
DRAFT REGULATION

Regulation on the Physical Protection of Nuclear Material and Nuclear Facilities

(FANR-REG-08)

Version 2

2023

Federal Authority for Nuclear Regulation (FANR)

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

regulation@fanr.gov.ae

Table of Contents

Preamble.....	5
Definitions.....	5
Article (1).....	5
Objective.....	8
Article (2).....	8
Scope.....	8
Article (3).....	8
General Requirements.....	9
Article (4).....	9
Records and Written Procedures	9
Article (5).....	9
Protection of Sensitive Nuclear Information.....	10
Article (6).....	10
Management System Requirements	10
Article (7).....	10
Specific Requirements for a Nuclear Facility Site.....	10
Article (8).....	10
Specific Requirements for Construction of a Nuclear Facility	11
Article (9).....	11
General Requirements for Physical Protection Plan for Operation of a Nuclear Facility	11
Article (10).....	11
Monitoring, Control and Response Measures.....	12
Article (11).....	12
Safety and Security Interface.....	13
Article (12).....	13
Protection against Potential Insider Threats	13
Article (13).....	13

Target Sets Analysis	14
Article (14).....	14
Physical Protection System	14
Article (15).....	14
Physical Barriers	14
Article (16).....	14
Owner Controlled Area	14
Article (17).....	14
Protected Area	15
Article (18).....	15
Vital Area	15
Article (19).....	15
Central Alarm Station.....	16
Article (20).....	16
Maintenance, Calibration and Testing.....	16
Article (21).....	16
Compensatory Measures	16
Article (22).....	16
Vulnerability Assessment.....	17
Article (23).....	17
Contingency Plan.....	17
Article (24).....	17
Suspension of Physical Protection Measures	17
Article (25).....	17
Nuclear Security Events notification, reporting and recording.....	18
Article (26).....	18
Cyber Security	19
Article (27).....	19
Effectiveness of the Physical Protection Plan	19
Article (28).....	19
Article (29).....	20

Specific Requirements for Transport of Nuclear Material.....	20
Article (30).....	20
Requirements for Specific Nuclear Facilities	21
Article (31).....	21
Entry into Force	23
Article (32).....	23
Annex 1	24
Categorization of Nuclear Material.....	24

Preamble

This regulation is issued by the Federal Authority for Nuclear Regulation (the Authority) 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 used in this regulation shall have the meaning ascribed to them in Article 1 of the Law, unless context requires otherwise: the Authority, Design, Emergency, Emergency Preparedness, Licence, Licensee, Management System, Nuclear Facility, Nuclear Fuel, Nuclear Security, Operation, Physical Protection, Radioactive Material, Safety, Spent Nuclear Fuel and State.
2. In addition, the following terms shall have the meaning set forth below:

Central Alarm Station	An installation, which 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 measure in the State and in its subdivisions.
Contingency Plan	Predefined sets of actions for response to unauthorized acts indicative of attempted Malicious Acts, including threats thereof, designed to effectively counter such acts.
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 of a Nuclear Facility. These functions include Safety-related and important-to-safety functions, security functions, and Emergency Preparedness functions (including off-site communications).
Cyber Security Plan	A plan that describes Cyber Security and includes the following elements: Cyber Security assessment team, critical digital assets identification for Safety, security, safeguards and Emergency Preparedness functions, Defence-in-depth

strategy, management control, control of Operation and technical control.

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 potential Insider and/or external adversaries, who might attempt Malicious Act, against which a Physical Protection System is designed and evaluated.
Guards	Persons who are entrusted by the Licensee with responsibility for patrolling, monitoring, assessing, 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 authorized access to Nuclear Facilities or Nuclear Material in Transport who could attempt a Malicious Act, or who could aid an external adversary to do so.
Intrusion Detection System	A system that gathers and analyzes 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 Unauthorized 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 to this regulation.
Nuclear Security Culture	The assembly of characteristics, attitudes and behaviours of individuals, organisations and institutions, which serve as a mean 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, which provides for 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 Unauthorized 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 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 as to perform specific active function and a Component is a discrete element of a system.
Target Set	The minimum combination of equipment or operator actions, 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 release of Radioactive Material.

Transport

International or domestic multiple shipments of Nuclear Material by any means of transportation, where each shipment begins with the departure from a Nuclear Facility of the shipper and ends with the arrival at a Nuclear Facility of the receiver.

Unauthorized 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, the Radiological Sabotage of which could directly or indirectly would result in release of Radioactive Material.

Vulnerability Assessment

A process for evaluation and documentation the features and effectiveness of the overall Physical Protection System.

