts;

(h) ***"Conveyance"*** means
a. for transport by road or rail: any vehicle;
b. for transport by water: any vessel, or any hold, compartment, or defined deck area of a vessel; and
c. for transport by air: any aircraft.

(i) ***"Continuous visual surveillance"*** means an obstructed view at all times of a shipment of special fissionable material, and of all access to a temporary storage area or cargo compartment containing the shipment.

(j) ***"Defence-in-depth"*** means the combination of multiple layers of systems and measures that have to be overcome or circumvented before nuclear security is compromised;

(k) ***"Delay"*** means the element of a physical protection system designed to increase adversary penetration time for entry into and exit from the nuclear installation or transport of nuclear material;

(l) ***"Design Basis Threat (DBT)"*** means the attributes and characteristics of potential insider and/or external adversaries, who might attempt unauthorized removal of nuclear material or sabotage, against which a physical protection system is designed and evaluated;

(m) ***"Detection"*** means a process in a physical protection 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;

(n) ***"Force"*** means violent methods used by adversary to attempt to steal special fissionable material or to sabotage a nuclear installation or violent methods used by response personnel to protect against such adversary actions.

(o) ***"Graded Approach"*** means the application of physical protection measures proportional to the potential consequences of a malicious act;

(p) ***"Guard"*** means a uniformed individual armed with a firearm whose primary duty is the protection of special fissionable material against theft, the protection of a nuclear installation against radiological sabotage, or both;

(q) ***"Inner area"*** means an area with additional protection measures inside a protected area, where Category I nuclear material is used and/or stored;

(r) ***"Insider"*** means one or more individuals with authorized access to nuclear facilities or nuclear material in transport who could attempt unauthorized removal or sabotage, or who could aid an external adversary to do so;

(s) ***"Isolation zone"*** means any area adjacent to a physical barrier, clear of all objects which could conceal or shield an individual;

(t) ***"Intrusion alarm"*** means a tamper indicating electrical, electromechanical, electro-optical, electronic or similar device which will detect intrusion by an individual into a building, protected area, vital area, or material access area, and alert guards or watchmen by means of actuated visible and audible signals;

(u) ***"Malicious act"*** means an act or attempt of unauthorized removal or sabotage;

(v) ***"Material access area"*** means any location which contains special fissionable material, within a vault or a building, the roof, walls, and floor of which each constitute a physical barrier;

(w) **"*Need to know"*** means a rule by which individuals, processes and systems are granted access to only the information, capabilities and assets that are necessary for execution of their authorized functions;

(x) ***"Performance testing"*** means testing of the physical protection measures and the physical protection system to determine whether or not they are: implemented as designed; adequate for the proposed natural, industrial and threat environments; and in compliance with established performance requirements;

(y) ***"Protected area"*** means an area encompassed by physical barriers and to which access is controlled;

(z) ***"Physical barrier"*** means a fence, wall or similar impediment which provides access delay and complements access control;

(aa) ***"Sabotage"*** means any deliberated act directed against a nuclear installation or nuclear material in use, storage or transport which could directly or indirectly endanger the health and safety of personnel, the public or the environment by exposure to radiation or release of radioactive substances;

(bb) ***"System for nuclear material accountancy and control"*** means an integrated

set of measures designed to provide information on, control of, and assurance of the presence of nuclear material, including those systems necessary to establish and track nuclear material inventories, control access to and detect loss or diversion of nuclear material, and ensure the integrity of those systems and measures;

(cc) ***"Threat"*** means a person or group of persons with motivation, intention and capability to commit a malicious act;

(dd) **"Threat assessment"** means an evaluation of the threats — based on available intelligence, law enforcement and open source information — that describes the motivations, intentions and capabilities of these threats;

(ee) ***"Transport"*** means an international or domestic carriage of nuclear material by any means of transportation, beginning with the departure from a facility of the shipper and ending with the arrival at a nuclear facility of the receiver.

(ff) ***"Transport control center"*** means a facility which provides for continuous monitoring of a transport conveyance location and security status and for communication with the transport conveyance, shipper/receiver, carrier and, when appropriate, its guards and the response forces.

(gg) ***"Unauthorized removal"*** means theft or other unlawful taking of nuclear material;

(hh) ***"Vault"*** means a windowless enclosure with walls, floor, roof and door(s) designed and constructed to delay penetration from forced entry;

(ii) ***"Vault-type room"*** means a room with one or more doors, all capable of being locked, protected by an intrusion alarm which creates an alarm upon entry of a person anywhere into the room and upon exit from the room or upon movement of an individual within the room;

(jj) ***"Vital area"*** means any area which contains vital equipment;

(kk) ***"Vital equipment"*** means any equipment, system, device, or material, the failure, destruction, or release of which could directly or indirectly endanger the public health and safety by exposure to radiation. Equipment or system which would be required to function to protect public health and safety following such failure, destruction, or release are also considered to be vital;

Section 4. ***Interpretation***

Except as specifically authorized by the PNRI Director in writing, no interpretation of the meaning of the requirements in this Part shall be recognized to be binding upon the PNRI.

Section 5. ***Communication***

All correspondence, reports, applications, and other communications from the applicant or licensee to the PNRI concerning the requirements in this Part or individual license conditions shall be addressed to:

The Office of the Director
Philippine Nuclear Research Institute
Commonwealth Avenue,
Diliman, Quezon City

Section 6. ***Specific Exemptions***

The PNRI may, upon application by the licensee or upon its own initiative, grant such exemptions from the requirements in this Part as it determines are authorized by law and will not result in undue hazard to life, property, and the environment.

II. ADMINISTRATIVE REQUIREMENTS

Section 7. ***General Responsibilities***

(a) The licensee shall be primarily responsible for the physical protection of its nuclear material in use, storage and during transport and for nuclear installation and associated activities in order to reduce the risk of malicious acts involving nuclear materials and its facilities.

(b) The licensee shall cooperate and coordinate with all organizations having physical protection responsibilities.

(c) The licensee shall design, evaluate and maintain a physical protection system requirement for nuclear material in use, storage and during transport and for nuclear material, nuclear installation and associated activities in accordance with the requirements of this Part. In addition, the licensee shall implement any additional physical protection measures as required by the PNRI, from time to time, based on Design Basis Threat or National Threat Assessment.

(d) The licensee shall ensure that the physical protection system shall be integrated and effective against both sabotage and unauthorized removal.

(e) The licensee shall ensure that the capabilities to detect, delay and respond to neutralize threats up to and including the design basis threat are always maintained.

Section 8. ***Security Culture***

The licensee shall be responsible to establish and maintain a dynamic and effective security culture where there is recognition that credible threat exist and every individual has a role in physical protection.

Section 9. ***Graded Approach***

(a) Physical protection measures shall be based on a graded approach, considering the current assessment of the threat, the relative attractiveness, the nature of the material and potential consequences associated with the unauthorized removal of nuclear material and with the sabotage against nuclear material or nuclear installations.

(b) The licensee shall implement the graded approach on the basis of categorization of nuclear material as described in Table 1, Categorization of Nuclear Material to ensure protection against unauthorized removal or sabotage is consistent to the level of threat identified taking into account existing nuclear safety and radiation protection.

Section 10. ***Defence-in-Depth***

(a) The licensee shall reflect the concept of defence-in-depth and methods of physical protection against sabotage and unauthorized removal thru design of hardware, procedures and facility design.

