Extraordinary

Federal Republic of Nigeria
Official Gazette

No. 31 **Lagos - 22nd February, 2021** **Vol. 108**

Government Notice No. 30

The following is published as supplement to this *Gazette* :

Printed and Published by The Federal Government Printer, Lagos, Nigeria
FGP 77/022021/1,250

Annual Subscription from 1st January, 2021 is Local : ₦45.000.00 Overseas : ₦60.500.00 [Surface Mail] ₦75.000.00 [Second Class Air Mail]. Present issue ₦3.000 per copy. Subscribers who wish to obtain *Gazette* after 1st January should apply to the Federal Government Printer, Lagos for amended Subscriptions.

NUCLEAR SAFETY AND RADIATION PROTECTION ACT
(1995 No. 19)

NIGERIAN PHYSICAL PROTECTION OF NUCLEAR MATERIAL AND NUCLEAR FACILITIES REGULATIONS, 2021

ARRANGEMENT OF REGULATIONS

Regulation :

PART III—REQUIREMENTS FOR PROTECTION AGAINST UNAUTHORIZED REMOVAL OF NUCLEAR MATERIAL IN USE AND STORAGE

26. Category I nuclear material.
27. Limited access, protected, and inner areas.
28. Authorized access to protected and inner areas.
29. Detection and prevention of unauthorized access.
30. Continuous surveillance of activity in inner area.
31. Access control records.
32. Storage area.
33. Procedures for nuclear material handlers.
34. On-site movements of nuclear material.
35. Central alarm station.
36. Guards and response forces.
37. Evaluation of physical protection systems and measures.
38. Category II nuclear material.
39. Limited access and protected areas.
40. Detection and prevention of unauthorized access.
41. Authorized access to protected area.
42. Procedures for nuclear material handlers.
43. On-site movement of nuclear material between protected areas.
44. Central alarm station.
45. Guards and response forces.
46. Evaluations of physical protection measures and system.
47. Category III nuclear material.
48. Limited access area.
49. Intrusion detection and response.
50. procedure for nuclear material handlers.
51. Means and procedures for access control.
52. Movements of nuclear material within a limited access area.
53. Evaluations of physical protection measures and system.
54. Protection of nuclear material below category III.

PART IV—REQUIREMENTS FOR PROTECTION AGAINST SABOTAGE AND PROTECTION OF HIGH RADIOLOGICAL CONSEQUENCE FACILITIES

55. Sabotage scenarios.
56. Physical protection system design.
57. Vital areas and protected areas.
58. Authorized access.
59. Detection and prevention of unauthorized access to protected area.
60. Control of access to protected area.
61. Detection and prevention of access to vital area.
62. Control of access to vital areas.
63. Access control records.
64. Central alarm station.

S. I. No. 19 of 2021

NUCLEAR SAFETY AND RADIATION PROTECTION ACT (1995 No. 19)

NIGERIAN PHYSICAL PROTECTION OF NUCLEAR MATERIAL AND NUCLEAR FACILITIES REGULATIONS, 2021

[11*th Day of January*, 2021] Commencement.

In exercise of the powers conferred on it by Section 47 of the Nuclear Safety and Radiation Protection Act No. 19 of 1995 and of all other powers enabling it in that behalf, the Nigerian Nuclear Regulatory Authority, with the approval of the President, makes the following Regulations—

PART I—GENERAL PROVISION

Objectives.

1. These Regulations specify the requirement for licensees, shippers, and license applicants to provide physical protection measures and systems that—

(*a*) protect against unauthorised removal of nuclear material ;

(*b*) account for nuclear material within its possession ;

(*c*) protect nuclear material and nuclear facilities against sabotage ; and

(*d*) mitigate or minimize the radiological consequence of sabotage.

Scope.

2. These Regulations—

(*a*) apply to all nuclear facilities and nuclear material in use, storage or transport ; and

(*b*) do not apply to nuclear facilities and nuclear material in military or defence programmes.

Applicability to existing and new facilities.

3.—(1) A security plan approved by the Authority prior to entry into force of these Regulations shall continue to be effective in accordance with the terms of its applicable license, and the Authority may require further compliance with some or all of the provisions of these Regulations.

(2) A licensee having an approved security plan under an existing license applicable to the licensee shall comply with the provisions of these Regulations.

(3) Facilities that have not been licensed prior to the effective date of these Regulations shall comply with the provisions of these Regulations.

Relation to other Regulations and requirements and resolution of conflicts.

4.—(1) The provisions of these Regulations are in addition to, and not in place of, other applicable national laws and regulations and nothing in these Regulations shall be construed as relieving a licensee from complying with other applicable laws and regulations.

(2) Where a licensee identifies an apparent or actual conflict between the provisions of these Regulations and other laws or regulations, they shall notify the Authority in order to resolve the conflict.

(3) Nothing in these Regulations shall be construed as restricting any actions that may otherwise be necessary for physical protection on nuclear material or nuclear facilities.

(4) A licensee shall comply with any additional requirement imposed by the Authority, by any regulation, order or terms and conditions of a license, in addition to those established in these Regulations, as deemed appropriate or necessary for the physical protection of nuclear material or nuclear facilities.

PART II—PRINCIPAL REQUIREMENT FOR PHYSICAL PROTECTION

Licensee responsibility for physical protection.

5. A licensee shall—

(*a*) have prime responsibility for the implementation of physical protection measures for nuclear material and nuclear facilities and shall comply with all applicable requirements in these Regulations ; and

(*b*) cooperate with the Authority and all other security agencies having physical protection responsibilities.

Design basis threat.

6. In applying the physical protection requirement under these Regulations, a licensee shall design and evaluate its physical protection systems to ensure protection against any threat as defined in the Design Basis Threat (DBT) provided under these Regulations.

Safety-physical protection interface.

7. A licensee shall access and manage the physical protection interface with safety in a manner that shall ensure that they—

(*a*) do not adversely affect each other ; and

(*b*) are mutually supportive of each other.

System for nuclear material accountancy and control and its interface with physical protection.

8.—(1) A licensee shall—

(*a*) maintain control of and account for all nuclear material at all time ;

(*b*) ensure that information from the system for nuclear accountancy and control that indicates possible unauthorised removal of nuclear material are communicated as soon as possible to the facility manager responsible for physical protection ; and

(*c*) report all confirmed accounting discrepancies to the Authority in line with the provisions of the Nigerian Nuclear Safeguards Regulations.

(2) A licensee shall access and manage the physical protection interface with nuclear material accountancy and control activities in a manner that shall ensure that they—

(*a*) do not adversely affect each other ; and

(*b*) are mutually supportive of each other.

Defence-in-depth.

9.—(1) In applying the requirements of these Regulations, a licensee shall employ the principle of defence-in-depth.

(2) A licensee's measures to perform the three physical protection functions of detection, delay, and response shall each be based on defence-in-depth principle applied with a graded approach.

(3) The licensee shall take into account the capability of the physical protection system and the system for nuclear material accountancy and control to protect against insiders and external threats.

Graded approach for protection against unauthorized removal

10. A licensee shall—

(*a*) categorize their nuclear material in accordance with First Schedule to these Regulations ; and

(*b*) establish, subject to the approval of the Authority, the required levels of protection for all their nuclear material, taking into account the quantity and the characteristics of their nuclear material and its location within the nuclear facility.

Graded approach for protection against Sabotage.

11. A licensee shall—

(*a*) for each nuclear facility perform an analysis validated by the Authority to determine whether the radioactive inventory has the potential to result in consequences exceeding the lower and upper thresholds for unacceptable radiological consequences, assuming that the sabotage acts will be successfully completed while ignoring the impact of the physical protection or mitigation measures ; and

(*b*) implement measures for protection against sabotage as required in Part IV of these Regulations.

Integrated protection against unauthorized removal and sabotage.

12. A licensee shall—

(*a*) when implementing requirements for protection of nuclear material and nuclear facilities, apply the requirements for protection against unauthorized removal and sabotage ; and

(*b*) ensure that the required physical protection system is based on the more applicable requirements and implemented for both sets of requirements in an integrated manner.

New facilities.

13.—(1) License applicants for a new nuclear facility shall incorporate—

(*a*) physical protection at the design phase ; and

(*b*) interface issues with safety and nuclear material accountancy and control.

(2) License applicants shall ensure that the design of the physical protection system satisfies all applicable requirements including the effectiveness of the physical protection measures.

Performance testing.

14. A licensee shall develop and implement means and procedures for physical protections system effectiveness evaluations, including weekly performance testing to ensure that administrative and technical measures continue to function or are capable of performing their functions when required.

Maintenance and sustainability programme.

15. A licensee shall—

(*a*) develop and implement means and procedures for maintenance of physical protection systems including preventive and corrective measures ; and

(*b*) establish sustainability programme for their physical protection systems that encompass—

(*i*) operating procedures,

(*ii*) human resource management and training,

(*iii*) equipment updating, maintenance, repair, and calibration,

(*iv*) performance testing and operational monitoring, and

(*v*) configuration management.

Compensatory measures and corrective actions.

16.—(1) Where the physical protection system is determined to be incapable of providing the required level of protection, the licensee shall immediately implement compensatory measures to provide adequate protection.

(2) Where deficiencies in the physical protection system are identified by the licensee or Authority, the licensee shall within 7 working days submit a corrective action plan for review and approval by the Authority prior to implementation.

Security management.

