NATIONAL NUCLEAR REGULATOR

For the protection of persons, property and the environment against nuclear damage

REGULATORY GUIDE

INTERIM GUIDANCE ON THE IMPLEMENTATION OF PHYSICAL PROTECTION SYSTEMS AT NORM FACILITIES AND ASSOCIATED ACTIVITIES

RG-0010

Rev 0

NOVEMBER 2017

APPROVAL RECORD				
	Name	Designation	Signature	Date
Prepared	G. Pitsoane	Senior Nuclear Security Advisor	**Note: The original, signed document is retained by the Record Management.**	
Recommended for approval	C.O. Phillips	Senior Manager: SARA		
Approved	Dr M. B. Tyobeka	Chief Executive Officer		

The following persons contributed to the preparation of the document:

G.F.A. Pretorius

M. Skosana

P. Bester

A. Muller

TABLE OF CONTENTS

1 INTRODUCTION

The NNR exercises regulatory control over NORM facilities which have to implement physical protection systems or physical security in accordance to authorisation conditions of the Certificate of Registration. Due to varying activity levels of radioactive material or contaminated material handled, processed, transported and/or stored by authorisation holders; physical protection conditions are implemented in a graded manner commensurate to associated radiation hazard or attractiveness of material for diversion or unauthorised removal from regulatory control. Regulatory guidance is therefore provided to the holders to prevent the successful execution of a malicious act and to prevent and/or mitigate radiological consequences thereof.

Use of physical protection systems and physical security in relation to regulated NORM facilities and actions must be understood and defined interchangeably, to carry the same meaning. Authorisation holders need to manage the level of risk related to the potential consequences of an act of unauthorized removal and/or sabotage of radioactive material or geo-political implications of diverted natural uranium including required adequate measures to protect computer systems and implemented cyber security.

This document provides guidance on the regulatory requirements as contained in the draft General Nuclear Safety regulations and the draft General Nuclear Security Regulations.

The NNR strives to ensure that this Regulatory Guidance document is complete and accurate. However, in recognition of the fact that this document is being presented to authorisation holders prior to the promulgation of its associated Regulations, the NNR makes no warranty, express or implied, to the accuracy, completeness, or usefulness of any information, including warranties to the adequacy of its contents. This Regulatory Guidance document is provided as INTERIM guidance in good faith and its aim is to assist authorisation holders to achieve high levels of safety for facilities and activities that are part of the nuclear fuel cycle. The NNR assumes no legal liability or responsibility for any action taken by you due to information in this document and such actions are expressly carried out at your own risk. The information in this document is subject to change due to promulgation of its associated Regulations. Complying with applicable laws remains the responsibility of authorisation holder.

2 PURPOSE

The purpose of the document is to provide authorisation holders with interim regulatory guidance against which physical protection systems have to be put in place to prevent theft or diversion or unauthorised removal of radioactive material or natural uranium, and sabotage of facilities and associated infrastructure.

3 SCOPE

The guidance document is geared towards assuring implementation and maintenance of physical protection systems or physical security based on a graded approach for the prevention of, detection of and response to, theft, sabotage, unauthorised access or any malicious acts involving radioactive material, natural uranium and associated facilities. Authorised facilities and/or actions associated with naturally occurring radioactive material are also to ensure effective implementation of physical protection systems.

4 DEFINITIONS AND ABBREVIATIONS

4.1 Definitions

need-to-know: A determination made by a possessor of classified or controlled information that a prospective recipient, in the interest of security management, has a requirement for access to, knowledge, or possession of this information in order to perform tasks or services essential to the fulfilment of an official obligation.

physical protection systems (PPS): Systematic and procedural measures intended to prevent a security threat from completing criminal or intentional unauthorised acts involving or directed at nuclear material, other radioactive material, associated facilities, or associated activities or to detect or respond to security breaches or events. In this document, the terms PPS and PS carry the same meaning and will be used interchangeably.

security culture: The assembly of characteristics, attitudes and behaviour of individuals, organisations and institutions that serves as a means to support and enhance physical protection measures.

security event: An event that has potential or actual implications to compromise physical protection or security measures.