(b) The licensee shall ensure that the physical protection measures for detection, delay and response are based on the principle of defence-in-depth applied with a graded approach.

Section 11. ***Security Plan***

(a) The licensee shall develop a security plan based on the threat assessment or the design basis threat which includes the design, evaluation, implementation, and maintenance of the physical protection system, and contingency plans. The security plan shall be reviewed and approved by PNRI. The structure and suggested content of a security plan is provided in Appendix A.

(b) The licensee shall implement the approved security plan for nuclear material based on its category, prior to arrival of the nuclear material on site.

(c) The licensee shall ensure the implementation of approved security plan through drills and exercises before introducing nuclear material into the systems of the nuclear installation.

(d) The licensee shall review the security plan regularly to ensure it remains up to date with the current operating conditions and the physical protection system.

(e) The licensee shall submit an amendment to the security plan for prior approval by the PNRI before making any significant modifications, including temporary changes, to the arrangements detailed in the approved security plan.

Table 1. Categorization of Nuclear Material

Material	Form	Category		
		Category I	Category II	Category III[1]
1. Plutonium[2]	Unirradiated[3]	2 kg or more	Less than 2 kg but more than 500 g	500 g or less but more than 15 g
2. Uranium-235 (235U)	Unirradiated[b] – Uranium enriched to 20% 235U or more – Uranium enriched to 10% 235U but less than 20% 235U – Uranium enriched above natural, but less than 10% 235U	5 kg or more	Less than 5 kg but more than 1 kg 10 kg or more	1 kg or less but more than 15 g Less than 10kg but more than 1 kg 10 kg or more
3. Uranium-233 (233U)	Unirradiated[b]	2 kg or more	Less than 2 kg but more than 500 g	500 g or less but more than 15 g
4. Irradiated fuel (The categorization of irradiated fuel in the table is based on international transport considerations. The State may assign a different category for domestic use, storage and transport taking all relevant factors into account.)			Depleted or natural uranium, thorium or low enriched fuel (less than 10% fissile content)[4,5]	

[1]Quantities not falling in Category III and natural uranium, depleted uranium and thorium should be protected at least in accordance with prudent management practice.

[2]All plutonium except that with isotopic concentration exceeding 80% in plutonium-238.

[3]Material not irradiated in a reactor or material irradiated in a reactor but with a radiation level equal to or less than 1 Gy/h. (100 rad/h) at 1 m unshielded.

[4]Although this level of protection is recommended, it would be open to States, upon evaluation of the specific circumstances, to assign a different category of physical protection.

[5]Other fuel which by virtue of its original fissile material content is classified as Category I or II before irradiation may be reduced one category level while the radiation level from the fuel exceeds 1 Gy/h (100 rad/h) at one meter unshielded.

Section 12. ***Contingency Plan***

(a) The licensee shall develop contingency plans for the rapid location and recovery of nuclear material which has been declared missing or stolen from nuclear installations. An example of a contingency plan is contained in Appendix B.

(b) Contingency plans to respond to unauthorized removal of nuclear material or sabotage of nuclear material or nuclear installations, or attempts thereof, shall be prepared, and appropriately exercised periodically by the licensees and authorities concerned.

Section 13. ***Safety and Physical Protection Interface***

(a) The licensee shall assess and manage the physical protection interface with safety and nuclear material accountancy and control activities in a manner to ensure that they do not adversely affect each other and that, to the degree possible, they are mutually supportive.

(b) In case of a new nuclear installation, physical protection features shall be incorporated into the facility design in the initial design phase and address interface issues with safety and nuclear material accountancy and control to avoid any conflicts and to ensure that all three elements support each other.

Section 14. ***Review and Evaluation***

(a) The licensee shall review security plan on periodic basis by individuals independent of both security plan management and personnel who have direct responsibility for implementation.

(b) Review of the security plan shall include, but not be limited to, an audit of the effectiveness of the security plan, relevant plans, implementing procedures, safety and physical protection interface activities, the performance testing, maintenance, and calibration program.

(c) The outcome of the security plan review, and any actions taken as a result of prior reviews, shall be documented and reports shall be maintained in an auditable form.

(d) Evaluations, including performance testing of physical protection measures and of the integrated physical protection system, including timely response of the guards and response forces shall be conducted regularly to determine the reliability and effectiveness against the threat.

(e) Performance testing of physical protection system shall include appropriate exercises to determine if the response forces can provide an effective and timely response to prevent malicious act.

Section 15. ***Maintenance, Testing and Sustainability Program***

(a) The licensee shall develop, implement and maintain means and procedures for

maintenance and testing of physical protection systems.

(b) Performance testing shall be carried out in accordance with the physical protection plans and implementing procedures.

(c) The licensee shall establish sustainability programs for its physical protection systems. The sustainability programs shall encompass:

(1) Operating procedures and instructions;

(2) Human resource management and training;

(3) Equipment updating, maintenance, repair and calibration;

(4) Performance testing and operational monitoring;

(5) Configuration management; and

(6) Resource allocation and operational cost analysis.

(d) Maintenance of physical protection equipment shall be performed according to approved procedures, vendor's recommendations, experience feedback, and system performance to ensure that design requirements are not compromised.

(e) In all cases of modifications and replacement of physical protection equipment, it shall be ensured that the intended function of the system is not compromised.

Section 16. ***Compensatory Measures***

(a) The licensee shall identify and immediately implement measures to compensate for degraded or inoperable equipment, systems and components, and in case the physical protection equipment is taken out of service.

(b) Compensatory measures shall provide a level of protection that is equivalent to the protection that was provided by the equipment, system or components before degradation or inoperability.

(c) Compensatory measures shall be implemented as identified in physical protection program. However, any design change in physical protection system that affects system performance shall require approval from the PNRI before implementation.

Section 17. ***Protection of Sensitive Information***

The licensee shall identify and classify sensitive information which can add to adversary's capability to perform sabotage or unauthorized removal of nuclear material and protect such information against unauthorized disclosure.

Section 18. ***Insider Mitigation***

The licensee shall establish, maintain and implement insider mitigation measures to monitor the initial and continual trustworthiness and reliability of individuals granted

or retaining unescorted access authorization to a protected or vital area or sensitive information and implement defence-in-depth methodologies to minimize the potential for an insider to adversely affect, either directly or indirectly, the licensee's capability to prevent sabotage and unauthorized removal of nuclear material.

Section 19. ***Protection of Computers, Communication Systems and Networks***

The licensee shall protect the computers, communication systems and networks associated with functions important-to-safety and physical protection from cyber attacks that would:

(a) Adversely impact the integrity or confidentiality of data and software;

(b) Cause unauthorized access to systems, services, and data;

(c) Adversely impact the operation of systems, networks and associated equipment; and

(d) Contribute to physical damage of equipment or aid in the unauthorized removal of nuclear material.

III. REQUIREMENTS FOR MEASURES AGAINST UNAUTHORIZED REMOVAL OF NUCLEAR MATERIAL IN USE AND STORAGE

Section 20. ***Category III Nuclear Material***

(a) The licensee shall use or store Category III nuclear material within limited access area.

(b) Provision shall be made for detecting unauthorized intrusion into the limited access area.

(c) Provision shall be made for appropriate actions by guards or response forces, in case of unauthorized intrusion into the limited access area.