Objective

Article (2)

The objective of this regulation is to provide the requirements for the Physical Protection of a Nuclear Facility and of category I, II or III Nuclear Material, as categorized in Annex 1, during Transport in order to detect, delay and respond to a Malicious Act.

Scope

Article (3)

1. This regulation applies to:
 - a) an applicant and holder of a Licence for Construction of a Nuclear Facility;
 - b) an applicant and holder of a Licence for Operation of a Nuclear Facility;
 - c) an applicant and holder of a Licence for Transport of category I, II or III Nuclear Material undertaking Transport of category I, II or III Nuclear Material within the State.
2. This regulation applies to a Nuclear Facility of a lower Nuclear Security risk, as determined by the Authority ("specific Nuclear Facility") and referred to in Article 31 of this regulation.

General Requirements

Article (4)

The applicant for a Licence shall develop and the Licensee shall implement and maintain a Physical Protection Plan and/or a transport security plan, as applicable, to prevent, detect, delay and respond to Malicious Acts.

Records and Written Procedures

Article (5)

1. The Licensee shall maintain records as required in the Physical Protection Plan and/or the transport security plan in either hard copy 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, records 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 with the time of entry into and exit from a Vital Area,
 - d) The names of individuals in possession of keys, key-cards and/or having any authorised access to systems including computer systems that control access to category I, II or III of Nuclear Material, Protected Area or Vital Areas,
 - e) The name and time of each entry into and exit from the Protected Area who are of each individual granted escorted access,
 - f) Documentation of each routine security tour and inspection,
 - g) Record of tests and maintenance of security-related equipment carried out in Article 21 of this regulation,
 - h) Record of each on-site security alarm and details of the response,
 - i) Records detailing the shipments of category I, II or III Nuclear Material,
 - j) Security-related procedures.
3. 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 transport security plan.

Protection of Sensitive Nuclear Information

Article (6)

1. The Licensee shall take appropriate measures consistent with the requirements of the Information Protection Programme Operating Manual (IPPOM) to protect Sensitive Nuclear Information.
2. The Licensee shall establish and maintain a list of the individuals who are authorised to access Sensitive Nuclear 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 was denied and a list of the individuals whose access to Sensitive Nuclear Information was cancelled.
3. The Licensee shall report to the Authority within twenty four (24) hours of discovery of the loss, compromise, unauthorized receipt or suspected compromise of Sensitive Nuclear Information.

Management System Requirements

Article (7)

1. The Licensee's Management System shall cover 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 a strong Nuclear Security Culture.

Specific Requirements for a Nuclear Facility Site

Article (8)

1. The selection and/ or preparation of a site for the Construction of a Nuclear Facility shall take into account the Physical Protection as early as possible and 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 do not come into the proximity of the site of the Nuclear Facility through the use of public roads and other public areas.
3. The impact of topographical features and terrain line 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.

Specific Requirements for Construction of a Nuclear Facility

Article (9)

1. On a site hosting multiple units, where the activities at different units of a Nuclear Facility can vary from an initial site preparation through different phases of their Construction up to and including Operation, 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 individuals crossing 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. The applicant for a Licence for the Construction of a Nuclear Facility shall develop the Physical Protection Plan and obtain the approval by the Authority thereof at least one (1) month before the departure of the first shipment of Nuclear Fuel on the site of the Nuclear Facility. As a minimum, the Physical Protection Plan shall include the description of:
 - a) The physical barrier around the Nuclear Fuel with a detection system,
 - b) The control of access to the area referred to in Article 9.2.a of this regulation, and
 - c) The response actions against Nuclear Security Events.
3. The applicant for a Licence for Construction of a Nuclear Facility shall develop and the Licensee shall implement and maintain a fitness for duty programme for individuals who are Constructing or directing the Construction of Structures, Systems and Components or Physical Protection System and measures on the site of the Nuclear Facility. This program shall deter substance abuse and detect indications of:
 - a) Possible use, sale, or possession of illegal drugs;
 - 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.

General Requirements for Physical Protection Plan for Operation of a Nuclear Facility

Article (10)

1. The 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 organization, 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 in the State and shall review the Physical Protection Plan at least every twenty-four (24) months.
4. The Licensee shall inform the Authority about any intended change to the Physical Protection Plan and provide an explanation and justification for the change for review and approval by the Authority prior to implementing the change in the Physical Protection Plan. Should the intended change to the Physical Protection Plan be determined by the Licensee as such that does not reduce the overall effectiveness of the latter, the Licensee shall inform the Authority of the implementation of the change within ninety (90) days from the date of the change.