17.—(1) A licensee shall establish a security management system which ensures that—

(*a*) policies and procedures that give security high priority are established ;

(*b*) clear lines of authority for decisions on security issues are defined ;

(*c*) responsibilities of each person for security issues are stated ; and

(*d*) each person is suitably trained and skilled in security issues.

(2) A licensee shall appoint a person in a senior management position to be responsible for all issues relating to physical protection.

(3) A licensee shall establish and implement quality assurance policies and programmes which ensure that—

(*a*) their physical protection system is designed, implemented, operated and maintained in a condition capable of effectively responding to the threat assessment or design basis threat ; and

(*b*) they meet applicable regulatory requirements.

(4) A licensee and other relevant agencies with responsibility for security shall give priority to nuclear security, its development and maintenance to ensure its effective implementation.

Security plan.

18.—(1) A license applicant shall, as part of its application to obtain a license, prepare a security plan—

(*a*) based on the design basis threat or the threat assessment ; and

(*b*) including provisions dealing with design, evaluation, implementation, and maintenance of the physical protection system, and contingency plans.

(2) The licensee shall—

(*a*) submit the security plan to the Authority for review, approval, and incorporation as part of the licence conditions ;

(*b*) review its security plan biennially, on receipt of threat statement or as DBT is reviewed to ensure it remains consistent with facility conditions and approved physical protection system ; and

(*c*) submit any amendment to the security plan for prior approval by the Authority before making significant modifications, including temporary changes, to arrangements detailed in the approved security plan.

Contingency plan.

19.—(1) A licensee shall establish and implement a contingency plan to effectively counter the threat or design basis threat, including attempted or completed unauthorized removal of nuclear material or sabotage, taking actions of the response forces into consideration.

(2) The contingency plan shall be approved by the Authority as a part of the security plan.

(3) The licensee shall in collaboration with the Authority and relevant security agencies, ensure that coordination between the guards and response forces during a nuclear security event is exercised annually or biennially depending on the categorization indicated in the First Schedule to these Regulations.

(4) The licensee shall ensure that other facility personnel are trained and prepared to act in coordination with the guards, response forces and other response teams.

(5) The licensee shall ensure that during emergency conditions and exercises, the effectiveness of the physical protection system is maintained.

(6) The licensee shall implement its contingency plan after detection of any malicious act.

(7) The Authority in collaboration with the Office of the National Security Adviser shall ensure that response forces are familiarized with the site and nuclear material locations and have adequate knowledge of radiation protection to ensure that they are fully prepared to conduct necessary response actions.

Information security.

20. A licensee shall—

(*a*) identify and protect all information where the unauthorized disclosure may compromise their physical protection systems in accordance with the requirements specified in the Second Schedule to these Regulations ; and

(*b*) limit access to sensitive information taking into account the individuals who require the information for the performance of their duties.

Electronic system security.

21.—(1) A licensee shall—

(*a*) protect electronic systems used for physical protection, nuclear safety, and nuclear material accountancy and control against compromise, consistent with the design basis threat in accordance with the Third Schedule to these Regulations ;

(*b*) provide assurance that computer, communication systems and networks are adequately protected against cyber-attacks and design basis threat ;

(*c*) protect computer, communication systems and networks associated with—

(*i*) safety-related and important-to-safety functions,

(*ii*) security functions,

(*iii*) emergency preparedness functions, including offsite communications, and

(*iv*) support systems and equipment which, if compromised, will adversely impact safety, security, or emergency preparedness functions ; and

(*d*) protect the systems and networks referred to in this sub regulations from cyber-attacks that will—

(*i*) adversely impact the integrity or confidentiality of data or software ;

(*ii*) deny access to systems, services, or data ; and

(*iii*) adversely impact the operation of systems, networks, and associated equipment.

(2) The licensee shall, in order to comply with the provisions of sub-regulations (1) of this regulation—

(*a*) analyze computer and communication systems and networks and identify assets to be protected against cyber-attacks to comply with the provisions of sub-regulations (3) and (4) of this regulation ;

(*b*) establish, implement, and maintain a cyber-security program for the protection of the identified assets ; and

(*c*) incorporate the cyber security program as a component of the physical protection program ;

(*d*) develop and maintain written policies and implementing procedures to implement the cyber security plan ;

(*e*) submit policies, implementing procedures, site-specific analysis, and other supporting technical information used by the licensee for periodic inspection by the Authority.

(3) The licensee shall establish, implement, and maintain a cyber-security plan which shall—

(*a*) describe how the requirements of this regulation will be implemented and state the site-specific conditions that affect plan implementation ;

(*b*) include measures for incident response and recovery for cyber-attacks showing how the licensee shall—

(*i*) maintain the capability for timely detection and response to cyber-attacks,

(*ii*) mitigate the consequences of cyber-attacks,

(*iii*) correct exploited vulnerabilities, and

(*iv*) restore affected systems, networks, and any equipment affected by cyber-attacks.

(4) Licensee shall ensure that the cyber security program is designed to—

(*a*) implement security controls to protect the identified assets from cyber-attacks ;

(*b*) apply and maintain defense-in-depth protective strategies to ensure the capability to detect, respond to, and recover from cyber-attacks ;

(*c*) mitigate the adverse effects of cyber-attacks ; and

(*d*) ensure that the functions of protected assets referred to in sub-regulation (5)(*a*) of this regulation are not adversely impacted due to cyber-attacks.

(5) Licensee shall as part of the cyber security program—

(*a*) ensure that appropriate facility personnel, including contractors, are aware of cyber security requirements and receive the training necessary to perform their assigned duties and responsibilities ;

(*b*) evaluate and manage cyber risks ; and

(*c*) ensure that modifications to assets, identified are evaluated before implementation to ensure that the cyber security performance objectives referred to in sub-regulation (3) of this regulation are maintained.

(6) Licensee shall review the cyber security program as a component of the physical security program including the periodicity requirements.

(7) Licensee shall retain all records and supporting technical documentation required to satisfy these requirements as a record until the Authority terminates the license for which the records were developed, and shall maintain superseded portions of these records for at least 5 years after the record is superseded, unless otherwise specified by the Authority.

Trustworthiness of personnel.

22.—(1) Licensee shall, subject to the approval of the Authority, establish and implement a programme to ensure the trustworthiness of persons for the purpose of granting authorized access to sensitive information or to nuclear material or nuclear facilities.

(2) The Licensee shall establish comprehensive human reliability program and identify critical positions covered under the programme.

Security event reporting.

23.—(1) Licensee shall immediately report the following events to the Authority—

(*a*) any failure to comply with any applicable requirement of these Regulations ;

(*b*) inability to fulfill its functions because of failure of a single component or physical protection system or general failure ;

(*c*) inability of the personnel on physical protection to fulfill their duties ;

(*d*) natural disasters, industrial accidents, fires and catastrophes ; and

(*e*) other cases related to infringement of physical protection system functioning.

(2) The Licensee shall, in the case of occurrence of any of the events referred to in sub-regulation (1) of this regulation, take prompt action to remedy the failure and within—

(*a*) 24 hours initiate the process to investigate the failure and its causes, circumstances, and consequences ; and

(*b*) 72 hours submit a report to the Authority on the causes of the failure, its circumstances and consequences, and on the corrective actions taken or to be taken in accordance with regulation 15 of these Regulations.

(3) The licensee shall report to the Authority immediately in case of actual or attempt to—

(*a*) threaten, steal, rob, or carry out other illegal activities, with the use of nuclear material or radioactive substances, including encouraging individual or entity, international organisation or State, to carry out such activity ;

(*b*) misappropriate or possess nuclear material or radioactive substances by deception ;

(*c*) blackmail to obtain nuclear material or radioactive substances, including use of force or threat ;

(*d*) sabotage or cause threat to life or personal injury to one or more individuals or material damages by the use of nuclear material or radioactive substances ; and

(*e*) carry out activities threatening the site security and safety by using an aircraft in the air protected area.

(4) The Licensee shall in case of occurrence of any of the events referred to in sub-regulation (3) of this regulation, take immediate action to remedy the situation and immediately notify the Authority and relevant security agencies in writing and within—

(*a*) 24 hours investigate the event and its causes, circumstances, and consequences ; and

(*b*) 72 hours provide the Authority with a written report on the causes of the event, its circumstances and consequences, and on the corrective actions taken or to be taken in accordance with regulation 15 of these regulation.

Measures to locate and recover missing or stolen nuclear material.

24.—(1) The licensee shall—

(*a*) ensure that the system for nuclear material accountancy and control and the physical protection system detect in a timely manner any missing or stolen nuclear material ;

(*b*) immediately determine by means of a rapid emergency inventory whether any nuclear material is missing or stolen and the licensee's system for nuclear material accountancy and control shall provide accurate information about the missing or stolen nuclear material ;

(*c*) immediately notify the Authority and other relevant security agencies of missing or stolen nuclear material ;

(*d*) take all appropriate measures to locate, as soon as possible, any declared missing or stolen nuclear material on site, or collaborate with security agencies for off-site search and recovery of the missing or stolen nuclear material ;

(*e*) secure the missing or stolen nuclear material in-situ after it has been located and identified and return it immediately to the facility or to another facility authorized by the Authority ; and

(*f*) provide any other necessary assistance to the Authority and other relevant security agencies to locate and recover nuclear material and shall cooperate during subsequent investigations and prosecution.

