REGULATION

Regulation on Physical Protection of Nuclear Material and Nuclear Facilities and on Cyber Security

(FANR-REG-08)

Version 2

2024

Federal Authority for Nuclear Regulation (FANR)

P.O. Box 112021, Abu Dhabi, United Arab Emirates

regulation@fanr.gov.ae

Contents

Preamble

This regulation is issued by the Federal Authority for Nuclear Regulation pursuant to the powers conferred to its Board of Management in Article 11(4) and Article 38(1) of the Federal Law by Decree No. 6 of 2009 Concerning the Peaceful Uses of Nuclear Energy (the Law).

Definitions

Article (1)

1. For the purposes of this regulation, the following terms shall have the meaning ascribed to them in Article 1 of the Law, unless context requires otherwise: Authority, Construction, Design, Emergency, Emergency Preparedness, Ionising Radiation, Licence, Licensee, Management System, Nuclear Facility, Nuclear Fuel, Nuclear Reactor, Nuclear Safety, Nuclear Security, Operation, Person, Physical Protection, Radioactive Material, Safety, Spent Nuclear Fuel and State.

2. In addition, the following terms shall have the meaning set forth below:

Advanced Nuclear Technologies (ANTs)	ANTs encompass a wide range of innovative nuclear technologies, including Small Modular Reactors (SMRs) and Advanced Modular Reactors (AMRs), which may vary depending on their size, scalability, location, modularity, application, fuel types, cooling medium, remote operability, enhanced Nuclear Safety features and centralised monitoring capabilities.
Central Alarm Station	An installation that provides for the complete and continuous monitoring and assessment of alarms and communication with Guards, facility management and Security Response Forces.
Competent Authorities	The government entities that are responsible for security measures in the State and in each Emirate of the State.
Contingency Plan	Predefined sets of actions for effective response to unauthorised acts indicative of attempted Malicious Acts, up to and including the Design Basis Threat, as well as threats thereof.
Contraband	Unauthorised firearms, explosives, incendiaries, dangerous items, materials and/or vehicles that

	could be used to commit a Malicious Act, including threat thereof.
Cyber Security	Protection from cyber attacks of digital computer and communications systems and networks associated with certain categories of functions and support systems and equipment, which if compromised, would adversely impact the Safety, security, safeguards and Emergency Preparedness functions (including off-site communications) of a Nuclear Facility.
Cyber Security Plan	A plan that describes Cyber Security measures and the governance for their implementation by the Licensee.
Defence-in-depth	The combination of multiple layers of systems and measures that have to be overcome or circumvented before Physical Protection or Cyber Security is compromised.
Design Basis Threat	The attributes and characteristics of a potential Insider and/or external adversaries, who might attempt a Malicious Act, against which a Physical Protection System is designed and evaluated.
Detection	A process in a Physical Protection System, which begins with sensing a potentially Malicious Act or otherwise unauthorised act with an alarm and which is completed with the assessment of the cause of the alarm.
Guards	Persons who are entrusted by the Licensee with responsibility for patrolling, monitoring, assessing, and escorting individuals or Transport, controlling access, reporting Nuclear Security Events and/or providing initial response in coordination with the Security Response Forces.
Insider	One or more individuals with authorised access to a Nuclear Facility or Nuclear Material in Transport who could attempt or carry out a Malicious Act, or who could aid an external adversary to do so.