(d) Procedures for transferring custody of nuclear material shall be established.

(e) Technical means and procedures for access control shall be established and protected against compromise such as manipulation and falsification.

(f) Contingency plans shall be prepared to counter malicious acts effectively and to provide for appropriate response by guards or response forces.

Section 21. ***Category II Nuclear Material***

(a) The licensee shall use or store Category II nuclear material within a protected area located inside a limited access area.

(b) The licensee shall meet the requirements of Section 20 of this Part along with following additional requirements:

(1) The protected area perimeter shall consist of a physical barrier and an isolation zone.

(2) The isolation zone shall be:

(i) Designated and of sufficient size to permit detection and assessment of activities on either side of protected area barrier;

(ii) Monitored with intrusion detection equipment capable of detecting both attempted and actual penetration of protected area perimeter barrier; and

(iii) Monitored with assessment equipment capable to provide real-time and play-back/recorded video images of detected activities before and after each alarm annunciation.

(3) The intrusion detection and assessment systems shall:

(i) Ensure that alarm devices to include transmission lines to annunciators are tamper indicating and self-checking; and

(ii) Ensure intrusion detection and assessment equipment at the protected area perimeter remains operable from an uninterruptible power supply in the event of the loss of normal power.

(c) The licensee shall provide isolation zones and appropriate exterior areas within the protected area with illumination level sufficient to perform proper assessment of alarms.

(d) The licensee shall identify and analyze site-specific conditions to determine the specific use, type, function, and placement of physical barriers as necessary to control access into installation areas. The barriers shall be designed and constructed to provide deterrence, delay, or support access control, support effective implementation of the licensee’s protective strategy.

(e) The number of access points into the protected area shall be kept to the minimum necessary. All points of potential access shall be appropriately secured and alarmed.

(f) The licensee shall take following measures for authorized access to protected area:

(1) Establish effective access control measures under which only authorized persons have access to the protected area. The number of authorized persons entering the protected area shall be kept to the minimum necessary. Persons authorized for unescorted access to the protected area shall be limited to persons whose trustworthiness has been determined. Persons whose trustworthiness has not been determined such as temporary repair, service or construction workers and visitors shall be escorted by authorized personnel.

(2) Identity and verify authorized persons entering the protected area.

(3) Keep record of all persons having access to or possession of keys, key cards and other systems, including computer systems that control access to protected area.

(4) Establish procedures and technical means for access control, including keys and computerized access lists against manipulation, falsification, or other form of compromise.

(g) The licensee shall search all personnel, vehicles, packages and materials entering and leaving the protected areas for contraband or other prohibited items which could be used to commit sabotage or removal of nuclear material.

(h) The licensee shall ensure that all emergency exits in the protected area are secured by locking devices and with alarm systems while allowing prompt egress during emergency.

(i) Central Alarm Station:

(1) The licensee shall establish a permanently and adequately staffed central alarm station for monitoring and assessment of alarms, initiation of response, and communication with the guards, response forces, and facility management. Information acquired at the central alarm station shall be stored in a secure manner. The central alarm station shall be protected so that its functions can continue in the presence of threat, e.g. hardened. Access to the central alarm station shall be strictly minimized and controlled.

(2) Alarm equipment, alarm communication paths, and the central alarm station shall be provided with an uninterruptible power supply and be tamper-protected against unauthorized monitoring, manipulation and falsification.

(3) Dedicated, redundant, secure and diverse transmission systems for two-way voice communication between the central alarm station and the response forces shall be provided for activities involving detection, assessment and response. Dedicated two-way secure voice communication shall be provided between guards and the central alarm station.

(4) The licensee shall establish secondary alarm station to ensure that the functions of central alarm station in monitoring and assessment of alarms, initiation of response and communication shall continue during emergency.

(j) Guards and Response Forces:

(1) The licensee shall establish and maintain, at all times, properly trained and equipped guards and response force to interdict and neutralize threats.

(2) The licensee shall ensure that firearms, ammunition, and equipment necessary to implement the security plan are in sufficient supply, in working condition, and readily available for use.

(3) Sufficient number of response force personnel shall remain available at all times inside the protected area.

(k) On-Site Movements of Nuclear Material between Protected Areas:

The licensee shall establish measures under which on-site movements of nuclear material between two protected areas are treated in compliance with the requirements for nuclear material during transport, taking into account existing physical protection measures at the installation.

Section 22. ***Category I Nuclear Material***

(a) The licensee shall use or store Category I nuclear material within an inner area located within a protected area.

(b) The licensee shall meet the requirements of Section 21 of this Part along with following additional requirements:

(1) Inner areas shall be appropriately secured and alarmed when unattended.

(2) Inner areas shall provide delay against unauthorized access to allow for a timely and appropriate response to a malicious act. Delay measures shall be designed considering both insider's and external adversary's capabilities and be balanced for all potential points of intrusion.

(3) Vehicle barriers shall be installed at an appropriate distance from the inner area to prevent the penetration of unauthorized land or waterborne vehicles that could be used by an adversary for committing a malicious act. Attention shall also be given to providing protection measures against any airborne threat.

(4) Authorized Access to Inner Areas:

The licensee shall allow only authorized persons to have access to an inner area. Effective access control measures shall be taken to ensure the detection and prevention of unauthorized access. The number of authorized persons entering an inner area shall be kept to the minimum necessary. Persons with authorized access to an inner area shall be limited to those whose trustworthiness has been determined. In exceptional circumstances and for a limited period, persons whose trustworthiness has not been determined shall be provided access only when escorted by persons authorized unescorted access.

(5) Detection and Prevention of Unauthorized Access:

The licensee shall establish measures under which vehicles, persons and packages are subject to search on entering and leaving inner areas to detect and prevent unauthorized access and the introduction of prohibited items. Vehicles, persons, and packages leaving the inner area shall be subject to search to detect and prevent removal of nuclear material. Access of private vehicles shall be prohibited to inner areas.

(6) Continuous Visual Surveillance of Activity in Inner Area:

To counter the insider threat, the licensee shall ensure detection of unauthorized action by continuous visual surveillance, through the two-person rule or other equivalent means, whenever an inner area is occupied.

(7) Storage Area:

The licensee shall store nuclear material in a hardened or strong room or hardened enclosure inside the inner area that provides an additional layer of detection and delay against removing the material. This storage area shall be locked, and alarms activated except during authorized access to the material. When nuclear material is kept in an unoccupied work area outside this storage area, equivalent compensatory physical protection measures shall be established.

(8) The number of access points into the inner area shall be kept to the minimum necessary. All points of potential access shall be appropriately secured and alarmed.

Section 23. ***Measures to Locate and Recover Missing or Stolen Nuclear Material***

(a) The licensee shall ensure that any missing or unauthorizedly removed nuclear material is detected in a timely manner and the responsible person for physical protection is informed.

(b) The licensee shall confirm any missing or stolen nuclear material by means of a rapid emergency inventory as soon as possible. A system for nuclear material accountancy and control should provide accurate information about the potentially missing nuclear material in the facility following a nuclear security event.

(c) The measures to locate and recover missing or stolen nuclear material shall be included in the contingency plan and shall be tested and evaluated regularly.

(d) The licensee shall take all appropriate measures to locate, as soon as possible, any declared missing or stolen nuclear material on-site and possibly off-site in accordance with the national law and the contingency plan.