(2) The licensee's measures to locate and recover missing or stolen nuclear material shall be included in its contingency plan, and shall be tested and evaluated at least once every two years depending on the categorization of the nuclear material as indicated in the First Schedule to these Regulations and for this purpose, appropriate joint exercises shall be held with the Authority and other relevant organizations.

Associated measures to mitigate and minimize radiological consequences of sabotage.

25. A licensee shall—

(*a*) establish within the contingency plan, measures to prevent further damage from a sabotage event, secure the nuclear facility and protect emergency equipment and personnel ;

(*b*) ensure that the nuclear facility personnel are prepared to act in full coordination with guards, response forces, law enforcement agencies and safety response teams in implementing the contingency plans ;

(*c*) on detection of a malicious act, assess whether the act could lead to radiological consequences ; and

(*d*) notify the Authority and other relevant organizations of sabotage or attempted sabotage.

PART III—REQUIREMENTS FOR PROTECTION AGAINST UNAUTHORIZED REMOVAL OF NUCLEAR MATERIAL IN USE AND STORAGE

Category I nuclear material.

26. The provisions of regulations 27 to 37 of these Regulations shall apply in relation to protection of category I nuclear material.

Limited access, protected, and inner areas.

27.—(1) A licensee shall—

(*a*) use or store category I nuclear material within an inner area ; and

(*b*) make provision for detecting unauthorized intrusion into the limited access area and for appropriate action by guards or response forces to unauthorized attempted intrusions.

(2) The licensee shall ensure that—

(*a*) a protected area perimeter is equipped with a physical barrier, intrusion detection and assessment measures to detect unauthorized access and these protection measures are configured to provide time for assessment of the cause of alarms and an appropriate response under all operational conditions ;

(*b*) alarm generated by intrusion detection sensors is promptly and accurately assessed and appropriate action taken ;

(*c*) the number of access points into the protected and inner area are kept to the minimum necessary and every point of potential access are appropriately secured and alarmed ;

(*d*) an inner area shall—

(*i*) provide an additional layer to the protected area for detection, access control and delay against unauthorized removal,

(*ii*) be appropriately secured and alarmed when unattended,

(*iii*) provide delay against unauthorized access to allow for a timely and appropriate response to a malicious act, and

(*iv*) have delay measures designed to take account insiders' and external adversaries capability and all points intrusion ;

(*e*) vehicle barriers are installed at an appropriate distance from the inner area to prevent the penetration of an unauthorized land and waterborne vehicle specified in the design basis threat that could be used by an adversary in committing a malicious act ; and

(*f*) provide protection measures against any airborne threat.

Authorized access to protected and inner areas.

28.—(1) The licensee shall—

(*a*) establish measures under which only authorized persons have access to the protected area ;

(*b*) ensure that the number of authorized persons entering the protected and inner areas is kept to the minimum necessary ;

(*c*) ensure that persons authorized for unescorted access to the protected area are limited to persons whose trustworthiness has been determined ;

(*d*) ensure that persons whose trustworthiness have not been determined such as temporary repair, service or construction workers and visitors shall be escorted by persons authorized for unescorted access ;

(*e*) verify the identity of any authorized persons entering the protected and inner areas ; and

(*f*) issue passes or badges to person authorized to enter protected and inner areas and the passes and badges shall be visibly displayed by such authorized person inside the protected and inner area.

(2) A Licensee shall—

(*a*) keep records of all persons having access to or possession of keys, key-cards and other systems, including computer systems that control access to nuclear material ; and

(*b*) protect technical means and procedures for access control, including keys and computerized access list against manipulation, falsification or other forms of compromise.

Detection and prevention of unauthorized access.

29. A licensee shall—

(*a*) establish measures under which vehicles, persons and packages are searched on entering and leaving both protected and inner areas to detect and prevent unauthorized access, introduction of prohibited items or removal of nuclear material ;

(*b*) use instruments for the detection of nuclear material, metals, and explosives for all searches ; and

(*c*) ensure that entry of vehicles into the protected area is strictly minimized and limited to designated parking areas and that private vehicles are not allowed in the inner areas.

Continuous surveillance of activity in inner area.

30. A licensee shall ensure detection of unauthorized activity by continuous surveillance through the two-person rule or other equivalent means where an inner area is occupied to counter the insider threat.

Access control records.

31. A licensee shall maintain a record which shall be retained for a period of five years, of all persons having access to or possession of keys, key-cards and other systems, including computer systems that control access to nuclear material or to inner areas.

Storage area.

32. A licensee shall—

(*a*) store nuclear material in a hardened room, strong room or hardened enclosure inside the inner area that provides an additional layer of detection and delay against removal of nuclear material ;

(*b*) ensure that a storage area is locked and alarms activated except during authorized access to the material ; and

(*c*) where nuclear material is kept in an unoccupied work area outside this storage area, set up equivalent compensatory physical protection measures as the ones referred to under these Regulations.

Procedures for nuclear material handlers.

33.—(1) A licensee shall establish the procedure for transferring custody of nuclear material among their nuclear material handlers.

(2) The procedures established under these Regulations shall require nuclear material handlers who are reporting for duty to endeavour to ascertain that there has not been any interference with or unauthorized removal of nuclear material.

On-site movements of nuclear material.

34. A licensee shall establish modalities for movements of nuclear material between two protected areas which shall—

(*a*) comply with the requirements for transporting nuclear material ; and

(*b*) take into account existing facilities physical protection measures.

Central alarm station.

35. A licensee shall—

(*a*) establish permanent staffed central alarm station for monitoring and assessment of alarms, initiation of response, and communication with the guards and response forces in a secure manner ;

(*b*) ensure that—

(*i*) the central alarm station is located in a protected area and be protected so that it can continue in the presence of a threat, and

(*ii*) access to the central alarm station is minimized and controlled ;

(*c*) ensure that alarm equipment, alarm communication paths, and the central alarm station are provided with an uninterruptable power supply and are tamper-protected against unauthorized monitoring, manipulation and falsification;

(*d*) ensure that—

(*i*) detected, redundant, secure and diverse transmission system for two-way voice communication between the central alarm station and the response forces are provided for activities involving detection, assessment and response,

(*ii*) dedicated two-way secure voice communication is provided between guards and the central alarm station ; and

(*e*) establish provisions, including redundancy measures, to ensure that the central alarm stations functions of monitoring and assessment of alarms, initiation of response and communication can continue during an emergency.

Guards and response forces.

36. A licensee shall—

(*a*) provide a 24-hour guarding service and arrange for response forces to ensure an adequate and timely response to prevent an adversary from completing a malicious act ;

(*b*) ensure that the central alarm station personnel report at schedule intervals to the off-site response forces ;

(*c*) ensure that the guards and response forces referred to in this regulation are adequately trained and equipped for their function ; and

(*d*) ensure that guards conduct random patrols of the protected area to—

(*i*) deter an adversary,

(*ii*) deter intrusion,

(*iii*) visually inspect the physical protection components,

(*iv*) supplement the existing physical protection measures, and

(*v*) provide an initial response.

Evaluation of physical protection systems and measures

37. A licensee shall—

(*a*) conduct weekly evaluations of protection systems and measures, including—

(*i*) performance testing of the implemented physical protection measures and integrated physical protection system, and

(*ii*) timely response of the guards and response forces,

to determine their reliability and effectiveness against threat or to detect equipment malfunction as the case may be ;

(*b*) ensure that the evaluations under this regulation are carried out with the cooperation of the response forces and that significant deficiencies and actions taken to remedy them shall be reported to the Authority ; and

(*c*) at least annually, conduct performance testing of the full scope of physical protection system for Category I nuclear material through appropriate exercises, including force-on-force exercise or other equivalent exercise, to determine if the response forces can provide an effective and timely response to prevent an unauthorized removal of nuclear material.

Category II nuclear material.

38. The provisions of regulations 39 to 46 of these Regulations shall apply in relation to protection of category II nuclear material.

Limited access and protected areas.

39. A licensee shall—

(*a*) use or store category II nuclear material within a protected area located inside limited access area ;

(*b*) make provision for detecting unauthorized intrusion into the limited access area and for appropriate action by guards or response forces to unauthorized intrusion ;

(*c*) ensure that the protected area perimeter is equipped with physical barrier, intrusion detection and assessment measures to detect unauthorized access and these protection measures shall be configured to provide time for assessment of the cause of alarms and appropriate response under all operational conditions ;

(*d*) ensure that alarms generated by intrusion detection sensors are promptly and accurately assessed and appropriate action taken ; and

(*e*) ensure that the number of access points into the protected area is kept to the minimum necessary and any points of potential access are appropriately secured and alarmed.

Detection and prevention of unauthorized access.

40. A licensee shall—

(*a*) establish measures under which vehicles, persons and packages entering and leaving a protected area are searched for detection and prevention of unauthorized access, introduction of prohibited items or removal of nuclear material ; and

(*b*) ensure that entry of vehicles into a protected area is strictly minimized and limited to designated parking areas.

Authorized access to protected area.

41.—(1) A licensee shall—

(*a*) establish measures under which only authorized persons have access to the protected area ;

(*b*) ensure that—

(*i*) the number of authorized persons entering the protected area is kept to the minimum necessary for the examination of any job,

(*ii*) persons authorized for unescorted access area to the protected area are limited to persons whose trustworthiness has been determined,

(*iii*) persons whose trustworthiness have not been determined such as temporary repair, service or construction workers and visitors are escorted by persons authorized for unescorted access,

(*iv*) the identity of authorized persons entering the protected area is verified, passes or badges are issued to authorized persons and visibly displayed inside the protected area.