Intrusion Detection System	A system that gathers and analyses information from various areas to identify possible security breaches, which include, among others, intrusions into the Protected Area.
Malicious Act	An attempt or act of Unauthorised Removal, Radiological Sabotage or cyber attack, which may result in a Nuclear Security Event.
Nuclear Material	The term covers the categories of nuclear material specified in Annex 1 of this regulation.
Nuclear Security Culture	The assembly of characteristics, attitudes and behaviours of individuals, organisations and institutions, which serve as means to support, enhance and sustain Nuclear Security.
Nuclear Security Event	An event that is assessed as having implications for Physical Protection or Cyber Security.
Owner Controlled Area	A designated area containing a Nuclear Facility or Nuclear Material to which access is limited and controlled for Physical Protection purposes.
Physical Protection Measures	The personnel, procedures, and equipment that constitute a Physical Protection System.
Physical Protection Plan	A plan that shall be developed by an applicant as part of its application for a Licence, and which shall be implemented and maintained by a Licensee.
Physical Protection System	An integrated set of Physical Protection Measures intended to prevent the completion of a Malicious Act.
Protected Area	An area inside an Owner Controlled Area containing category I or II Nuclear Material and/or Radiological Sabotage Target Sets surrounded by a physical barrier with additional Physical Protection Measures.
Radiological Sabotage	Any deliberate act directed against a Nuclear Facility or against 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 Ionising Radiation or the release of Radioactive Material.
Secondary Alarm Station	An installation that provides for the redundant functionality of the Central Alarm Station.
Security Response Forces	Individuals assigned by the Competent Authorities and stationed on-site or off-site who are armed and appropriately equipped and trained to counter an attempted Unauthorised Removal or Radiological Sabotage.
Sensitive Nuclear Information	Information in verbal, written or electronic form, which is classified either for national security or Nuclear Security reasons.
Structures, Systems and Components (SSCs)	A general term encompassing all the elements of a Nuclear Facility, which contribute to protection and Nuclear Safety, except human factors. Structures are the passive elements such as building vessels and shielding. A System comprises several components assembled in such a way so as to perform a specific active function and a Component is a discrete element of a system.
Target Elements	Structures, Systems or Components of a Nuclear Facility, as well as any personnel performing actions or functions to prevent core damage or Spent Nuclear Fuel damage.
Target Set	The minimum combination of Target Elements, which if all are prevented from performing their intended function or prevented from being accomplished, would cause core damage or Spent Nuclear Fuel damage and result in a release of Radioactive Material.
Transport	An international or domestic shipment of Nuclear Material by any means of transport, beginning with the departure of the Nuclear Material from a Nuclear Facility of a supplier and ending with the arrival of the Nuclear Material at the site of a Nuclear Facility of the recipient.

Unauthorised Removal	The theft or other unlawful taking of Nuclear Material.
Vital Area	An area inside a Protected Area containing equipment, systems or devices, or Nuclear Material, a Radiological Sabotage of which could directly or indirectly result in a release of Radioactive Material.
Vulnerability Assessment	A process for evaluating and documenting the features and effectiveness of the overall Physical Protection System.

Objective and Scope

Article (2)

1. This regulation establishes requirements for Physical Protection and Cyber Security and applies to:

    a) an applicant for and/or a Licensee holding a Licence for the Construction of a Nuclear Facility that contains a Nuclear Reactor;

    b) an applicant for and/or a Licensee holding a Licence for the Operation of a Nuclear Facility that contains a Nuclear Reactor; and

    c) an applicant for and/or a Licensee holding a Licence for Transport within the State of category I, II or III Nuclear Material categorised in Annex 1.

2. Article 28 of this regulation establishes requirements for Physical Protection and Cyber Security, which apply to:

    a) an applicant for and/or a Licensee holding a Licence for the Construction of a Nuclear Facility that does not contain a Nuclear Reactor; and

    b) an applicant for and/or a Licensee holding a Licence for the Operation of a Nuclear Facility that does not contain a Nuclear Reactor.

3. Article 29 of this regulation establishes requirements for Physical Protection and Cyber Security, which apply to Persons planning to develop and/or deploy Advanced Nuclear Technologies in the State.

Records and Written Procedures

Article (3)

1. The Licensee shall maintain records as per the approved Physical Protection Plan and/or the Transport security plan in either hard copy format or electronic media for at least three (3) years after the record is made, or until the record is superseded, whichever is longer, or as specified in the Physical Protection Plan or in the Transport security plan approved by the Authority.

2. At a minimum, the records pertinent to the Physical Protection Plan shall include the following:

    a) the names and badge numbers of all individuals granted unescorted access to the Protected Area;

    b) the names of individuals granted access to category I, II or III Nuclear Material and to a Vital Area;

    c) the name of each individual and the time of entry into and exit from a Vital Area;

    d) the names of individuals in possession of keys or key-cards and/or have any authorised access to systems, including computer systems, that control access to category I, II or III Nuclear Material, the Protected Area or Vital Areas;

    e) the name of each individual granted escorted access to the Protected Area and the time of each entry into and exit of such individual from the Protected Area;

    f) documentation of each routine security tour and inspection;

    g) details of tests and maintenance of security-related equipment carried out in accordance with Article 19 of this regulation;

    h) details of each on-site security alarm triggered and details of the response; and

    i) security-related procedures.

3. At a minimum, the records pertinent to the Transport security plan shall include the following:

    a) the names of individuals granted access to category I, II or III Nuclear Material;

    b) the names of individuals in possession of keys or key-cards and/or have any authorised access to systems, including computer systems, that control access to category I, II or III Nuclear Material;

    c) documentation of each routine security tour and inspection;

    d) details of the shipments of category I, II or III Nuclear Material; and

e) security-related procedures.

4. The applicant for a Licence shall develop and the Licensee shall implement and maintain a system of written procedures for the conduct of the activities described in the Physical Protection Plan and/or the Transport security plan.