(e) The licensee shall secure the nuclear material in situ as soon as the missing or unauthorizedly removed nuclear material has been located and identified in accordance with the contingency plan.

(f) The licensee shall assist/coordinate with the response organizations to locate and recover the missing or unauthorizedly removed nuclear material.

Section 24. ***Prudent Management Practices***

For nuclear material below Category III, prudent management practices for physical protection shall include the following:

(1) Access to the nuclear material shall be restricted to authorized persons only;

(2) When not under the operating control of authorized persons, the nuclear material shall be physically secured; and

(3) Measures to detect unauthorized removal shall be implemented.

IV. REQUIREMENTS FOR MEASURES AGAINST SABOTAGE OF NUCLEAR INSTALLATIONS AND NUCLEAR MATERIAL IN USE AND STORAGE

Section 25. *Process for Design of Physical Protection Systems against Sabotage*

(a) The licensee shall define and submit to the PNRI, credible scenarios by which adversaries could carry out sabotage of nuclear material or nuclear installation.

(b) The licensee shall identify equipment, structure, system or components, and nuclear material, the sabotage of which could directly or indirectly lead to events with high radiological consequences.

(c) The licensee shall design a physical protection system that is effective against the defined sabotage scenarios and complies with the required level of protection for its nuclear installation and nuclear material.

(d) The physical protection system against sabotage shall be designed as an element of an integrated system to prevent the potential consequences of sabotage by taking into account the robustness of the engineered safety and operational features, and the fire protection, radiation protection and emergency preparedness measures.

(e) The physical protection system shall be designed to deny unauthorized access of persons or equipment to the targets, to minimize the opportunity of insiders, and to protect the targets against possible stand-off attacks consistent with design basis threat. The response strategy shall be based on denial of adversary access to the sabotage targets or denial of adversary task completion at the sabotage targets.

Section 26. *Measures for Protection against Sabotage for High Consequence Nuclear Installations including Nuclear Power Plants (NPPs)*

(a) All equipment, systems or devices, or nuclear material, the sabotage of which could directly or indirectly lead to high radiological consequences shall be located inside one or more vital areas.

(b) The licensee shall meet the requirements of Section 22 of this Part along with following additional requirements:

(1) Timely detection of tampering or interference with vital area equipment, systems or devices shall be provided.

(2) During a shutdown and maintenance period, strict access control to vital areas shall be maintained. Searches and testing shall be conducted to detect

any tampering that may have been committed during shutdown and maintenance.

(3) The reactor control room, the central alarm station, and the location within which the last access control function for access to the protected area is performed, shall be bullet-resisting.

Section 27. ***Measures for Protection against Sabotage for other Nuclear Installations and Nuclear Material***

For nuclear material and installations other than NPPs and RRs sabotage of which can result in radiological consequences to the public shall also be protected depending on the degree of consequences. Measures specified in Section 26 of this Part shall be applied by using graded approach.

Section 28. ***Measures to Mitigate or Minimize the Radiological Consequences of Sabotage***

(a) The licensee shall assess, on detection of a malicious act, whether this act could lead to radiological consequences and notify the PNRI;

(b) Immediately following an act of sabotage, the licensee shall take measures specified in the contingency plan to prevent further damage, secure the nuclear installation and protect emergency equipment and personnel.

V. REQUIREMENTS FOR MEASURES AGAINST UNAUTHORIZED REMOVAL AND SABOTAGE OF NUCLEAR MATERIAL DURING TRANSPORT

Section 29. ***General Requirements.***

(a) Aggregation: The licensee shall use the total amount of nuclear material on or in a single conveyance to determine an aggregate categorization for both unauthorized removal and potential radiological consequences associated with sabotage and identify the appropriate protection measures for the conveyance. Appendix C provides a description of nuclear material aggregation.

(b) Common Requirements: The licensee shall implement the following measures in accordance with the graded approach:

(1) Minimize the number of transfers and duration of transport of nuclear material;

(1) When the conveyance makes a planned stop, protect nuclear material in designated storage facility incidental to transport in a manner consistent with the protection required for the applicable category of that nuclear material;

(2) If the conveyance makes an unplanned extended stop, apply the physical protection measures appropriate for that category of material in storage to the fullest extent possible;

(3) Avoid the use of predictable movement schedules by varying times and routes;

(4) Predetermine the trustworthiness of individuals involved during transport of nuclear material;

(5) Limit advance knowledge of transport information to the minimum number of persons necessary;

(6) Use a material transport system with passive and/or active physical protection measures appropriate for the threat assessment or design basis threat; and

(7) Use routes which avoid areas of natural disaster, civil disorder or known threat.

(c) Information Protection:

The licensee shall protect sensitive information relating to transport operations, including detailed information on the schedule and route, and shall disseminate such information based on the need to know. The licensee shall not use unnecessary markings on conveyances and shall avoid the use of open channels for transmission of messages concerning shipments of nuclear material. When a security related message is transmitted, such information shall be protected in accordance with applicable information protection requirements.

(d) Key Control:

The licensee shall ensure the security of keys for conveyance and security locks.

Section 30. ***Protection of Category III Nuclear Material against Unauthorized Removal.***

In addition to the general requirements given in Section 29 of this Part, the following requirements also apply to Category III nuclear material:

(a) Arrangements Prior to Shipment:

The licensee shall ensure that prior agreements among, receiver, and carrier specify the time, place and procedures for transferring physical protection responsibilities; and adequate physical protection arrangements are in place.

(b) Locks and Seals:

Packages containing nuclear material shall be carried in a closed, locked and sealed conveyance, compartment or freight container.

(c) Search Prior to Shipment:

There should be a detailed search of conveyance to ensure that nothing has been tempered with and that nothing has been affixed to the package or conveyance that might compromise the security of the consignment.

(d) Communications:

The licensee shall ensure the availability of a communication system for the conveyance to communicate with response forces.

(e) Checks upon Receipt:

The licensee shall ensure that the receiver checks the integrity of the packages and locks and seals to verify that the security of the consignment has not been compromised and accepts the shipment and notifies in writing immediately upon arrival.

Section 31. ***Protection of Category II Nuclear Material against Unauthorized Removal.***

In addition to the general requirements prescribed in Section 29 and specific requirements in Section 30 of this Part, the following requirements also apply to Category II nuclear material:

(a) Arrangements Prior to Shipment:

(1) Prior to shipment, the licensee shall submit a transport security plan to the PNRI for approval. This plan shall include the route, with alternative routing in case of any emergency, stopping places, destination hand-over arrangements, identification of persons authorized to receive delivery, emergency procedures and reporting procedures. In choosing the route, the capabilities of the response forces shall be taken into account.

(2) Prior to commencing transport, the licensee shall ensure that all measures necessary to implement the approved transport security plan are in place.

(b) Search Prior to Shipment and Surveillance:

The conveyance shall be searched immediately prior to loading and shipment. Immediately following completion of the search, the conveyance shall be placed in a secure area or kept under guard surveillance until its loading and shipment for transport and unloading.

(c) Delay Measures:

Physical protection measures shall provide sufficient delay in the conveyance, freight container and package so that guards and response forces have reasonable time to intervene the removal of the material.

(d) Guards:

The licensee shall ensure that appropriately equipped and trained guards shall accompany each shipment, including before and during loading and unloading

operations. Surveillance of the route shall be conducted for any threat indicators and necessary response shall be initiated. Continuous, effective surveillance of the packages or locked cargo hold, or compartment holding the packages, shall be maintained at all times, especially when the conveyance is not on move.