(2) A licensee shall—

(*a*) keep a record of all persons having access to or possession of keys, key-cards or other systems, including computer systems that control access to nuclear material ; and

(*b*) protect technical means and procedures for access control, including keys and computerized access lists against manipulation, falsification, or other forms of compromise.

Procedures for nuclear material handlers.

42. A licensee shall—

(*a*) establish the procedures to be approved by the Authority for transferring custody of category II nuclear material among their nuclear material handlers ; and

(*b*) require nuclear material handlers on reporting for duty to ascertain that there has been no interference with, or unauthorized removal of, nuclear material.

On-site movement of nuclear material between protected areas.

43. A licensee shall establish modalities for the movement of nuclear material between two protected areas which shall—

(*a*) comply with the requirements for transporting nuclear material ; and

(*b*) take into account existing facilities physical protection measures.

Central alarm station.

44. A licensee shall—

(*a*) establish a permanently staffed central alarm station for monitoring and assessment of alarms, initiation of response, and communication with the guards, response forces, and facility management ;

(*b*) ensure that—

(*i*) information acquired at the central alarm station established under this regulation is stored in a secure manner,

(*ii*) the central alarm station is located in a protected area so that its functions shall continue in the presence of a threat, and

(*iii*) access to the central alarm station is strictly minimized and controlled ;

(*c*) ensure that the alarm equipment, alarm communication paths, and the central alarm station are—

(*i*) provided with an uninterruptible power supply, and

(*ii*) tamper-protected against unauthorized monitoring, manipulation and falsification ;

(*d*) ensure that dedicated, redundant, secured and diverse transmission systems for two-way voice communication between the central alarm station and the response forces are provided for activities involving detection, assessment and response ; and

(*e*) ensure that a dedicated two-way secure voice communication is provided between guards and the central alarm station.

Guards and response forces.

45. A licensee shall—

(*a*) provide a 24-hour guarding service and arrange for response forces to ensure an adequate and timely response to prevent an adversary from completing a malicious act ;

(*b*) ensure that—

(*i*) the staff of the central alarm station established in regulation 44 of these Regulations report at scheduled intervals to the off-site response forces, and

(*ii*) the guards and response forces shall be adequately trained and equipped for their function ; and

(*c*) The licensee shall ensure that guards conduct random patrols of the protected area to—

(*i*) deter an adversary,

(*ii*) is 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 the applicable design basis threat.

(2) A licensee's response strategy shall be based on denial of adversary access to the sabotage targets or denial of adversary task completion at the sabotage targets and the—

(*a*) denial of access to the targets shall be accomplished by the primary physical protection functions of detection, delay and response ; and

(*b*) protection against stand-off attacks shall be accomplished by facility design and barrier design considerations to implement stand-off distance and other disruption measures.

(3) The licensee shall—

(*a*) evaluate the design of physical protection system for effectiveness and submit its evaluation to the Authority to verify that it complies with the required level of protection for the nuclear facility and nuclear material ;

(*b*) ensure that the evaluation referred to in this sub-regulation include performance testing of the physical protection system and of the timely response of the guards and response forces ; and

(*c*) redesign the physical protection system and re-evaluate its effectiveness if its evaluation or the Authority's review determines that the physical protection system is ineffective.

Vital areas and protected areas.

57.—(1) A Licensee shall locate nuclear material and the equipment, systems or devices which if sabotaged could lead to high radiological consequences within one or more vital areas, located inside a protected area.

(2) A licensee shall ensure that—

(*a*) a protected area is located inside a limited access area ;

(*b*) the protected area perimeter is equipped with a physical barrier, intrusion detection and assessment to detect unauthorized access ;

(*c*) the protection measures employed are configured to provide time for assessment of the cause of alarms, and provide adequate delay for an appropriate response, under all operational conditions ; and

(*d*) alarms generated by intrusion detection sensors are promptly and accurately assessed and necessary action taken.

58. A licensee shall—

(*a*) limit the number of access points into the protected area to the minimum necessary for any duty ; and

(*b*) ensure that all points of potential access are appropriately secured and alarmed.

Detection and prevention of unauthorized access to protected area.

59. A licensee shall—

(*a*) establish measures under which vehicles, persons and packages entering and leaving the protected area are searched to detect and prevent unauthorized access and introduction of prohibited items or taking out of any item without permit ; and

(*b*) ensure that entry of vehicles into the protected area is strictly minimized and limited to designated parking areas.

Control of access to protected area.

60.—(1) A licensee shall ensure that—

(*a*) only authorized persons have access to the protected area ; and

(*b*) effective access control measures are taken to ensure the detection and prevention of unauthorized access.

(2) A licensee shall ensure that—

(*a*) the number of authorized persons entering the protected area is kept to the minimum necessary ;

(*b*) persons authorized for unescorted access to the protected area are limited to those whose trustworthiness have been determined ; and

(*c*) persons whose trustworthiness have not been determined, such as temporary repair, service or construction workers and visitors, are escorted by persons authorized for unescorted access.

(3) A licensee shall—

(*a*) verify the identity of authorized persons entering the protected area ; and

(*b*) issue passes or badges to persons authorized to enter the protected area and the passes or badges shall be visibly displayed inside the protected area.

61.—(1) A licensee shall—

(*a*) implement measures for detection, access control and delay against sabotage at the vital area boundary ; and

(*b*) ensure that vital areas are secured and alarmed when unattended.

(2) A licensee shall—

Detection and prevention of access to vital area.

(*a*) design delay measures to address both the insiders and external adversaries capabilities, and shall take into account all potential points of intrusion ;

(*b*) install vehicle barriers at a standoff distance from the vital area sufficient to protect nuclear material and equipment, system and devices against unauthorized land and waterborne vehicles specified in the design basis threat ; and

(*c*) provide protective measures against any airborne threat specified in the applicable design basis threat.

(3) A licensee shall—

(*a*) ensure timely detection of unauthorized activity where persons are present in vital areas to counter insider threat ;

(*b*) examine systems or devices with vital area equipment for timely detection of tampering or interference ; and

(*c*) provide timely report to the Authority where there is reason to suspect that any malicious activity has occurred.

Control of access to vital areas.

62.—(1) A licensee shall—

(*a*) keep the number of access points to the vital areas to the minimum necessary ; and

(*b*) ensure that all points of potential access are secured and alarmed.

(2) A licensee shall ensure that—

(*a*) only authorized persons have access to the vital area ;

(*b*) effective access control measures are taken to ensure the detection and prevention of unauthorized access ;

(*c*) the number of authorized persons entering the vital area are kept to the minimum necessary to perform any duty ;

(*d*) persons authorized to access the vital area are limited to those whose trustworthiness have been determined and in exceptional circumstances and for a limited period to be determined by the licensee ;

(*e*) persons whose trustworthiness have not been determined shall be provided access only when escorted by persons authorized for unescorted access.

(3) A licensee shall ensure that private vehicles are prohibited access to vital areas.

(4) A licensee shall maintain strict access control to vital areas during a shutdown or maintenance period and also ensure that prior to facility start-up, searches and testing are conducted to detect any tampering that may have been committed during shutdown or maintenance.

Access control records.

63. A licensee shall keep record for a period of 5 years, of all persons having access to or possession of keys, key- cards and other systems, including computer systems that control access to nuclear material or to vital areas.

Central alarm station.

64. Licensee shall—

(*a*) establish a permanently staffed central alarm station where a protected area is needed, for monitoring and assessment of alarms, initiation of response, and communication with the guards, response forces, and facility management ;

(*b*) ensure that information acquired at the central alarm station is stored in a secured manner ;

(*c*) ensure that the central alarm station is located in a protected area and protected so that its functions can continue in the presence of a threat ;

(*d*) ensure that access to the central alarm station is strictly minimized and controlled ;

(*e*) make provisions for redundancy or backup alarm station to ensure that the central alarm stations key functions shall continue during an emergency ;

(*f*) provide alarm equipment, alarm communication paths, and the central alarm station with uninterruptible power supply and be tamper-protected against unauthorized monitoring, manipulation and falsification ;

(*g*) provide a dedicated, redundant, secured and diverse transmission systems for two-way voice communication between the central alarm station and the response forces for activities involving detection, assessment and response ; and

(*h*) provide a dedicated two-way secure voice communication between guards and the central alarm station.

Guards and response force.

65.—(1) A licensee shall—

(*a*) provide for a 24-hour guarding service and arrange for response forces to ensure an adequate and timely response to prevent an adversary from completing a malicious act ;

(*b*) ensure that the central alarm station personnel report at scheduled intervals to the off-site response forces ; and

(*c*) ensure that the guards and response forces are trained and adequately equipped for their function.

(2) A licensee shall ensure that the guards conduct random patrols of the protected area in order to—

(*a*) deter an adversary ;

(*b*) detect intrusion ;

(*c*) inspect visually the physical protection components ;

(*d*) supplement the existing physical protection measures ; and

(*e*) provide initial response.

(3) The Authority shall, in collaboration with the Office of National Security Adviser, ensure that the response forces—

(*a*) are familiarized with the site and sabotage targets ; and

(*b*) have adequate knowledge of radiation protection to ensure that they are prepared to conduct necessary response actions, considering their potential impact on safety.