Sensitive Nuclear Information and Other Classified Information

Article (4)

1. The Licensee shall take appropriate measures for the protection of Sensitive Nuclear Information consistent with the requirements of the Information Protection Programme Operating Manual (IPPOM).

2. The Licensee shall establish, implement and maintain an information classification and protection system in accordance with all the relevant applicable legislation in the State to protect Sensitive Nuclear Information and other classified information.

3. The Licensee shall establish and maintain a list of the individuals who are authorised to access Sensitive Nuclear Information and other classified information. The list shall be reviewed and updated at least twice a year. The Licensee shall establish and maintain a list of the individuals whose application for access to Sensitive Nuclear Information and other classified information has been denied and a list of the individuals whose access to Sensitive Nuclear Information and other classified information has been cancelled.

4. The Licensee shall report to the Authority within twenty-four (24) hours of discovery of the loss, compromise, unauthorised receipt or suspected compromise of Sensitive Nuclear Information and other classified information.

Management System Requirements

Article (5)

1. The Licensee's Management System shall include all the activities related to the Physical Protection of a Nuclear Facility and Transport of category I, II and III Nuclear Material.

2. The Licensee shall use the Management System to promote and support an effective Nuclear Security Culture including through continuous awareness and training.

Nuclear Facility Site

Article (6)

1. The selection and/or preparation of a site for the Construction of a Nuclear Facility shall take into account the Physical Protection Measures as early as possible in coordination with the relevant Competent Authorities and the Authority. It shall also address interface

between Physical Protection and Safety to avoid any conflicts and to ensure that the two elements support each other.

2. As required under the Design Basis Threat for a Nuclear Facility, the siting of the Nuclear Facility shall be such that unauthorised individuals are not able to be in proximity to the site of the Nuclear Facility through the use of public roads and other public areas.

3. The impact of topographical features and topographic terrain lines on the Physical Protection of the site of a Nuclear Facility shall be taken into consideration by an applicant for a Licence for the selection and/or preparation of a site for the Construction of a Nuclear Facility.

Construction of a Nuclear Facility

Article (7)

1. On a site hosting multiple units, where the activities at different units of a Nuclear Facility undergo different phases, the Physical Protection for each unit shall be implemented in line with the Construction or Operation phase of each unit of the Nuclear Facility. A boundary shall be established and maintained between the units that are not in the same phase of implementation of Physical Protection requirements so that any material and/or individuals seeking to cross the boundary are controlled in line with the Physical Protection requirements for the unit into which entry is sought. Entry into a unit in Operation from a unit under Construction shall be controlled in accordance with the Physical Protection requirements for the unit in Operation.

2. An applicant for a Licence for the Construction of a Nuclear Facility shall develop a Physical Protection Plan that shall include a description of:

    a) the physical barrier around the Nuclear Fuel with an Intrusion Detection System;

    b) the control of access to the area referred to in Article 7(2)(a) of this regulation; and

    c) the response actions to Nuclear Security Events.

3. The applicant for a Licence for the Construction of a Nuclear Facility shall develop and the Licensee shall implement and maintain a fitness-for-duty programme, including psychological assessments, tests for drugs, psychotropic substances and alcohol, for individuals who are involved in or directing the Construction of Structures, Systems and Components or Physical Protection System and measures on the site of the Nuclear Facility. This fitness-for-duty programme shall deter substance abuse and detect indications of:

    a) possible use, sale or possession of illegal drugs or psychotropic substances;

    b) possible use, sale or possession of alcohol; and

c) impairment from any cause that if left unattended may result in a risk to Safety or Physical Protection.

Physical Protection Plan for the Operation of a Nuclear Facility

Article (8)

1. An applicant for a Licence for the Operation of a Nuclear Facility shall develop a Physical Protection Plan to address the protection of the Nuclear Facility against the Design Basis Threat and shall obtain the Authority's approval thereof.

2. The Physical Protection Plan shall include, inter alia, the following elements:

   a) description of the monitoring, control and response measures of the Licensee;

   b) description of arrangements between the Licensee's security organisation, Competent Authorities and Security Response Forces to respond to Nuclear Security Events;

   c) description of the Physical Protection System;

   d) Target Set analysis;

   e) Vulnerability Assessment;

   f) Contingency Plan;

   g) description of compensatory measures; and

   h) Cyber Security Plan.

3. The Licensee shall implement the approved Physical Protection Plan in coordination with the Competent Authorities and shall review the Physical Protection Plan at least every twenty-four (24) months.

4. The Licensee shall inform the Authority of any intended change to the Physical Protection Plan and provide an explanation and justification for the change for review and approval thereof by the Authority prior to implementing the change in the Physical Protection Plan.