Monitoring, Control and Response Measures

Article (11)

1. The Licensee shall establish and maintain the twenty-four (24) hours on duty Guards for day-to-day activities in the 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 Security Response Forces response 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. A dedicated and secured voice communication shall be provided between the Guards, Security Response Forces and the Central Alarm Station.

Safety and Security Interface

Article (12)

1. The Licensee shall assess and manage the Physical Protection interface with Safety and control activities in a manner to ensure 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 is thoroughly evaluated to verify that it does not result in significant implications for Safety or does not jeopardize Physical Protection.

Protection against Potential Insider Threats

Article (13)

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 Malicious Act.
3. The following elements shall support the Insider mitigation programme:
 - a) an access authorisation programme,
 - b) a fitness-for-duty programme, including drug and alcohol test, to be performed when an individual is granted a first access to the Protected Area and when an individual is involved in an any event. Moreover, the Licensee shall conduct random drug and alcohol tests on individuals granted access to the Protected Area,
 - c) the Cyber Security Plan, and
 - d) the Physical Protection System.

Target Sets Analysis

Article (14)

1. The Licensee shall identify the Target Sets, the Radiological Sabotage of which could directly or indirectly result in 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 design control process to ensure that changes to Target Sets are evaluated for potential adverse impacts on the Physical Protection Plan.

Physical Protection System

Article (15)

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

Physical Barriers

Article (16)

1. The Licensee shall develop, implement and maintain a Defence-in-depth approach for protecting a Nuclear Facility against the Unauthorized 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 Area.
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 tamper-protected against unauthorized monitoring, manipulation and falsification.

Owner Controlled Area

Article (17)

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,
- b) A limited and controlled access for individuals and vehicles,

- c) A detection, surveillance and alarm system.

Protected Area

Article (18)

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

- a) A physical barrier with limited access points and with features against unauthorized 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 any obstruction,
- c) An illumination of the isolation zone and of all the exterior areas within the Protected Area sufficient and not less than 0.2 foot-candle measured horizontally at the ground level,
- d) A limited and controlled access for individuals and vehicles with a comprehensive continuous search for prohibited items at the entrance to and exit from the Protected Area for 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 (19)

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 the 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.

Central Alarm Station

Article (20)

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 so that its functions can continue in any circumstances,
- c) Secured with minimized 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 in accordance with 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 (21)

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 (22)

1. The Licensee shall identify the criteria and measures to compensate for 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 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 (23)

1. The Licensee shall prepare and submit to the Authority the Vulnerability Assessment.
2. The Vulnerability Assessment shall ensure the effectiveness of the Physical Protection System associated with the defined response actions against the Design Basis Threat.

Contingency Plan

Article (24)

1. The Licensee shall prepare and submit to the Authority a Contingency Plan.
2. The Contingency Plan shall effectively respond to attempted Malicious Acts up to and including the Design Basis Threat.

Suspension of Physical Protection Measures

Article (25)

1. The Licensee may suspend the implementation of the Physical Protection Measures and associated procedures in an Emergency when:
 - 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 operation shift manager of the Licensee shall supersede the authority of the head of security operation of the Licensee.
3. In case the decisions taken by the operation shift manager of the Licensee affect the implementation of the Physical Protection Measures resulting in their suspension, the responsibility for such decisions shall remain with the operation shift manager of the Licensee.
4. In the event that the decision to suspend Physical Protection Measures is made, the head of security operation of the Licensee shall discuss with the operation shift manager the implementation of appropriate Physical Protection Measures.

Nuclear Security Events notification, reporting and recording

Article (26)

1. The Licensee shall notify the Authority within four (4) hours, followed by a written report within sixty (60) days, of 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 Unauthorized 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 unauthorized use of or tampering with its machinery, components, or controls, including the Physical Protection System.
 - b) any other cyber-attack that adversely impacted or could have caused an adverse impact to Safety, security, safeguards functions, or Emergency Preparedness functions (including off-site communications), or that compromised or could have compromised support systems and equipment resulting in adverse impacts to Safety, security functions or Emergency Preparedness functions;
 - c) an actual entry of an unauthorized individual into the Owner Controlled Area, Protected Area or a Vital Area; and
 - d) any failure, degradation, or discovered vulnerability in a Physical Protection System that could allow unauthorized or undetected access to the Owner Controlled Area, Protected Area or a Vital Area.
 - e) an 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 discovery of a Nuclear Security Event, the Licensee shall maintain an open and continuous communication channel with the Emergency Operations Center of the Authority.