(e) Communications:

Physical protection measures shall include provision of continuous two-way voice communication systems between the conveyance, any guards accompanying the shipment, the designated response forces, and where appropriate, the shipper and receiver. Such systems shall be redundant, diverse and secure.

(f) Response Forces:

The licensee shall make arrangements for the availability of response forces proportional to the prevailing threat to deal with physical protection events in time to prevent the unauthorized removal of nuclear material.

(g) Modal Requirements:

(1) For shipments by road, the consignment shall be shipped in a conveyance under exclusive use conditions i.e., in a conveyance used exclusively for that shipment.

(2) For shipments by rail, the consignment shall be shipped in a freight train in an exclusive use condition. Unless operationally impracticable, the consignment shall be shipped in a fully enclosed and locked conveyance. If not shipped in a fully enclosed and locked conveyance, additional approval by the PNRI is required.

(3) For shipments by water, the consignment shall be shipped on a vessel in a secure compartment or container which is locked and sealed.

(4) For shipments by air, the consignment shall be shipped in an aircraft designated for cargo only and in a secure compartment or container which is locked and sealed.

Section 32. ***Protection of Category I Nuclear Material against Unauthorized Removal.***

(a) In addition to the general requirements prescribed in Section 29 and specific requirements in Section 30 and 31 of this Part, the following requirements also apply to Category I nuclear material:

(1) Prior Shipment Requirements:

(i) The PNRI shall be intimated about exact date and time of shipment prior to the commencement of each shipment.

(ii) A detailed route surveillance shall be conducted based on the threat assessment or intelligence information.

(2) Transport Control Center:

The licensee shall establish a transport control center for the purpose of keeping track of the current position and physical protection measures status of the shipment of nuclear material, alerting response forces in case of an attack and maintaining continuous secure two-way voice communication with the shipment and the response forces. The transport control center shall be protected so that its function can continue in the presence of the threat. While the shipment is in process, the transport control center shall be staffed by appropriate personnel whose trustworthiness has been predetermined.

(3) Communication:

The licensee shall maintain continuous two-way communication between the conveyance, transport control center, guards accompanying the shipment, the response forces, and the receiver.

(4) Modal Requirements:

(i) For shipments by water, the consignment shall be transported in a dedicated transport vessel.

(ii) For shipments by air, the consignment shall be transported in an aircraft designated for cargo only and for which the nuclear material is its sole cargo.

Section 33. ***Prudent Management Practices.***

For nuclear material below Category III, prudent management practices of physical protection shall include the following:

(1) Basic security awareness training for all personnel involved;

(2) Verification of the identity of all personnel involved;

(3) Verification of security of conveyances used;

(4) Availability of written instructions;

(5) Exchange of information on security measures between operators, shippers or carriers and with competent authorities ensuring the need for confidentiality; and

(6) Determining the trustworthiness of the personnel involved.

Section 34. ***Measures to Locate and Recover Missing or Stolen Nuclear Material during Transport.***

(a) The licensee shall immediately notify the PNRI if nuclear material packages are determined to be missing or have been tampered with.

(b) The measures to locate and recover missing or stolen nuclear material shall be

included in the contingency plan and shall be tested and evaluated regularly.

(c) The licensee shall secure the nuclear material in situ as soon the missing or unauthorizedly removed nuclear material has been located and identified in accordance with the contingency plan.

(d) The licensee shall assist and coordinate with the response organizations to locate and recover its missing or unauthorizedly removed nuclear material.

Section 35. ***Measures for Protection against Sabotage.***

(a) Integration of Safety and Physical Protection: The safety features of the design of transport package, container and conveyance should be considered while deciding additional physical protection measures for protection of the material against sabotage.

(b) Additional Measures for Protection against Sabotage: Based on threat assessment or design basis threat and potential radiological consequences, licensee shall identify and implement additional physical protection measures to prevent sabotage of nuclear material during transport.

Section 36. ***Measures to Mitigate or Minimize the Radiological Consequences of Sabotage.***

(a) The licensee shall assess, on detection of a malicious act, whether this act could lead to radiological consequences and notify the PNRI.

(b) Immediately following an act of sabotage, the licensee shall take measures specified in the contingency plan to prevent further damage.

VI. RECORDS, REPORTS, AND NOTIFICATIONS

Section 37. ***Reportable Physical Protection Events***

The licensee shall report the following physical protection events:

(a) Actual or attempted intrusion into the nuclear installation or into a limited access area, protected area, inner area, or vital area.

(b) Attempted or actual unauthorized removal, loss or unauthorized movement of nuclear material, whether involving external adversaries or insiders.

(c) Attempted or actual acts of sabotage, including tampering or interference with vital area equipment, systems or devices.

(d) Loss or unauthorized disclosure of sensitive information.

(e) Failure of any physical protection equipment and system leading to loss of

physical protection system's function.

(f) Compromise or attempted compromise of digital computers, communication systems and networks used for physical protection and safety.

Section 38. ***Notifications of Events***

The licensee shall immediately notify PNRI by telephone or by any other fast means of communications of any events described in Section 37.

Section 39. ***Reports and Records***

(a) The licensee shall file within thirty (30) days an event report to the PNRI on the causes of the event, its circumstances and consequences, and on the compensatory measures or corrective actions taken after the occurrence or discovery of the event.

(b) The licensee shall maintain all records and reports required under this Part and license conditions for at least three (3) years after the record or report is superseded, unless specified otherwise by the PNRI.

(c) The licensee should include the names, addresses and contact details of all individuals who have been designated as authorized individuals.

VII. INSPECTION AND ENFORCEMENT

Section 40. ***Inspection***

(a) The licensee shall permit inspection, by duly authorized PNRI representatives, of his records, premises, activities, and of licensed materials in possession or use, related to the license as may be necessary to effectuate the purposes of the Act, as amended.

(b) The licensee shall afford any PNRI Inspector assigned to that site, or other PNRI inspectors identified as likely to inspect the nuclear installation, immediate unfettered access, equivalent to access provided to regular employees in the nuclear installation, following proper identification and compliance with applicable access control measures for security, radiation protection and personal safety.

(c) The licensee shall ensure that the arrival and presence of a PNRI inspector, who has been properly authorized access to the nuclear installation, is not announced or otherwise communicated by its employees or contractors to other persons at the nuclear installation unless specifically requested by the PNRI inspector.

Section 41. ***Enforcement***

In case of any non-compliance of these requirements, enforcement action will be initiated by the PNRI.

Section 42. ***Violation***

Any person who willfully violates or attempts to violate any provision of this Part or any order issued thereunder by the PNRI, shall be punished in accordance with the penal provision of the Act.

VIII. EFFECTIVITY

Section 43. ***Effectivity***

This Part shall take effect fifteen (15) days following the publication in the Official Gazette or in a newspaper of general circulation

Approved:

CARLO A. ARCILLA, Ph. D.
Director, PNRI

Date: 13 April 2022

APPENDIX A. SECURITY PLAN

A.1. An example of the possible structure for a security plan is set out in Box 1. After this outline, there is a brief discussion of the suggested contents of each section. The PNRI should review this proposed structure and modify it to meet their requirements and specific needs.