Monitoring, Control and Response Measures

Article (9)

1. The Licensee shall establish and maintain the twenty-four (24) hours on duty Guards for day-to-day activities in the Owner Controlled Area and Protected Area. The minimum number of Guards shall be defined in the Physical Protection Plan.

2. The Guards shall be trained, qualified and equipped to ensure the implementation of the day-to-day activities as well as to implement their responsibilities as per the Contingency Plan in coordination with the Security Response Forces.

3. The Licensee shall support the response of the Security Response Forces to any Nuclear Security Event up to and including the Design Basis Threat.

4. The Competent Authority shall ensure the Security Response Forces respond, in coordination with the Licensee, to any Nuclear Security Event up to and including the Design Basis Threat.

5. The Licensee shall establish and maintain arrangements between the Guards and the Security Response Forces to respond to Nuclear Security Events. These arrangements shall be described in the Physical Protection Plan.

6. The Licensee shall establish and maintain a dedicated and secured voice communication network between Guards, Security Response Forces, the Central Alarm Station and Secondary Alarm Station.

Physical Protection Interface with Safety

Article (10)

1. The Licensee shall assess and manage the Physical Protection interface with Safety and control activities in such a manner that ensures that they do not adversely affect each other and that they are mutually supportive to the extent possible.

2. The Licensee shall establish, implement and maintain an effective process to ensure that any proposed change to the Physical Protection interface with Safety is thoroughly evaluated to verify that it does not result in significant implications for Safety and/or does not jeopardise Physical Protection.

Potential Insider Threats

Article (11)

1. The Licensee shall establish, maintain and implement an Insider mitigation programme and shall describe the programme in the Physical Protection Plan.

2. The Insider mitigation programme shall monitor the initial and continuing trustworthiness and reliability of individuals granted or retaining unescorted access authorisation to a Protected Area or Vital Area, and implement Defence-in-depth methodologies to minimise the potential for an Insider to adversely affect, either directly or indirectly, the Licensee's capability to prevent a Malicious Act.

3. The following elements shall support the Insider mitigation programme:

a) an access authorisation programme;

b) a fitness-for-duty programme, including psychological assessments and tests for drugs, psychotropic substances and alcohol to be conducted

   i. when an individual is first granted access to the Protected Area; and

   ii. after an event involving an individual who may have caused or contributed to the event.

c) the Cyber Security Plan; and

d) the Physical Protection System.

4. The Licensee shall conduct random drugs and alcohol tests on individuals granted access to the Protected Area.

Target Sets Analysis

Article (12)

1. The Licensee shall identify the Target Sets, the Radiological Sabotage of which could directly or indirectly result in the release of Radioactive Material.

2. The Licensee shall document and maintain the process used to develop and identify Target Sets. Such documentation shall be classified and maintained as Sensitive Nuclear Information.

3. The Licensee shall consider the threat of cyber attacks in the development and identification of Target Sets.

4. The Licensee shall implement a control process for Design change to ensure that changes to Target Elements or Target Sets are evaluated for potential adverse impacts on the Physical Protection Plan.

Physical Protection System

Article (13)

The Licensee shall develop and maintain a detailed description of the Physical Protection System, which, through the implementation of Physical Protection Measures, shall prevent, detect and delay access by a potential adversary to a Nuclear Facility and prevent completion of a Malicious Act.

Physical Barriers

Article (14)

1. The Licensee shall develop, implement and maintain a Defence-in-depth approach for protecting a Nuclear Facility against Unauthorised Removal or Radiological Sabotage. As a minimum, three (3) layers of protection of the Target Sets from outside the Nuclear Facility shall be put in place at the Owner Controlled Area, Protected Area and Vital Areas.

2. The Licensee shall ensure that all alarm equipment, alarm communication paths and the Central Alarm Station are provided with an uninterruptible power supply and are protected from equipment tampering and unauthorised monitoring, manipulation and falsification.

Owner Controlled Area

Article (15)

The Licensee shall establish, implement and maintain an Owner Controlled Area surrounding the Protected Area and Vital Areas within the Nuclear Facility. As a minimum, the Owner Controlled Area shall have:

a) a physical barrier to protect against unauthorised access;

b) a limited and controlled access for individuals and vehicles; and

c) arrangements and measures to detect and respond to any Malicious Act or unauthorised access.