(*b*) not use unnecessary markings on conveyances, and shall avoid the use of open channels for transmission of messages concerning shipments of nuclear material ; and

(*c*) when a security-related message is transmitted, protect such information in accordance with applicable information protection requirements.

Key control.

73. A licensee or shipper shall ensure the security of keys to conveyances and security locks, commensurate with the categorization of the nuclear material transported.

International shipments.

74. A licensee or shipper shall, before commencing international shipments, confirm that the arrangements are in accordance with the physical protection regulations of the receiving country and other countries which are transited.

Protection of category I nuclear material against unauthorized removal.

75. In addition to the general requirements under regulations 70 to 74 of these Regulations, the requirements under regulations 76 to 90 of these Regulations shall apply to category I nuclear material.

Transport security plan.

76. A licensee or shipper shall—

(*a*) prior to commencing a program of shipping Category I nuclear material, submit a transport security plan as contained in the Fourth Schedule to these Regulations for approval by the Authority ; and

(*b*) ensure that the plan include arrangements for making changes, such as alteration of the route during the shipment, in response to unexpected changes in the physical environment, threat and operating conditions.

Arrangements prior to shipment.

77. A licensee or Shipper shall ensure that—

(*a*) the carrier gives the receiver of nuclear material advance notification of the planned shipment ;

(*b*) an advance notification under this regulation shall specify the mode of transport, estimated time of arrival of the shipment and point of hand-over where the hand over is to be done before the ultimate destination ;

(*c*) an advance notification of planed shipment is supplied to the receiver within 3 days to enable the receiver to make adequate physical protection arrangements ;

(*d*) prior agreements among shipper, receiver, and carrier specify the time, place and procedures for transferring physical protection responsibilities ;

(*e*) prior to the commencement of each shipment, the receiver has confirmed that it will accept delivery and hand-over, if applicable, at the planned time and location ;

(*f*) a transport security plan is submitted to the Authority for approval not later than 7 days prior to shipment ;

(*g*) a transport security plan include the route for shipping the nuclear material, with alternative routing if necessary, stopping places, destination, hand-over arrangements, identification of persons authorized to take delivery, accident procedures, and reporting procedures of both routine and emergency nature ;

(*h*) in choosing the route, the capabilities of the response forces are taken into account ;

(*i*) prior to transportation, the carrier has put in place all measures necessary to implement the approved transport security plan ; and

(*j*) provision is made for sufficient access delay or compensating measures to counter any threat while nuclear material is on board a conveyance before departure.

78. A licensee shall— Authorization of shipment.

(*a*) seek authorization from the Authority for each shipment not later than 7 days prior to commencing transport and the issuance of the authorization shall be conditional on the receipt of safely report based on current threat assessment and intelligence gathering ;

(*b*) when directed by the Authority, conduct a detailed route surveillance to observe the current environment based on the threat assessment or intelligence available ; and

(*c*) comply with all specific limitations and conditions relating to the circumstances peculiar to the given shipment as specified by the Authority.

79. A licensee shall ensure that— Search prior to shipment.

(*a*) immediately before dispatch and after any intermodal transfer, checks are made of each nuclear material consignment to verify that the integrity of the conveyance, the package, and the locks and seals have not been compromised ; and

(*b*) the conveyance is promptly placed in a secure area or kept under guard surveillance pending its loading and shipment.

80. A licensee or shipper shall ensure that physical protection measures include surveillance of the cargo, load compartment or conveyance. Surveillance.

81. A licensee shall ensure that its physical protection measures provide sufficient delay in the conveyance, freight container and package so that guards and response forces have time to intervene to prevent removal of the material. Delay measures.

82. A licensee shall ensure that— Locks and seals.

(*a*) locks and seals are applied to conveyances, compartments and freight containers ;

(*b*) significant compensating physical protection measures above Design Basis Threat (DBT) are applied when locked or sealed packages weighing more than 2000 kg are transported in open vehicles ; and

(*c*) the package is tied down or attached to the conveyance or freight container with multiple locking mechanisms that can only be unlocked by two different keys held by two different authorized persons.

Guards.

83. A licensee or shipper shall—

(*a*) accompany each shipment with enough trained and armed security guards to withstand the DBT before and during loading and unloading operations ;

(*b*) ensure that the guards conduct surveillance of the route for any threat indicators and initiate a necessary response ; and

(*c*) ensure that continuous and effective surveillance of the packages, locked cargo hold, or compartment holding the packages are maintained by the guards at all times.

Transport control centre.

84. A licensee or shipper shall—

(*a*) use a transport control centre for the purpose of keeping track of the current position and security 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 ;

(*b*) ensure that the transport control centre is protected so that its function can continue in the presence of a threat ; and

(*c*) ensure that the transport control centre is staffed by qualified personnel whose trustworthiness has been predetermined.

Communications.

85. A licensee and shipper shall—

(*a*) maintain continuous two-way communication systems between the conveyances, transport control centre, guards accompanying the shipment, the response forces, and the shipper and receiver ;

(*b*) ensure that such systems are effective, diverse and secure ; and

(*c*)ensure that the guard or conveyance crew reports by secure two-way voice communications to the transport control centre at intervals approved in the transport security plan at each overnight stopping place, place of hand-over of the shipment and upon arrival at the final destination.

Response forces.

86.—(1) A licensee and shipper shall make arrangements for the availability of necessary response forces to deal with nuclear security events in time to prevent the unauthorized removal of nuclear material.

(2) The Authority shall, in collaboration with the Office of National Security Adviser ensure that the licensee emplace adequate measures to ensure that the response forces—

(*a*) are familiarized with typical transport operations and sabotage targets ; and

(*b*) have adequate knowledge of radiation protection to ensure that they are prepared to conduct necessary response actions.

Requirement to follow procedures.

87. A licensee and shipper shall require personnel with physical protection responsibilities for a particular shipment to follow procedures detailing their responsibilities during the transport in accordance with the transport security plan.

Information protection.

88. A licensee and shipper shall protect sensitive information relating to transport operations, including dissemination of information only to persons who need to have them for the performance of their duties.

Checks upon receipt.

89. A licensee and shipper shall ensure that the receiver—

(*a*) checks the integrity of the packages, locks and seals to verify that the security of the consignment has not been compromised and accepts the shipment and notifies the shipper immediately upon arrival ; or

(*b*) notifies the shipper of non-arrival within 1 hour after the estimated time of arrival at the destination.

Modal requirements.

90.—(1) For shipment by road, the licensee shall ensure that—

(*a*) designated conveyance used exclusively for each consignment be specially designed to resist attack and equipped with a conveyance disabling device ;

(*b*) each conveyance carries a guard or crew member in addition to the driver ;

(*c*) each conveyance is accompanied by at least one vehicle with guards to conduct a surveillance of the route for any threat indicators and to protect the nuclear material by providing an initial response to a threat ;

(*d*) 24 hours armed security guards are on duty at the stop locations, in cases where the transport cannot be done within a day ; and

(*e*) fire fighting equipment is available on board of the transport vehicle.

(2) For shipment by rail, the licensee shall ensure that—

(*a*) the consignment is transported in a freight train in an exclusive use conveyance ;

(*b*) the consignment is shipped in a fully enclosed and locked conveyance ;

(*c*) accompanying guards travel in the rail car with the shipment or in a nearby car to conduct surveillance for any threat indicators and to protect the nuclear material by providing an initial response to a threat ; and

(*d*) an access control area during extraordinary stop of the transport is established and the transport control centre is immediately notified.

(3) For shipment by water, the licensee shall ensure that the consignment is transported in a dedicated vessel in a secure compartment or container which is locked and sealed.

(4) For shipment by air, the licensee shall ensure that the consignment is transported in an aircraft designated for cargo only and for which the nuclear material is its sole cargo, in a secure compartment or container which is locked and sealed.

Protection of category II nuclear material against unauthorized removal.

91. In addition to the general requirements under regulations 70 to 74 of these Regulations the requirements under regulations 92 to 103 of these Regulations shall apply to category II nuclear material.

Arrangements prior to shipment.

92. A licensee or shipper shall—

(*a*) ensure that the carrier gives the receiver of the nuclear material advance notification of the planned shipment ;

(*b*) ensure that an advance notification specify the mode of transport, estimated time of arrival of the shipment and point of hand-over where the hand-over is to be done before the ultimate destination ;

(*c*) supply an advance notification of the planned shipment to the receiver at least 3 days prior to shipment to enable the receiver to make adequate physical protection arrangements ;

(*d*) ensure that prior agreements among shipper, receiver, and carrier specify the time, place and procedures for transferring physical protection responsibilities ;

(*e*) prior to the commencement of each shipment, ensure that the receiver has confirmed that it will accept delivery and hand-over, as applicable at the planned time and location ;

(*f*) submit a transport security plan to the Authority for approval at least 7 days prior to shipment ;

(*g*) ensure that a transport security plan include the route, with alternative routing if necessary, stopping places, destination hand-over arrangements, identification of persons authorized to take delivery, accident procedures, and reporting procedures of both routine and emergency nature ;

(*h*) in choosing the route, ensure that the capabilities of the response forces are taken into account ;

(*i*) ensure that the carrier has put into place all measures necessary to implement the approved transport security plan prior to commencing transport ; and

(*j*) make provision for sufficient access delay or compensating measures to counter any threat while nuclear material is on board a conveyance before departure.

Search prior to shipment.