Cyber Security

Article (27)

1. The applicant for a Licence shall develop and the Licensee shall implement and maintain a Cyber Security Plan to prevent any unauthorised access to the digital computer systems, communications systems and networks for the purpose of:
 - a) Gaining unauthorised access to Sensitive Nuclear Information,
 - b) Altering systems parameters or data,
 - c) Operating or denying access to equipment or functions of the Nuclear Facility, or
 - d) Defeating components of the Physical Protection Plan or Physical Protection System.
2. The Cyber Security Plan shall include a description of implementation procedures for the prevention and mitigation of cyber-attacks, assessment of cyber risks prior to Nuclear Facility modifications, and personnel awareness training.
3. The Licensee shall develop a plan the implementation of which shall ensure continuity of safe Operation of the Nuclear Facility and of the implementation of Physical Protection, safeguards and Emergency Preparedness functions during and following a cyber-attack.

Effectiveness of the Physical Protection Plan

Article (28)

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.

Specific Requirements for Physical Protection of Nuclear Material

On-site of Nuclear Facilities

Article (29)

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 a 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 should 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.

Specific Requirements for Transport of Nuclear Material

Article (30)

1. The applicant for a Licence of Transport of category I, II or III Nuclear Material shall develop a transport security plan to address the protection against Unauthorized Removal of category I, II or III Nuclear Material and, where relevant, Radiological Sabotage during Transport and obtain the Authority's approval to be authorised by the Authority as a Licensee to carry out shipment of Nuclear Material covered by the transport security plan.
2. The Licensee shall notify the Authority in writing at least three (3) working days before the proposed date and time of the shipment of Nuclear Material, and shall receive confirmation of receipt of the notification from the Authority before such shipment takes place.
3. The Licensee shall provide to the Authority 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, description of any deficiencies in the Physical Protection System noted by the Licensee during the shipment.
4. The Licensee shall inform to the Authority about any intended change to the transport security plan and provide an explanation and justification for the change for review and

approval by the Authority prior to implementing the change in the transport security plan. Should the intended change to the transport security plan be determined by the Licensee as such that does not reduce the overall effectiveness of the latter, the Licensee shall inform the Authority of the implementation of the change within ninety (90) days from the date of the change.

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.

Requirements for Specific Nuclear Facilities

Article (31)

1. The applicant for a Licence for the Construction of a Nuclear Facility of a lower Nuclear Security risk, as determined by the Authority ("specific Nuclear Facility"), shall develop and submit to the Authority a Physical Protection Plan for approval as part of an application for the Licence to Construct such Nuclear Facility. As a minimum, the aforementioned Physical Protection Plan shall include the description of the following:
 - a) physical barriers pertinent to an Owner Controlled Area,

- b) a limited and controlled access for individual and vehicles to the Owner Controlled Area,
 - c) a detection, surveillance and alarm system of unauthorized access to or Unauthorized Removal and/or Radiological Sabotage by an external adversary within the Owner Controlled Area,
 - d) integrated and effective Physical Protection System against Unauthorized Removal and/or Radiological Sabotage;
 - e) minimum number and responsibilities of Guards for monitoring, assessing, controlling access and providing initial response against actual or attempted Unauthorized Removal and/or Radiological Sabotage;
 - f) arrangements between the Licensee's security organization, Competent Authorities and Security Response Forces to respond to an actual or attempted Unauthorized Removal and/or Radiological Sabotage;
3. The Licensee shall implement the approved Physical Protection Plan one (1) month before the arrival of the first Nuclear Material on the site.
 4. 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.
 5. The Licensee shall establish and maintain requirements of the Physical Protection Plan.
 6. The Licensee shall ensure that Nuclear Material is used or stored within an Owner Controlled Area.
 7. The Licensee shall establish, implement and maintain an 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 accessing 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 to ensure that they do not adversely affect each other and that they are mutually supportive to the extent possible.
 12. Computer based systems used for Physical Protection and Nuclear Material accountancy and control should be protected against a Malicious Act.

13. The Licensee shall ensure that the personnel adheres to the Licensee procedures for handling of the nuclear material.
14. The licensee should 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 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 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 Unauthorized 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 allowed Unauthorized 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.

Entry into Force

Article (32)

This regulation shall be published in the Official Gazette and shall enter into force one (1) month following the date of its publication.

Annex 1
 Categorization 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 15g
	– uranium enriched to 10% U ²³⁵ but less than 20% U ²³⁵		10 kg or more	Less than 10kg 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 fuel			Depleted or natural uranium, thorium or low-enriched fuel (less than 10% fissile content) ^d	

^a All plutonium except that with isotopic concentration exceeding 80% in plutonium-238.

^b Material not irradiated in a reactor or material irradiated in a 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 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/hr at one metre unshielded.