Protected Area

Article (16)

The Licensee shall establish, implement and maintain a Protected Area inside the Owner Controlled Area, which itself contains Vital Areas. As a minimum, the Protected Area shall have:

a) a physical barrier with limited access points and with features to protect against unauthorised access by land and waterborne vehicles as specified in the Design Basis Threat;

b) an isolation zone adjacent to the Protected Area perimeter barrier to permit observation and assessment of the activities on either side of that barrier without obstructions;

c) sufficient illumination of the isolation zone and of all the exterior areas within the Protected Area of not less than 0.2 foot-candle measured horizontally at the ground level;

d) a limited and controlled access for individuals and vehicles that includes a comprehensive search for prohibited items at the entrance from the Protected Area at all access points; and

e) an Intrusion Detection System to monitor the isolation zone as well as an assessment system for confirming an intrusion around the perimeter of the Protected Area, including access points and emergency exits.

Vital Area

Article (17)

1. The Licensee shall establish, implement and maintain Vital Areas inside the Protected Area. As a minimum, the Vital Area shall have:

a) a physical barrier made of solid walls and a floor and ceiling without any unattended pathway outside each Vital Area;

b) a limited and controlled access of individuals with two authentication systems;

c) a limited and controlled access only to the vehicles required for activities inside the Vital Area;

d) an Intrusion Detection System and a system of closed-circuit television (CCTV) to be used to confirm any attempt of intrusion; and

e) a protection against a stand-off attack up to the Design Basis Threat.

2. Any Vital Area that is outside of the Protected Area shall have Physical Protection Measures that are equivalent or higher than Physical Protection Measures of the Protected Area and Vital Area collectively.

Central Alarm Station

Article (18)

The Licensee shall establish, implement and maintain a Central Alarm Station to be located inside the Protected Area. As a minimum, the Central Alarm Station shall be:

a) continuously manned (minimum staffing shall be provided in accordance with the Physical Protection Plan) for monitoring and assessment of alarms, initiation of response and communication with the Guards, Security Response Forces and facility management without any operational activities that would interfere with the execution of the alarm response function;

b) protected against any Malicious Act that can impede its functions;

c) secured with minimised access and control thereof; and

d) backed up by a Secondary Alarm Station with functionally equivalent capabilities of the Central Alarm Station so that no single act foreseen in the Design Basis Threat could simultaneously disable the key functions of both the Central Alarm Station and the Secondary Alarm Station.

Maintenance, Calibration and Testing

Article (19)

The Licensee shall establish, maintain and implement a maintenance, testing and calibration programme to ensure that the Physical Protection System and equipment are tested for operability and performance at pre-determined intervals, maintained in operable condition, and are capable of performing their intended functions.

Compensatory Measures

Article (20)

1. The Licensee shall identify the criteria and measures to compensate for a degraded or inoperable Physical Protection System. These compensatory measures shall provide a level of protection equivalent to the protection that was provided by the degraded or inoperable Physical Protection System.

2. The Licensee shall implement compensatory measures within the time frames necessary to meet the conditions described in the Physical Protection Plan.

3. The Licensee shall define the acceptable duration for the implemented compensatory measures. If the acceptable duration for the implemented compensatory measures is exceeded, it shall be reported to the Authority as a Nuclear Security Event.

Vulnerability Assessment

Article (21)

1. The Licensee shall prepare and submit to the Authority a Vulnerability Assessment.

2. The Vulnerability Assessment shall ensure the effectiveness of the Physical Protection System associated with the defined response actions to the Design Basis Threat.

Suspension of Physical Protection Measures

Article (22)

1. The Licensee may suspend the implementation of the Physical Protection Measures and associated procedures in an Emergency when:

a) a suspension is immediately needed to protect the health and Safety of members of the public or of the personnel at the Nuclear Facility; and

b) no action consistent with Licence conditions and technical specifications, which can provide adequate or equivalent protection of the health and Safety of members of the public or of the personnel at the Nuclear Facility, is immediately apparent.

2. In the case of a declared Emergency, the authority of the Licensee's operation shift manager shall supersede the authority of the Licensee's head of security operation.

3. In case the decisions taken by the Licensee's operation shift manager affect the implementation of the Physical Protection Measures resulting in their suspension, the responsibility for such decisions shall remain with the Licensee's operation shift manager.

4. In the event that the decision to suspend Physical Protection Measures is made, the Licensee's head of security operation shall discuss the implementation of appropriate Physical Protection Measures with the operation shift manager.