BOX 1: EXAMPLE STRUCTURE OF THE SECURITY PLAN

1. ADMINISTRATIVE INFORMATION
    - 1.1. Introduction and schedule for implementation
    - 1.2. Facility description (operations and layout)
        - 1.2.1. General facility description, mission and operations
        - 1.2.2. Facility layout
    - 1.3. Security policy
        - 1.3.1. Management policy
        - 1.3.2. Nuclear security culture
        - 1.3.3. Quality assurance
        - 1.3.4. Trustworthiness policy
        - 1.3.5. Sustainability program
    - 1.4. Security organization
        - 1.4.1. Security organization structure
        - 1.4.2. Security management and allocation of responsibilities
        - 1.4.3. Qualification requirements for security personnel
        - 1.4.4. Security personnel training
        - 1.4.5. Guards/response force armament and equipment
    - 1.5. Security of nuclear information
    - 1.6. Computer security
2. DEFINING THE PHYSICAL PROTECTION SYSTEM
    - 2.1. Objectives and requirements of the physical protection system
    - 2.2. Target identification
    - 2.3. Threat definition
    - 2.4. Law enforcement liaison
3. PHYSICAL PROTECTION SYSTEM

3.1. Detailed description of the physical protection system

BOX 1: EXAMPLE STRUCTURE OF THE SECURITY PLAN (cont.)

- 3.2. Insider threat mitigation program
- 3.3. Transport of nuclear material
- 3.4. Physical protection system testing, evaluation and maintenance
  - 3.4.1. Types of testing and evaluation
  - 3.4.2. Frequency of testing and evaluation
  - 3.4.3. Maintenance
  - 3.4.4. Expansion and upgrade
- 3.5. Compensatory measures

4. RESPONSE PLANNING

- 4.1. Organization and responsibilities
- 4.2. Security forces
  - 4.2.1. Guards
  - 4.2.2. On-site response force
  - 4.2.3. Off-site response force
  - 4.2.4. Central alarm station staffing
- 4.3. Contingency plan
- 4.4. Incident communications command and control
- 4.5. Response to higher threat conditions

5. POLICIES AND OPERATIONAL PROCEDURES

- 5.1. Documented policies and operational procedures
- 5.2. Review, evaluation, audit and update of the security plan
- 5.3. Reporting of threats or incidents

REFERENCES

ABBREVIATIONS AND GLOSSARY

ADMINISTRATIVE INFORMATION

A.2. This section includes information on the complete legal name and address of the entity responsible under law for the protection of the nuclear facility. The appropriate telephone and fax numbers and email addresses of those who are applying for approval of the security plan may be contained in a covering letter.

Introduction and schedule for implementation

A.3. This section includes a short description of the facility's mission and operations, maps of the facility and other information to indicate on these maps the locations of the major activities. The maps may depict terrain, transport routes, nearby towns or hazardous material facilities, and any other areas that could

affect response activities. The maps may also indicate main and alternative routes for law enforcement or other off-site responders.

Facility description (operations and layout)

A.4. This section provides details of nuclear operations undertaken at the facility.

General facility description, mission and operations

A.5. This section gives a general description of the types of nuclear activity that take place at the facility and the nuclear and other radioactive material used or generated by these activities.

Facility layout

A.6. A map, diagram or image of the facility, with key buildings and activities identified, may be provided in this section. Block diagrams of the various operations may be useful in describing the facility's activities.

Security policy

A.7. This section contains the facility's written security policy.

Management policy

A.8. This section describes the management system that provides oversight of the facility's physical protection, the purpose of which is to develop, revise, implement and oversee physical protection procedures. This section could also address how the safety–physical protection interface is managed.

Nuclear security culture

A.9. This section describes how the operator promotes nuclear security culture as an important part of delivering the security policy to management, employees and contractors.

Quality assurance

A.10. This section describes the quality assurance aspects of the management policy and program applicable to physical protection.

Trustworthiness policy

A.11. This section describes the trustworthiness levels and requirements applied to employees and contractors at the nuclear facility for access to specified areas within the facility (e.g. protected areas, inner areas, vital areas), to nuclear material and to sensitive information, as well as the measures taken to ensure continued trustworthiness.

Sustainability program

A.12. This section describes the sustainability program for the physical protection system.

Security organization

A.13. All individuals with security responsibilities may be identified with a brief description of their duties and responsibilities. This section may include the requirements for selecting, training, equipping, testing and qualifying individuals who will be responsible for protecting nuclear material and nuclear facilities. As appropriate to the operator's assigned responsibilities and capabilities, this section needs to state which parts of the security organization are provided by staff and which by external contractors. For contractors, this section may briefly describe the written agreements between the operator and contractors that describe how they will meet the requirements to protect the facility. The level of detail included in the security plan may vary depending on the facility, but this section needs to provide enough information for a reader to understand the capabilities of the security forces for the facility. The information provided seeks to confirm that the security organization is designed, staffed, trained, qualified and equipped to implement physical protection.

Security organization structure

A.14. This section describes the structure of the security organization, including management, guards and any on-site response force, technical security personnel and other persons responsible for physical protection related functions. This section may also contain a description of each supervisory and management position, including responsibilities and how lines of authority extend up to facility and corporate management.

Security management and allocation of responsibilities

A.15. This section describes the specific physical protection responsibilities assigned to the facility's security organization.

Qualification requirements for security personnel

A.16. A description may be provided of the requirements for the initial and continued suitability of individuals who are assigned security duties and responsibilities. This section may also describe the process to ensure that these personnel continue to be qualified to provide the required services. This section also includes a description of the firearms qualification and requalification requirements for guards and on-site response force members.

Security personnel training

A.17. This section describes the training program for guard and on-site response forces. It also describes how they demonstrate their ability to carry out their

assigned duties or responsibilities. For response forces, a description of the training program in response tactics may be included.

Guards/response force armament and equipment

A.18. This section describes the armaments assigned to members of the guards and on-site response force, by position title. A description of other equipment available to the guards and response forces to enable them to provide effective response capabilities may be provided.

Security of nuclear information

A.19. This section defines the measures that are taken to maintain the confidentiality, integrity and availability of sensitive information. Information management procedures also need to describe how the distribution of sensitive information is limited to appropriate individuals, whose trustworthiness has been appropriately determined, on a need-to-know basis. Controls applied to sensitive information may include records of its receipt, location, dispatch and destruction.

Computer security

A.20. This section describes the access control procedures, protocols and physical security arrangements in place to ensure the confidentiality, integrity and availability of sensitive information held on computers and computer based systems, as well as the integrity and availability of instrumentation and control systems.

DEFINING THE PHYSICAL PROTECTION SYSTEM

Objectives and requirements of the physical protection system

A.21. This section describes the objectives for the protection of different types of target, grouped according to their level of sensitivity.

Target identification

A.22. This section lists the potential theft or sabotage targets and their location. It also lists the computer systems important to physical protection, safety and nuclear material accounting and control the compromise of which could help facilitate a malicious act.

Threat definition

A.23. This section describes, in broad terms, the types of threat the physical protection system is designed to protect against and references the threat assessment or design basis threat defined by the State.

Law enforcement liaison

A.24. Details may be provided of how routine liaison is maintained with law enforcement agencies to help ensure early warning of potential security events.

PHYSICAL PROTECTION SYSTEM

A.25. This section is a description of the physical protection system at the facility.