93. A licensee or shipper shall ensure that—

(*a*) immediately before dispatch and after any intermodal transfer, checks are made of each nuclear material consignment to verify that the integrity of the conveyance, the package, and the locks and seals have not been compromised ; and

(*b*) immediately following completion of the search, the conveyance is placed in a secure area or kept under guard surveillance pending its loading and shipment.

Surveillance.

94. A licensee or shipper shall ensure that physical protection measures include surveillance of the cargo, load compartment or conveyance.

Delay measures.

95. A licensee or shipper shall ensure that physical protection measures provide sufficient delay in the conveyance, freight container and package so that guards and response forces have time to intervene to prevent removal of the material.

Locks and seals.

96. A licensee or shipper shall ensure that—

(*a*) locks and seals are applied to conveyances, compartments or freight containers ;

(*b*) packages containing nuclear material are carried in closed, locked conveyances, compartments or freight containers ; and

(*c*) packages weighing more than 2000kg that are locked or sealed may be transported in open vehicles if tied down or attached to the vehicle or freight container.

Guards.

97. A licensee or shipper shall ensure that armed guards accompany each shipment at all times.

Communications.

98. A licensee and shipper shall ensure that physical protection measures include a two-way voice communication system between the conveyance, any guards accompanying the shipment, the response forces and where necessary the shipper and receiver.

Response forces.

99. A licensee or shipper shall make arrangements for the availability of necessary response forces to deal with nuclear security events in time to prevent the unauthorized removal of nuclear material.

Requirement to follow procedures.

100. A licensee and shipper shall require personnel with physical protection responsibilities for a particular shipment to follow procedures detailing their responsibilities during the transport in accordance with the transport security plan.

Information protection.

101. A licensee and shipper shall protect sensitive information relating to transport operations, including dissemination of information only to persons who need to have the information for the performance of their duties.

Checks upon receipt.

102. A licensee and shipper shall—

(*a*) ensure that the receiver checks the integrity of the packages, locks and seals to verify that the security of the consignment has not been compromised and accepts the shipment and notifies the shipper immediately upon arrival ;

(*b*) confirm from the receiver the arrival of shipment within one hour after the estimated time of arrival at the destination ; and

(*c*) notify the shipper of the non-arrival of the shipment within one hour after the estimated time of arrival at the destination.

Modal requirements.

103. A licensee or shipper shall ensure that—

(*a*) for shipment by road, the consignment is shipped in a conveyance under exclusive use ;

(*b*) for shipment by rail, the consignment is shipped in a freight train in a conveyance under exclusive use and unless operationally impracticable, the consignment is shipped in a fully enclosed and locked conveyance and if not shipped in a fully enclosed and locked conveyance, the Authority shall give further approval for such conveyance ;

(*c*) for shipment by water, the consignment is shipped on a vessel in a secure compartment or container which is locked and sealed ; and

(*d*) for shipment by air, the consignment is shipped in an aircraft designated for cargo only and in a secure compartment or container which is locked and sealed.

Protection of category III nuclear material against unauthorized removal.

104. In addition to the general requirements under regulations 70 to 74 of these Regulations the requirements under regulations 105 to 110 of these Regulations shall apply to category III nuclear material.

Arrangements prior to shipment.

105. A licensees or shipper shall ensure that—

(*a*) the carrier gives the receiver of the nuclear material advance notification of the planned shipment ;

(*b*) an advance notification under this regulation shall specify the mode of transport, estimated time of arrival of the shipment and the point of hand-over where this is to be done before the ultimate destination ;

(*c*) an advance notification under this regulation is supplied at least 3 days to enable the receiver to make adequate physical protection arrangements ; and

(*d*) prior agreements among shipper, receiver and carrier specify the time, place and procedures for transferring physical protection responsibilities.

Locks and seals.

106. The licensee and shipper shall ensure that—

(*a*) packages containing nuclear material are carried in closed, locked conveyances, compartments or freight containers ;

(*b*) packages weighing more than 2000 kg that are locked or sealed may be transported in open vehicles if tied down or attached to the vehicle or freight container ; and

(*c*) locks and seals are applied to conveyances, compartments or freight containers.

Search prior to shipment.

107. A licensee and shipper shall ensure that—

(*a*) before dispatch and after any intermodal transfer, checks are made of each nuclear material consignment to verify the integrity of the package and to confirm that the locks and seals of the conveyance, compartment or freight container have not been compromised ; and

(*b*) before dispatch and after any intermodal transfer, a search of the conveyance is conducted to verify that the security of the consignment has not been compromised.

Communications.

108. A licensee and shipper shall ensure that there is a communication system in place in the conveyance to communicate with the guards, response forces and the receiver.

Checks upon receipt.

109. A licensee or receiver shall—

(*a*) check 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 shall notify the Shipper immediately upon arrival ; or

(*b*) notify the shipper of non-arrival within 2 hours after the estimated time of arrival at the destination.

Guards and response forces.

110. A licensee shall—

(*a*) make arrangements for the provision of sufficient guards and response forces to deal with nuclear security events ; and

(*b*) ensure that the physical protection measures include communication system in place within the conveyance capable of communicating with appropriate response forces.

PART VI—MISCELLANEOUS PROVISIONS

Integration of safety and physical protection.

111. A licensee and shipper shall take into account the safety features of the design for the transport package, container and conveyance when implementing required physical protection measures to protect against sabotage.

Additional measures for protection against sabotage.

112. A licensee and shipper shall identify and implement additional physical protection measures to prevent sabotage of nuclear material during transport based on design basis threat and potential radiological consequences which measures shall include—

(*a*) postponing the shipment ;

(*b*) rerouting the shipment to avoid high-threat areas ;

(*c*) enhancing the robustness of the package or the conveyance ;

(*d*) detailed route surveillance to observe the current environment ; and

(*e*) provision for additional guards.

Offences and penalties.

113.—(1) A person who contravenes any of the provisions of these Regulations commits an offence and is liable on conviction to the penalties stipulated under the Act and any other extant law or guidelines made pursuant to the Act.

(2) Notwithstanding the provisions of sub-regulation (1) of this regulation, the Authority may impose penalties such as administrative fine, suspension, revocation of authorization, Sealing of facility or any combination of these.

Appeal.

114. Any person or organisation may appeal to the Governing Board of the Authority against any decision made by the Authority pursuant to these Regulations.

Interpretation.

115. In these Regulations—

"*Act*" means the Nuclear Safety and Radiation Protection Act 19 of 1995 ;

"*Authority*" means the Nigerian Nuclear Regulatory Authority established under Section 1 of the Act ;

"*access delay*" means the element of a physical protection system designed to increase adversary penetration time for entry into or exit from the nuclear facility or transport ;

"*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 ;

"*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 and incorporated into the facility documentation ;

"*contingency plan*" means a predefined set of actions for responses to unauthorised acts indicative of attempted unauthorised removal or sabotage, including threats, designed to effectively counter such acts ;

"*conveyance*" for transport —

(*i*) by road or rail means any vehicle used for the carriage of nuclear material cargo,

(*ii*) by water means any seagoing vessel or inland waterway craft used for carriage of nuclear cargo, and

(*iii*) by air means any aircraft used for the carriage of any nuclear material cargo ;

"*defence-in-depth*" means the combination of multiple layers of systems and measures that have to be overcome or circumvented before physical protection is compromised ;

"*design basis threat*" means the attributes and characteristics of potential insider or external adversaries, who might attempt unauthorised removal of nuclear material or sabotage, against which a physical protection system is designed and evaluated ;

"*detection*" means a process in a physical protection system that begins with sensing a potentially malicious or otherwise unauthorised act that is completed with the assessment of the cause of the alarm ;

"*dose limit*" means, in relation to persons of a specified class, the limit on effective dose or equivalent dose specified in the Nigerian Basic Ionizing Radiation Regulations, 2003 in relation to a person of that class ;

"*force-on-force exercise*" means performance test of the physical protection system that uses designated personnel in the role of adversary force to simulate an attack consistent with the threat of the design basis threat ;

"*graded approach*" means the application of physical protection measures proportional to the potential consequences of a malicious act ;

"*guard*" means a person who is entrusted with responsibility for patrolling, monitoring, assessing, escorting individuals or transport, controlling access or providing initial response ;

"*high radiological consequence*" means a level of radiological consequence, above which urgent protective actions shall be initiated, numerically it is the full body radiation dose in excess of 100mSv to an individual located at any point on its boundary for two hours immediately following onset of the postulated fission product release or a total radiation dose in excess of 3Sv to the thyroid from iodine exposure ;

"*inner area*" means an area with additional protection measures inside a protected area, where category 1 nuclear material is used or stored ;

"*insider*" means one or more individuals with authorised access to nuclear facilities or nuclear material in transport who could attempt unauthorised removal or sabotage, or who could aid an external adversary to do so ;

"*licence*" means an authorization granted by the Authority on the basis of a safety assessment and accompanied by specific requirements and conditions to be complied with by a licensee ;

"*licence applicant*" means any legal person who applies to the Authority for authorization to undertake any of the actions covered by the scope of these Regulations ;

"*licensee*" means the holder of a current licence granted by the Authority for a practice or source who has recognized rights and duties for the practice or source, particularly in relation to radiation protection, safety and security ;

"*limited access area*" means designated area containing a nuclear facility and nuclear material to which access is limited and controlled for physical protection purposes ;

"*malicious acts*" means an act or attempt of unauthorised removal of nuclear material or sabotage ;