Nuclear Security Events: Notification, Reporting and Recording

Article (23)

1. The Licensee shall notify the Authority within four (4) hours, followed by a written report within sixty (60) days, of the discovery of any of the following Nuclear Security Events:

   a) those in which there is reason to believe that an individual has committed or caused, or attempted to commit or cause, or has made a credible threat to commit or cause:

      i. an Unauthorised Removal,

      ii. significant physical damage to a Nuclear Facility or to the Nuclear Fuel or Spent Nuclear Fuel; or

      iii. interruption of normal Operation of a Nuclear Facility through a cyber attack or unauthorised use of or tampering with its machinery, components, or controls, including the Physical Protection System.

   b) any cyber attack that adversely impacted or could have adversely impacted the Safety, security, safeguards and Emergency Preparedness functions of a Nuclear Facility, or that compromised or could have compromised these functions including Safety-related and important-to-safety functions, security functions, safeguards functions, and Emergency Preparedness functions (including off-site communications);

   c) the actual entry of an individual without the required authorisation into the Owner Controlled Area, Protected Area or Vital Area;

d) any failure, degradation, or discovered vulnerability in a Physical Protection System that could allow unauthorised or undetected access to the Owner Controlled Area, Protected Area or Vital Area; and

e) the actual or attempted introduction of Contraband into the Owner Controlled Area, Protected Area or Vital Area.

2. The Licensee shall record a Nuclear Security Event in the security log within twenty-four (24) hours of the discovery of the Nuclear Security Event.

3. In case of the discovery of a Nuclear Security Event, or a declared Emergency class, the Licensee shall maintain an open and continuous secured communication channel with the Authority's Emergency Operations Centre.

Cyber Security Plan

Article (24)

1. An applicant for a Licence shall develop and the Licensee shall maintain a Cyber Security Plan that shall include a description of the following:

a) governance and implementation procedures for the Detection of, protection from and response to cyber attacks;

b) cyber risk management, assessment of cyber risks prior to and after modifications to a Nuclear Facility;

c) personnel awareness and training for all employees of the Licensee, vendors, and service providers;

d) critical digital assets identification for Nuclear Safety, Nuclear Security, safeguards and Emergency Preparedness functions, as well as the relevant operational and technical controls;

e) Defence-in-depth strategy;

f) response to and recovery from Cyber Security incidents; and

g) measures to ensure the continuity of the safe Operation of the Nuclear Facility and the implementation of Physical Protection, safeguards and Emergency Preparedness functions during and following a cyber attack.

2. The Licensee shall develop and maintain a Cyber Security programme to implement the Cyber Security Plan for the purpose of protecting digital computer systems, communications systems, networks and data from cyber attacks aiming to:

a) gain unauthorised access to Sensitive Nuclear Information;

b) alter the parameters or data of systems;

c) operate or deny access to the equipment or functions of the Nuclear Facility; or

d) defeat components of the Physical Protection Plan or Physical Protection System.

Effectiveness of the Physical Protection Plan

Article (25)

1. For each unit in Construction, the Licensee shall conduct exercises using scenarios up to and including the Design Basis Threat situations at least one (1) month prior to the first loading of Nuclear Fuel.

2. For units in Operation at the same Nuclear Facility, the Licensee shall conduct an exercise every two (2) years.

3. The results of the exercises shall be evaluated and used to demonstrate and improve the effectiveness of the Physical Protection Plan in the protection of Nuclear Material and the Nuclear Facility.

Physical Protection of Nuclear Material

On-site of a Nuclear Facility

Article (26)

1. The Licensee shall ensure that any missing or stolen Nuclear Material is detected in a timely manner by means such as the system for Nuclear Material accountancy and control and the Physical Protection System (e.g. periodic inventories, inspections, access control searches, radiation detection screening).

2. The Licensee shall notify the Authority and other relevant Competent Authorities of missing or stolen Nuclear Material in accordance with the procedures specified in the Physical Protection Plan.

3. A Contingency Plan of the Licensee shall specify arrangements to locate and recover missing or stolen Nuclear Material on-site and/or off-site of a Nuclear Facility. The Licensee shall ensure the regular testing and evaluation of such arrangements through appropriate joint exercises with the Competent Authorities.

4. The Licensee shall ensure prompt implementation of the Contingency Plan as soon as Nuclear Material on-site and/or off-site of a Nuclear Facility is declared by the Licensee as missing or stolen.

5. The Licensee shall provide the necessary assistance to the relevant Competent Authorities to locate and recover any missing or stolen Nuclear Material and shall cooperate with the Competent Authorities during any subsequent investigations.

Transport of Nuclear Material

Article (27)

1. The applicant for a Licence for Transport of category I, II or III Nuclear Material shall develop a Transport security plan to address the protection against Unauthorised Removal of category I, II or III Nuclear Material and, where relevant, Radiological Sabotage during Transport and shall obtain the Authority's approval thereof prior to the conduct of the Transport.