Detailed description of the physical protection system

A.26. In this section, a facility map indicating the layer boundaries and protection measures, such as personnel–vehicle control points, may be provided. A description of the protection measures needs to be provided, as described below:

(a) *Access control.* A description of the control and search of personnel, vehicles and material at each access control point needs to be provided. This description can also include how access authorization and access control systems will accommodate the rapid entry and exit of authorized individuals and vehicles during emergencies or in situations that could lead to emergencies. Attention may be given to the control of all keys, locks, combinations, passwords and related devices used to control access to limited access areas, protected areas, inner areas, vital areas and physical protection equipment.

(b) *Central alarm station.* This section describes the location of the central alarm station and any backup monitoring stations. It also describes the central alarm station alarm communication and display systems, communications equipment, and access control arrangements and details how the central alarm station is protected against attack and unauthorized access.

(c) *Communications.* The communications capabilities for the guards and on-site response forces need to be described, as do the communications between the central alarm station and the guard and response forces. This section describes how a continuous communications capability is maintained to ensure effective command and control with on-site and off-site response forces during normal and emergency situations. If there are areas of the facility where communication is limited, these areas need to be identified.

(d) *Detection and surveillance.* This section describes the detection system and how alarms are communicated to the central alarm station and assessed. The section may also describe procedures to address situations in which there are indications of tampering. It describes the methods to continuously survey, observe and monitor facility areas to detect intruders and to ensure the integrity of physical barriers or other components and functions of the physical protection system.

(e) *Lighting.* This section describes how the operator maintains the minimum illumination levels for selected applications, such as assessment after an alarm.

(f) *Physical barriers.* This section describes the barriers in different security areas within the facility (e.g. buildings, topography, fences, walls, doors). It may also contain a description of the vehicle barriers, their placement and operation, as well as associated surveillance arrangements.

(g) *Security areas/layers.* This section identifies the physical protection areas (or layers) that exist at the facility.

Insider threat mitigation program

A.27. This section should describe measures to protect against insider threats.

Transport of nuclear material

A.28. This section describes the procedures for the on-site transport of different categories of nuclear material, as well as the arrangements made on-site for the receipt and dispatch of nuclear material to and from the facility.

Physical protection system testing, evaluation and maintenance

A.29. This section identifies the procedures for evaluating and testing the physical protection system.

Types of testing and evaluation

A.30. This section describes the testing and evaluation programs that exist and how they are used to assess the effectiveness of the facility's physical protection system.

Frequency of testing and evaluation

A.31. Details need to be provided of the frequency with which the testing and evaluation programs are implemented.

Maintenance

A.32. This section describes the maintenance and calibration programs for all physical protection equipment.

Expansion and upgrade

A.33. This section is available to describe any schedule foreseen for implementing physical protection measures related to new construction or the significant physical modification of existing structures or the installation of equipment.

Compensatory measures

A.34. This section identifies all compensatory physical protection measures applied when physical protection barriers become degraded or equipment becomes inoperable, including during routine testing or maintenance. In particular, the provision of standby power to all types of physical protection equipment needs to be described.

RESPONSE PLANNING

Organization and responsibilities

A.35. This section provides details of the organization and responsibilities of the facility and off-site response forces to maintain an effective response strategy for the various targets at the facility.

Security forces

A.36. This section provides an overview of the response forces available to deliver a coordinated response strategy.

Guards

A.37. This section describes the number, location and duties of the guard force, including details of their weapons, equipment and transport.

On-site response force

A.38. This section describes the on-site response force capacity and capability to respond to nuclear security events in a timely manner, where such a force is employed.

Off-site response force

A.39. This section describes off-site response force capacity and capability to respond to nuclear security events, including estimated response times. The process of documenting and maintaining agreements for providing off-site response may be included.

Central alarm station staffing

A.40. This section describes the minimum number, duties, responsibilities and rotation schedule of staff employed in the central alarm station.

Contingency plan

A.41. This section describes the contingency plan for nuclear security events and for other events that may need a physical protection response. It identifies specific people and/or positions that have the responsibility and authority to carry out

the contingency plan should a nuclear security event occur. It details how and when the contingency plan is reviewed and exercised.

A.42. The list below suggests examples of different types of scenario that may be considered and addressed in the contingency plan:
(a) Location and recovery of missing nuclear material (including emergency inventory taking);
(b) Minimization and mitigation of the radiological consequences of sabotage;
(c) Discovery of an insider threat;
(d) Unauthorized intrusion into a nuclear facility;
(e) External threats (e.g. bomb warning);
(f) Stand-off attack;
(g) Airborne attack;
(h) Water-borne attack;
(i) Cyber attack;
(j) Compromise of sensitive information.

A.43. As the contingency plan will contain sensitive information, it needs to be appropriately marked to indicate the level of protection required. It also needs to address arrangements for coordination with emergency plans. An example of a contingency plan is given in Appendix II.

Incident communications command and control

A.44. The security plan describes how effective command and control will be exercised in response to a nuclear security event by the agencies involved, where the on-site and off-site incident command and control centre will be located and what communications facilities will be available at these locations.

Response to higher threat conditions

A.45. A list should be provided of the planned enhancements to physical protection procedures that will be put in place in the event of any increase in the overall level of threat within the State.

POLICIES AND OPERATIONAL PROCEDURES

Documented policies and operational procedures

A.46. This section lists the documented policies and operational procedures that govern physical protection at the facility, including procedures for interfacing with systems that complement the physical protection system, such as the safety and nuclear material accounting and control systems.

Review, evaluation, audit and update of the security plan

A.47. Details need to be provided of the procedures and review processes (including their frequency) employed to ensure that the security plan remains current,

together with an assurance that all necessary amendments to it will be submitted to the competent authority for approval prior to implementation.

Reporting of threats or incidents

A.48. The procedure for facility employees and contractors to report specified occurrences to the facility's security organization, and for their onward reporting to the competent authority, as appropriate, is described in this section.

APPENDIX B. EXAMPLE CONTINGENCY PLANS

OBJECTIVE

B.1. This section describes the objective of the contingency plan. The objective may be to prepare for a further response or to reduce the consequence of the adversary's actions.

INCIDENT RESPONSE PROCEDURES

Rules of engagement

B.2. This section includes the rules of engagement that define what sort of force is authorized under the law and when and where such force can be used.

Response procedures

B.3. This section describes how the response is organized and coordinated. It identifies those indicators that will be used to signal the initiation of a response under this contingency plan. The section may include:

(a) All predetermined actions, areas of responsibility and timelines for the deployment of the response force for theft and sabotage scenarios;

(b) Procedures that limit the exposure of the response personnel to possible attack;

(c) Timelines to be used when notifying the off-site response force;

(d) The minimum number of responders.

Recapture and recovery

B.4. This section states how the response is organized when the adversary has left the facility in a theft scenario. It includes the protocols used to coordinate the different response teams, the chain of command and any change in responsibilities.

Minimize and mitigate

B.5. This section states how the physical protection response is organized to help emergency responders minimize and mitigate the consequences of a sabotage attack.

Command, control and communication

B.6. This section describes the arrangements documented in protocols agreed with external response organizations. It details which agency has the operational lead and the circumstances in which this lead may be handed over to another

agency. Details are provided of all the communication links to be used and the location of the incident control centers that may be used at different stages of the event, taking into account prevailing circumstances and the centers' strategic and tactical responsibilities.