"*nuclear facility*" means facility including associated buildings and equipment in which nuclear material is produced, processed, used, handled, stored or disposed of and for which a specific license is required ;

"*nuclear emergency*" means an emergency in which there is, or is perceived to be, a hazard due to energy resulting from a nuclear chain reaction, or from decay of the products of a chain reaction, or radiation exposure, which is capable of exceeding the occupational and public dose limits ;

"*nuclear material*" means material listed in the First Schedule to these Regulations ;

"*nuclear security culture*" means the assembly of characteristics, attitudes and behaviour of individuals, organizations and institutions which serves as a sustainable means to support and enhance nuclear security ;

"*nuclear security event*" means an event that is assessed as having implications for physical protection ;

"*operator*" means any person, organization, or government entity licensed or authorised to undertake the operation of a nuclear facility ;

"*performance testing*" means testing of the physical protection system element and the total system to determine whether or not they are implemented as designed ; adequate for the proposed natural, industrial and threat environment; and in compliance with established performance requirements ;

"*person*" means any individual, corporation, partnership, firm, association, trust, estate, public or private institution, group, government agency other than the Authority; and any legal successor, representative, agent, or agency of the foregoing ;

"*physical barrier*" means a fence, wall or similar impediment which provides access delay and complements access control ;

"*physical protection measures*" means the personnel, procedures and equipment that constitute a physical protection system ;

"*physical protection regime*" means the national regime including—

(*i*) the legislative and regulatory framework governing the physical protection of nuclear material and nuclear facilities,

(*ii*) the institution and organizations within the country responsible for ensuring the implementation of the legislative and regulatory framework, and

(*iii*) Facility and transport physical protection systems ;

"*physical protection system*" means an integrated set of physical protection measures intended to prevent the completion of a malicious act ;

"*practice*" means any human activity that introduces nuclear material so as to increase the exposure or the likelihood of exposure of people or the number of people exposed ;

"*protected area*" means area inside a limited access area containing category I or II nuclear material or sabotage targets surrounded by a physical barrier with additional physical protection measures ;

"*response forces*" means persons, on-site or off-site, who are armed and appropriately equipped and trained to counter an attempted unauthorised removal of nuclear material or an act of sabotage ;

"*sabotage*" means any deliberate act directed against a nuclear facility or nuclear material in use, storage or transport or any system, structures or components important from the aspect of radiological consequence, 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 ;

"*stand-alone*" means a computer or computer system to which access is limited to individuals authorized access to safeguarded information, a stand-alone computer or computer system is one which is not physically or in any other way connected to a network accessible by users who are not authorized access to safeguarded information ;

"*security agencies or law enforcement agencies*" means those Agencies of the Federal Government of Nigeria so designated by law to handle defence and security matters, which include Nigeria Police Force, Nigeria Security and Civil Defence Corps, Nigeria Army, Nigeria Air Force, Nigeria Navy, Department of State Services, National Intelligence Agency, Nigeria Customs Service, Nigeria Immigration Service, Federal Road Safety Commission as appropriate and Office of National Security Adviser ;

"*shipper*" means any person, organization or government that prepares or offers a consignment of nuclear material for transport (i.e. the consignor) ;

"*stand-off attack*" means an attack, executed at a distance from the target facility or transport, which does not require adversary hands-on access to the target, or require the adversary to overcome the physical protection system ;

"*sustainability*" means the continuous capability of the national physical protection regime, together with the operator's physical protection system at a nuclear facility or a carrier's physical protection system during transport, of satisfying all performance and prescriptive requirements ;

"*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 ;

"*threat*" means any person or group of persons with motivation, intention and capability to commit a malicious act ;

"*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 ;

"*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 facility of the receiver ;

"*transport control centre*" means a facility which provides for the continuous monitoring of a transport conveyance location and security status and for communication with the transport conveyance, shipper or receiver, carrier, and, where appropriate, its guard and the response forces ;

"*trustworthiness and reliability*" means characteristics of an individual considered dependable in judgement, character and performance such that disclosure of safeguarded information to that individual does not constitute an unreasonable risk to public health and safety or common defence and security ;

"*two-person rule*" means a procedure that requires at least two authorised and knowledgeable persons to be present to verify that activities involving nuclear material and nuclear facilities are authorised in order to detect access or actions that are unauthorised ;

"*unacceptable radiological consequences*" means a level of radiological consequence above which the implementation of physical protection measures is warranted, numerically it is the full body radiation dose to an individual located at any point on its outer boundary following a postulated fission product release (during the entire period of its passage) exceeding 50mSv or a total radiation dose in excess of 3Sv to the thyroid from iodine exposure ;

"*unauthorised removal*" means the theft or other unlawful taking of nuclear material ; and

"*vital area*" means an area inside a protected area containing equipment, systems or devices, or nuclear material, the sabotage of which could directly or indirectly lead to high radiological consequences.

Citation.

116. These Regulations may be cited as the Nigerian Physical Protection of Nuclear Material and Nuclear Facilities Regulations, 2021.

FIRST SCHELDULE

[*Regulations* 10(*a*), 19(3), 24(2)]

TABLE : CATEGORIZATION OF NUCLEAR MATERIAL

Material	*Form*	*Category 1*	*category II*	*Category IIIc*
Plutoniuma	Unirradiated[b]	2kg or more	Less than 2kg but more than 500g	500g or less but more than 15g
Uranium-235	-Unirradiatedb - uranium enriched to 20% ^{235}U or more	5kg or more	less than 5kg but more than 1kg	1kg or less but more than 15g
	- uranium enriched to 10% ^{235}U but less than 20% ^{235}U		10kg or more	Less than 10kg but more than 1kg
	- uranium enriched above natural, but less than 10% ^{235}U			10kg or more
Uranium-233	Unirradiated[b]	2kg or more	Less than 2kg but more than 500g	500g or less but more than 15g
Irradiated Fuel			Depleted or natural uranium, thorium or low-enriched fuel/ (less than 10% fissile content)[d]	500g, or less but more than 15g

[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 (100 rad/hr) at one meter unshielded.

[c] Quantities not falling in Category III and natural uranium, depleted uranium and thorium should be protected at least 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 (100 rad/hr) at one meter unshielded.

SECOND SCHEDULE *Regulation* 20(*a*)]

INFORMATION TO BE PROTECTED UNDER THE SECURITY SYSTEM

1. The types of information and documents that shall be protected as safeguarded information include non-public security-related requirements as specified in this schedule.

2. Physical protection Information not classified as restricted data or national security information related to physical protection, including the following shall be protected—

(*a*) the composite physical security plan for the facility or site ;

(*b*) site-specific drawings, diagrams, sketches, or maps that substantially represent the final design features of the physical security system not easily discernible by members of the public ;

(*c*) alarm system layouts showing the location of intrusion detection devices, alarm assessment equipment, alarm system wiring, emergency power sources for security equipment, and duress alarms not easily discernible by members of the public ;

(*d*) physical security orders and procedures issued by the licensee for members of the security organization detailing duress codes, patrol routes and schedules, or responses to security contingency events ;

(*e*) site-specific design features of plant security communications systems ;

(*f*) lock combinations, mechanical key design, or passwords integral to the physical security system ;

(*g*) documents and other matters that contain lists or locations of certain safety-related equipment explicitly identified in the documents or other matters as vital for purposes of physical protection, as contained in security plans and contingency measures ;

(*h*) the composite facility guard qualification and training plan or measures disclosing features of the physical security system or response procedures ;

(*i*) information relating to on-site or off-site response forces, including size, armament of response forces, and arrival times of such forces committed to respond to security contingency events ;

(*j*) the adversary characteristics document and related information, including implementing guidance associated with the Design Basis Threat ; and

(*k*) engineering and safety analyses, security-related procedures or scenarios, and other information revealing site-specific details of the facility or materials if the unauthorized disclosure of such analyses, procedures, scenarios, or other information could reasonably be expected to have a significant adverse effect on the health and safety of the public or the common defence and security by significantly increasing the likelihood of theft, diversion, or sabotage of source, by-product, or special nuclear material.

3. *Physical protection in transit*

Information not classified as restricted data or national security information related to the transportation of, or delivery to a carrier for transportation of a formula quantity of strategic special nuclear material or more than 100 grams of irradiated reactor fuel, include—

(*a*) the composite transport security plan ;

(*b*) schedules and itineraries for specific shipments of source material, by-product material, high-level nuclear waste, or irradiated reactor fuel ;

(*c*) vehicle immobilization features, intrusion alarm devices, and communications systems ;

(*d*) arrangements with and capabilities of response forces, and locations of safe havens identified along the transportation route ;

(*e*) limitations of communications during transport ;

(*f*) procedures for response to security contingency events ;

(*g*) information concerning the tactics and capabilities required to defend against attempted sabotage, or theft and diversion of formula quantities of nuclear material, irradiated reactor fuel, spent fuel or related information ; and

(*h*) engineering or safety analyses, security-related procedures or scenarios and other information related to the protection of the transported material if the unauthorized disclosure of such analyses, procedures, scenarios, or other information could reasonably be expected to have a significant adverse effect on the health and safety of the public or the common defence and security by significantly increasing the likelihood of theft, diversion, or sabotage of source, by-product, or nuclear material.