2. The Licensee shall notify the Authority in writing at least three (3) working days before the proposed arrival date and time of the shipment of Nuclear Material. The Licensee shall receive confirmation of receipt of the notification from the Authority before such shipment takes place.

3. The Licensee shall provide the Authority with a written report on the results of the implemented Transport security plan for each shipment of Nuclear Material to the Nuclear Facility within thirty (30) days after the said shipment is completed. This report shall include, inter alia, a description of any deficiencies in the Physical Protection System noted by the Licensee during the shipment.

4. The Licensee shall inform the Authority of any intended change to the Transport security plan and provide an explanation and justification for the change for review and approval thereof by the Authority prior to implementing the change in the Transport security plan.

5. The Licensee shall ensure that the following basic elements are included in the Transport security plan:

    a) Description of the administrative arrangements, including allocation of responsibilities and operational procedures such as testing and evaluation of the Transport security plan, review and update of the Transport security plan and event reporting, training requirements and information protection;

    b) Description of the transported Nuclear Material;

    c) The Transport Physical Protection System, including description of the packages and conveyances to be used, planned and alternate routes and modes of Transport, Physical Protection Measures, communication and positional tracking for normal operations, command and control for operations, maintenance and testing of systems and equipment and pre-shipment checks, as applicable; and

d) Description of the response planning, including Emergency arrangements, Contingency Plan, and escort of Transport by Security Response Forces, as applicable.

6. On-site movements of Nuclear Material between two Protected Areas within a Nuclear Facility should be conducted in compliance with the requirements applicable to Nuclear Material during Transport after taking into account existing Physical Protection Measures at the Nuclear Facility.

7. The Licensee shall provide the necessary assistance to the relevant Competent Authorities to locate and recover any missing or stolen category I, II or III Nuclear Material and shall cooperate during subsequent investigations.

Nuclear Facility that Does Not Contain a Nuclear Reactor

Article (28)

1. An applicant for a Licence for the Construction of a Nuclear Facility that does not contain a Nuclear Reactor shall develop and submit to the Authority a Physical Protection Plan for approval as part of an application for the Licence for the Construction of the Nuclear Facility that does not contain a Nuclear Reactor.

2. An applicant for a Licence for the Operation of a Nuclear Facility that does not contain a Nuclear Reactor shall develop and submit to the Authority a Physical Protection Plan for approval as part of an application for the Licence for the Operation of the Nuclear Facility that does not contain a Nuclear Reactor.

3. As a minimum, the Physical Protection Plan referred to in Article 28(2) above, shall include a description of the following:

    a) the physical barriers pertinent to an Owner Controlled Area;

    b) the limited and controlled access to the Owner Controlled Area for individuals and vehicles;

    c) a Detection, surveillance and alarm system for unauthorised access or Unauthorised Removal and/or Radiological Sabotage by an external adversary within the Owner Controlled Area;

    d) an integrated and effective Physical Protection System against Unauthorised Removal and/or Radiological Sabotage;

    e) the minimum number and responsibilities of Guards for monitoring, assessing and controlling access and providing initial response to actual or attempted Unauthorised Removal and/or Radiological Sabotage; and

f) the arrangements between the Licensee's security organisation, Competent Authorities and Security Response Forces to respond to an actual or attempted Unauthorised Removal and/or Radiological Sabotage.

4. The Licensee holding a Licence for Operation shall implement the approved Physical Protection Plan one (1) month before the arrival of the first Nuclear Material on the site.

5. The Licensee shall review the approved Physical Protection Plan at least every twenty-four (24) months to ensure its alignment with the current operating conditions and the Physical Protection System.

6. The Licensee shall ensure that Nuclear Material is used or stored within the Owner Controlled Area.

7. The Licensee shall establish, implement and maintain the Owner Controlled Area.

8. The Licensee shall establish, maintain and implement a maintenance, testing and calibration programme to ensure that the Physical Protection System and equipment are tested for operability and performance at pre-determined intervals, maintained in operable condition and are capable of performing their intended functions.

9. The Licensee shall establish and implement a trustworthiness programme for all personnel granted access to the Owner Controlled Area.

10. The Licensee shall prepare, implement and maintain a system of written procedures for the conduct of the activities described in the Physical Protection Plan.

11. The Licensee shall assess and manage the Physical Protection interface with Safety and Nuclear Material accountancy and control activities in a manner that ensures that they do not adversely affect each other and that they are mutually supportive to the extent possible.

12. The Licensee shall ensure that Cyber Security measures for computer-based systems used for Physical Protection and Nuclear Material accountancy and control are established and maintained to protect them against Malicious Acts.

13. The Licensee shall ensure that the personnel adheres to the Licensee's procedures for the handling of Nuclear Material.