EXERCISING THE CONTINGENCY PLAN

B.7. This section describes the type and frequency of exercises undertaken to test and practice implementation of the contingency plan. The information includes testing coordination between the contingency plan and the emergency plan through joint exercises in which both plans are implemented. The section also describes how lessons learned from these exercises are captured and used to further refine the contingency plan.

APPENDIX C. THE ADDITION OR AGGREGATION OF NUCLEAR MATERIAL

APPROACH 1

C.1. This example illustrates one way in which Table 1 may be used to categorize aggregated nuclear material. Nuclear material located in the same facility should be classified as outlined:

(a) Category I if:

$$\frac{Pu + {}^{233}U}{2000} + \frac{{}^{235}U(\geq 20\%)}{5000} \geq 1 \qquad (1)$$

(b) Category II if:

$$\frac{Pu + {}^{233}U}{500} + \frac{{}^{235}U(\geq 20\%)}{1000} + \frac{{}^{235}U(\geq 10\% \text{ and } < 20\%)}{10000} \geq 1 > \frac{Pu + {}^{233}U}{2000} + \frac{{}^{235}U(\geq 20\%)}{5000} \qquad (2)$$

(c) Category III if:

$$\frac{Pu + {}^{233}U}{15} + \frac{{}^{235}U(\geq 20\%)}{15} + \frac{{}^{235}U(\geq 10\% \text{ and } < 20\%)}{1000} + \frac{{}^{235}U(> U_{nat} \text{ and } < 10\%)}{10000} \geq 1 > \frac{Pu + {}^{233}U}{500} + \frac{{}^{235}U(\geq 20\%)}{1000} + \frac{{}^{235}U(\geq 10\% \text{ and } < 20\%)}{10000} \qquad (3)$$

(d) Below Category III if:

$$1 > \frac{Pu + {}^{233}U}{15} + \frac{{}^{235}U(\geq 20\%)}{15} + \frac{{}^{235}U(\geq 10\% \text{ and } < 20\%)}{1000} + \frac{{}^{235}U(> U_{nat} \text{ and } < 10\%)}{10000} \qquad (4)$$

or if the material consists only of natural uranium, depleted uranium or thorium,

where

Pu	is the mass in grams of all plutonium except that with isotopic composition exceeding 80% in 238Pu;
233U	is the mass in grams of 233U;
235U (≥20%)	is the mass in grams of 235U present in a form enriched to 20% 235U or more;
235U (≥10% and <20%)	is the mass in grams of 235U present in a form enriched to 10% 235U or more, but less than 20% 235U;

235U (>Unat and <10%) is the mass in grams of 235U present in a form enriched above natural but less than 10% 235U;

and the denominators are masses in grams.

C.2. These formulas relate to material that is not irradiated in a reactor or to material irradiated in a reactor but with a radiation level equal to or less than 1 Gy/h (100 rad/h) at 1 m unshielded.

APPROACH 2

C.3. Another approach for determining the category of aggregated nuclear material uses the following formula:

$$\frac{1}{S}=\sum_i \frac{f_i}{S_i} \qquad (5)$$

where

fi (dimensionless) is the mass fraction of material type i of the mixture (mass of each material type present divided by the total mass of material present);

Si (kg or g) is the mass threshold for material type i for the category being considered, as listed in Table 1;

and S (kg or g) is the mass threshold for the aggregation of material for the category being considered, as listed in Table 1.

C.4. The following are the mass thresholds for Category I:

(a) 2 kg of plutonium, all isotopes combined;
(b) 5 kg of 235U present in a form enriched to 20% 235U or more;
(c) 2 kg of 233U.

C.5. The following are the mass thresholds for Category II:

(a) 500 g of plutonium, all isotopes combined;
(b) 1 kg of 235U present in a form enriched to 20% 235U or more;
(c) 10 kg 235U present in a form enriched to at least 10% and less than 20% 235U;
(d) 500 g of 233U.

C.6. The following quantities are the mass thresholds for Category III:

(a) 15 g of plutonium, all isotopes combined;
(b) 15 g of 235U present in a form enriched to 20% 235U or more;
(c) 1 kg of 235U present in a form enriched to at least 10% and less than 20% 235U;

(d) 10 kg of 235U present in a form enriched to less than 10% 235U;
(e) 15 g of 233U.

C.7. All plutonium is considered, except that with isotopic concentration exceeding 80% in 238Pu.

C.8. These thresholds relate to material that is not irradiated in a reactor or to material irradiated in a reactor but with a radiation level equal to or less than 1 Gy/h (100 rad/h) at 1 m unshielded.

C.9. To determine the applicable category, first determine (step 1) whether the aggregated material is Category I. A material, or a mixture of materials, is Category I if the aggregated mass is greater than or equal to the Category I mass threshold calculated for the material or mixture. If it is not Category I, proceed to step 2.

C.10. If the aggregated material is not Category I, determine (step 2) whether it is Category II. A material, or a mixture of materials, is Category II if the aggregated mass is greater than or equal to the Category II mass threshold calculated for the material or mixture. If it is not Category II, proceed to step 3. III.11. If the aggregated material is not Category I or II, determine (step 3) whether it is Category III. A material, or a mixture of materials, is Category III if the aggregated mass is greater than or equal to the Category III mass threshold calculated for the material or mixture.

C.12. If the mass of the material or mixture of materials falls below the Category III mass threshold, it is below Category III.

Example 1

C.13. The nuclear material consists of 4 kg of 235U, contained in uranium enriched to greater than 20%, and 1 kg of plutonium, making a total of 5 kg of 235U and plutonium combined. The mass fraction of uranium enriched to greater than 20% is 4/5 and for plutonium is 1/5.

Step 1: The Category I mass threshold for this material is given by:

$$\frac{1}{S} = \frac{4/5}{S_{\mathrm{U-235}}} + \frac{1/5}{S_{\mathrm{Pu}}} = \frac{4/5}{5\ kg} + \frac{1/5}{2\ kg} = 0.2$$

Therefore, S = 3.85 kg. Since the mass of the material (5 kg) is greater than S (3.85 kg), it is above the threshold for Category I for this mixture.

The material is therefore a Category I quantity.

Example 2

C.14. The nuclear material consists of 2.5 kg of 235U, contained in uranium enriched to greater than 20%, and 500 g of plutonium, making a total of 3 kg of 235U and plutonium combined. The mass fraction of uranium enriched to greater than 20% is 2.5/3 (or 5/6) and for plutonium is 0.5/3 (or 1/6).

Step 1: The Category I mass threshold for this material is given by:

$$\frac{1}{S} = \frac{5/6}{S_{\mathrm{U-235}}} + \frac{1/6}{S_{\mathrm{Pu}}} = \frac{5/6}{5\ kg} + \frac{1/6}{2\ kg} = 0.25$$

Therefore, S = 4 kg. The total mass is 3 kg, which is below the mass threshold for the mixture for Category I.

Step 2: The Category II mass threshold for this material is given by:

$$\frac{1}{S} = \frac{5/6}{S_{\mathrm{U-235}}} + \frac{1/6}{S_{\mathrm{Pu}}} = \frac{5/6}{1\ kg} + \frac{1/6}{0.5\ kg}$$

Therefore, S = 0.86 kg. The total mass is 3 kg, which is above the mass threshold for the mixture for Category II. Therefore, the mixture is Category II.