4. *Inspections, audits and evaluations*

Information not classified as national security information or restricted data pertaining to safeguards and security inspections and reports, including—

(*a*) portions of inspection reports, evaluations, audits, or investigations that contain details of a licensee's or applicant's physical security system or that disclose uncorrected defects, weaknesses, or vulnerabilities in the system ;

(*b*) disclosure of corrected defects, weaknesses, or vulnerabilities which are subject to an assessment taking into account such factors as trending analyses and the impacts of disclosure on licensees having similar physical security systems ; and

(*c*) reports of investigations containing general information may be released after corrective actions have been completed, unless withheld pursuant to other authorities.

5. Portions of correspondence insofar as they contain safeguarded information as provided in this schedule.

THIRD SCHEDULE [*Regulations* 21(1*a*)]

HANDLING OF SAFEGUARDS INFORMATION

Processing of safeguarded information on electronic systems.

1.—(1) Safeguarded Information may be stored, processed and produced on a stand-alone computer or computer system.

(2) Each computer not located within an approved and lockable security storage container that is used to process safeguarded Information shall have a removable storage medium with a bootable operating system, and the bootable operating system shall be used to load and initialize the computer.

(3) The removable storage medium shall also contain the software application programs.

(4) Data may be saved on either the removable storage medium that is used to boot the operating system, or on a different removable storage medium ; the removable storage medium shall be secured in a locked security storage container when not in use.

(5) A mobile device may also be used for the processing of safeguarded information provided the device is secured in a locked security storage container when not in use and other systems may be used if approved for security by the Authority.

(6) Any electronic system that has been used for storage, processing or production of safeguarded information shall be free of recoverable safeguarded information prior to being returned to non-exclusive use.

(7) Safeguarded information designated for modified handling shall be stored, processed or produced on a computer or computer system, provided that the system is assigned to the licensee's or contractor's facility.

(8) Safeguarded information-modified Handling files shall be protected, either by a password or encryption, to prevent unauthorized individuals from gaining access word processors such as typewriters are not subject to these requirements as long as they do not transmit information offsite, where safeguarded information-modified handling is produced on a typewriter, the ribbon shall be properly marked, removed and stored in the same manner as other Safeguards Information-modified handling.

(9) Safeguarded Information-modified handling files may be transmitted over a network provided the file is encrypted, in such cases, the licensee will select an encryption system that is certified by the National Information Technology Development Agency ; safeguarded information-modified handling files may be properly labelled to indicate the presence of safeguarded information with modified handling requirements and saved to removable matter and stored in a locked file drawer or cabinet.

(10) A mobile device may also be used for the processing of safeguarded information-modified handling provided the device is secured in an appropriate locked storage container when not in use, other systems may be used where approved for security by the Authority.

(11) Any electronic system that has been used for storage, processing or production of safeguarded information shall be free of recoverable safeguarded Information designated as safeguarded information-modified handling prior to being returned to nonexclusive use.

Removal from safeguards information-modified handling category.

2. Documents or other matter originally containing safeguarded information-modified handling shall be removed from the safeguarded information category at such time as the information no longer meets the criteria contained in this Schedule, care shall be exercised to ensure that any document or other matter decontrolled shall not disclose safeguarded information in some other form or be combined with other unprotected information to disclose safeguarded information, the authority to determine that a document or other matter may be decontrolled will only be exercised by the Authority.

Destruction of matter containing Safeguarded Information designated as safeguarded information-modified handling.

3. Documents or other matter containing safeguarded information shall be destroyed when no longer needed, the information can be destroyed by burning, shredding, or any other method that precludes reconstruction by means available to the public at large ; piece sizes no wider than 6.35mm composed of several pages or documents and thoroughly mixed are considered completely destroyed.

FOURTH SCHEDULE [*Regulation* 77 (*a*)]

TRANSPORT SECURITY PLAN

1. A transport security plan (TSP) shall include all information necessary to describe the security approach and system being used for protection of the nuclear material during transport, the level of details and depth of content shall be commensurate with the category of the nuclear material covered by the plan.

2. The following shall be included in the plan referred to in this Schedule—

administrative requirements or information provided as follows—

(*a*) allocation of responsibilities shall cover—

(*i*) list of all personnel that will be involved in the shipment and their responsibilities,

(*ii*) information about the shipper, carrier or receiver, and

(*iii*) when shipment is to be changed from one party to another, the transfer of responsibilities shall be stipulated ;

(*b*) policies and operational procedures shall cover—

(*i*) vulnerability assessment,
(*ii*) testing and evaluation of the TSP,
(*iii*) review and update of the TSP,
(*iv*) response to higher threat conditions, and
(*v*) reporting of threats or incidents ;

(*c*) training requirements shall—

(*i*) provide detailed training program and exercises on physical protection that will be conducted, and

(*ii*) document the results of all trainings, exercises and lessons learnt ;

(*d*) the following information shall be retained and updated as appropriate—

(*i*) information on the nuclear material and nuclear material packages and their design,

(*ii*) information on the personnel involved in the shipment,

(*iii*) records of all nuclear material that has been transported,

(*iv*) records associated with the preparation and actual undertaking of a shipment, and

(*v*) records of personnel training and qualification ;

(*e*) confidentiality and protection of information shall be as follows—

(*i*) develop program for information security and this shall include protecting detailed information on the type, category and quantity of the nuclear material,

(*ii*) transportation schedule, route and timings,

(*iii*) physical protection arrangements and the names, number and qualifications of personnel involved in the shipment, and

(*iv*) define the precautionary measures put in place to prevent unauthorized access to any sensitive information contained in the TSP ; and

(*f*) Report of the conduct of personnel trustworthiness verification

3. Shipment Security shall provide the following information—

(*a*) Information on the nuclear material to be transported and this shall include—

(*i*) name of the nuclear material,

(*ii*) quantity of the nuclear material,

(*iii*) form of the material,

(*iv*) chemical and physical characteristics of the material,

(*v*) isotopic composition of the material,

(*vi*) enrichment values, and

(*vii*) radiation levels, and any other applicable data

(*b*) Description of the transport physical protection system such as—

(*i*) packages and conveyances,

(*ii*) description of the packages to be used, their designs pertinent to security,

(*iii*) description of physical protective measures,

(*iv*) description of the conveyances protective capabilities if any,

(*v*) planned and alternate routes and modes of transport, and

(*vi*) detailed description of the planned modes of transport and the planned primary routes to be followed and all available information on these routes ; the Information shall include description of current applicable road, rail, inland waterway, port facility, transfer and stopover facility, border crossing and airport conditions that affect the transport, and

(*vii*) information on—

(*A*) the permissible speeds,

(*B*) areas where repair or construction work is being, or is expected to be, performed,

(*C*) potential impacts of weather conditions,

(*D*) planned transfer point and stopover facility capabilities,

(*E*) refuelling sites, safe havens and subsistence locations,

(*F*) alternate routes that could be used in case of emergency,

(*G*) description of the structure of the primary and redundant alternate communications systems for the proposed transport operation,

(*H*) description of any system proposed to be used for tracking the conveyances,

(*I*) description of the command and control procedures and establishment of persons of authority for each phase of the transport operation,

(*J*) description of the command and co-ordination procedures between the response force and the guards, and between the primary response force and any secondary response forces that may be planned for deployment,

(*K*) description of the roles and responsibilities of the transport commander, the response force commander, and the transport control centre, and

(*L*) elaboration on how and when handoff of command and control would be made from the transport commander to the response force commander.

4. Maintenance and testing of systems and equipment shall provide the following—

(*a*) program for the maintenance and testing of systems and equipment ;

(*b*) program for testing all mission-related equipment (such as all transport conveyances, communications equipment and tracking systems, any delay systems built into the transport packages or conveyances; and individual guards and response force weapons and tactical equipment, protective gear and communication devices) prior to the beginning of the transport operations,

5. Response planning shall—

(*a*) provide information on emergency arrangements such as—

(*i*) planned actions and procedures to be taken in the event of an emergency situation such as a road closure, vehicle breakdown, vehicle accident, or driver illness that may occur during the shipment ;

(*ii*) backup vehicle and driver, heavy towing and lifting capability, safe havens, and alternative routes ; and

(*iii*) procedure to immediately inform any transport control centre or alternative central point of communication that is used, of any emergency situation and for that control centre or central point to be able to instigate the planned actions or procedures in response,

(*b*) contingency plans include the following—

(*i*) identify personnel who have the responsibility and authority to execute the contingency plans in case of any nuclear security event,

(*ii*) provide assurance that any transport control centre or alternative central point of communication would be notified immediately of a nuclear security event,

(*iii*) specify how the shipper or carrier will maintain and have readily available, accurate information on the availability and capability of potential local response forces close to the route chosen,

(*iv*) develop response force exercise program and conduct the emergency exercises and training and document lessons learnt, and

(*v*) identify—

(*A*) any designated guards that are to accompany the shipment,

(*B*) all designated response force units/organizations that are assigned responsibilities for the shipment,

(*C*) any other national assets that are projected to be available to support the movement or assist in response to an incident or emergency,

(*D*) all other support personnel, including fire, rescue and other asset units along the route, as applicable and the communications system required for appropriate information transfer, and

(*E*) incident communications, command and control and give description of the—

(*i*) structure of the entire primary and alternate communications system for the proposed transport operation, and

(*ii*) installed tracking system for the conveyances which shall be located at, and operated by a transport control centre or an alternative central point of communication.

MADE at Abuja this 11th day of January, 2021.

MUHAMMADU BUHARI
President of the Federal Republic of Nigeria
and Minister of Petroleum Resources