14. The Licensee shall confirm any missing or stolen Nuclear Material by means of a rapid emergency inventory as soon as possible within the time period specified in the Physical Protection Plan. The system for Nuclear Material accountancy and control shall provide accurate information about the potentially missing Nuclear Material in the Nuclear Facility that does not contain a Nuclear Reactor following a Nuclear Security Event.

15. The Licensee shall notify the Authority within four (4) hours, followed by a written report within sixty (60) days, of the discovery of any Nuclear Security Event in which there is reason to believe that an individual has committed or caused, or attempted to commit or

cause, or has made a credible threat to commit or cause an Unauthorised Removal or Radiological Sabotage.

16. The Licensee shall record as a Nuclear Security Event any failure, degradation, or discovered vulnerability in the Physical Protection System that could have resulted in Unauthorised Removal or Radiological Sabotage or undetected access to an Owner Controlled Area. Such Nuclear Security Event shall be recorded by the Licensee in the security log within twenty-four (24) hours of the discovery of the Nuclear Security Event.

Advanced Nuclear Technologies

Article (29)

1. A Person planning to develop and/or deploy Advanced Nuclear Technologies (ANTs) in the State, and in the process of planning and developing requirements for the procurement of the ANT, such as procedures and arrangements for the qualification, selection and evaluation of the ANT, shall:

   a) consider Physical Protection measures, including but not limited to the following:

      1) security-by-Design features:

         i. integration of security, safety and safeguards,

         ii. any specific Structures, Systems or Components that are self-protected, and

         iii. any other system that supplements the Physical Protection System.

      2) specific Physical Protection Measures for the unique characteristics of the Design of the ANT taking into consideration Defence-in-depth methodology;

      3) alternate Physical Protection Measures and/or Cyber Security measures that are reduced or degraded due to the Design of the ANT;

      4) a Contingency Plan compatible with the Design and deployment of the ANT;

      5) measures for protection of information from any theft, loss, compromise or unauthorised access, which ensure the confidentiality, availability and integrity of data-at-rest and in-motion based on information classification;

      6) an insider mitigation programme including fitness-for-duty for the employees who directly or indirectly may have the ability to impact the safe and secure operation of the ANT.

   b) consider Cyber Security measures, including but not limited to the following:

      1) secure Design of the ANT for the development of its digital systems and communication networks;

2) unique characteristics of the Design of the ANT, taking into consideration Defence-in-depth methodology including appropriate quality assurance, testing and supply chain control;

3) segregation and protection between interfacing networks and systems, both internally and externally, to defend the digital systems and communication networks of the ANT against any Malicious Act;

c) submit to the Authority the information and documentation referred to in Article 29.1.a and Article 29.1.b of this regulation, the Design of the ANT, and any other relevant information and documentation required by the Authority to seek additional guidance from the Authority in relation to Physical Protection measures and Cyber Security measures and for the Authority to determine whether a Licence is required and to develop licensing requirements.

2. In case a Licence is required, as referred to in Article 29.1.c of this regulation, the requirements of this regulation shall apply in a graded manner that will be determined by the Authority on a case-by-case basis specifying, among others, requirements for a Physical Protection Plan, including a Cyber Security Plan, which shall be submitted to the Authority as part of a Licence application.

Entry into Force

Article (30)

This regulation shall be published in the Official Gazette and shall enter into force six (6) months following the date of its publication.

Annex 1

Categorisation of Nuclear Material

Material	Form	Category I	Category II	Category III[c]
1. Plutonium [a]	Unirradiated[b]	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 (U^{235})	Unirradiated[b]			
	– uranium enriched to 20% U^{235} or more	5 kg or more	Less than 5 kg but more than 1 kg	1 kg or less but more than 15 g
	– uranium enriched to 10% U^{235} but less than 20% U^{235}		10 kg or more	Less than 10 kg but more than 1 kg
	– uranium enriched above natural, but less than 10% U^{235}			10 kg or more
3. Uranium-233 (U^{233})	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 Nuclear Fuel			Depleted or natural uranium, thorium or low-enriched Nuclear Fuel (less than 10% fissile content)[d]	

[a] All plutonium except that with isotopic concentration exceeding 80% in plutonium-238.
[b] Nuclear Material not irradiated in a Nuclear Reactor or Nuclear Material irradiated in a Nuclear Reactor but with a radiation level equal to or less than 1 Gy/hr at one metre unshielded.
[c] Quantities not falling in category III and natural uranium, depleted uranium and thorium should be protected in accordance with prudent management practice.
[d] Other Nuclear 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 Nuclear Fuel exceeds 1 Gy/hr at one metre unshielded.