Vital area: 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.

4.2 Abbreviations

IAEA	International Atomic Energy Agency
NNR	National Nuclear Regulator
NORM	naturally occurring radioactive material
PPS	physical protection systems
PS	physical security

5 REGULATORY FRAMEWORK FOR PHYSICAL PROTECTION SYSTEMS AT NORM FACILITIES

5.1 Legal basis

1) The legal basis for the NNR relating to physical protection systems for NORM facilities and activities is derived from the NNR Act, specifically Sections 5 (a) and (c), 22 and 23 of the Act.

5.2 Regulatory Standards

1) The NNR has promulgated in terms of section 36 of the Act regulations on Safety Standards and Regulatory Practices that must be complied with.
2) The NNR has drafted General Nuclear Security regulations that is in the process of being promulgated.
3) This document is applicable to NORM facilities and activities and provides guidance on the physical protection systems that have to be put in place to prevent theft or diversion or unauthorised removal of nuclear or radioactive material, and sabotage of NORM facilities and activities and associated infrastructure.

5.3 Graded Approach

1) The guidance provided must be implemented in a graded approach commensurate with the radiation hazard associated with the NORM facility and activity as well as the threat assessment.

6 MANAGEMENT OF PHYSICAL PROTECTION SYSTEMS AT NORM FACILITIES

6.1 Security policy

1) A policy statement should be in place that demonstrates commitment to comply with applicable physical protection or physical security conditions and with relevant NNR requirements.

6.2 Security Plan

1) Implemented management of physical protection systems or physical security should address the following characteristics:
   a) An organisational structure identifying security responsibilities which includes provision for ensuring adequate resources for the security programme.
   b) Responsibility to designate the development of procedures, policies, records, and plans for the security programme, security culture and handling of sensitive information and protecting it against unauthorized disclosure.
   c) Implementation of the principle of defence-in-depth providing several layers of defence, including administrative controls, technological and physical controls.
   d) Vulnerability assessment conducted in accordance to nature of vital areas.
   e) Vital areas designated and/or classified in terms of technology and equipment associated with plant processes, radioactive material and utility services.
   f) Periodic threat assessment or security risk analysis should be conducted in accordance to procedures for additional measures if the threat to the facility is increased based on credible information.
   g) Changes or updates to threat assessment or security risk analysis reported to the NNR.

6.3 Vetting and Trustworthiness

1) Appointed personnel responsible for strategic activities and vital material which when out of regulatory control may result in unacceptable radiological consequences should undergo vetting and/or trustworthiness checks.
2) Only suitably assessed and verified personnel should have access to confidential information in accordance to the authorisation holder's information classification and security programme.

6.4 Security Culture

1) The security culture awareness programme should be put in place.
2) Periodic forums or information sharing should be documented and disseminated to management and staff.

6.5 Incident Reporting

1) Security incidents should be recorded and reported to the NNR as per section 5.5 of RG-0022.
2) Incidents reported to the NNR should be approved by the designated senior officer.

6.6 Record Keeping

1) Procedures should be in place for security records to be kept for at least 40 years by the facility.
2) Records of incidents including testing and maintenance should be documented on-site in accordance to approved management procedures.
3) Security records should be accessible to authorised and cleared individuals on need-to-know basis.

7 PHYSICAL PROTECTION SYSTEMS AT NORM FACILITIES

7.1 Physical Protection Measures

1) There should be administrative controls that restrict access to authorized personnel at the facility boundary and at the entry points in the respective facility.
2) Administrative controls should include procedures for identifying and controlling visitor access, delivery vehicles or designated vehicles to enter or exit the facility.

3) A defined exterior boundary for the facility should be identified.
4) Access control should be exercised through entry checkpoints.
5) Signs and postings should provide a notification that access to the controlled area is restricted to authorized personnel.
6) Barriers such as fences, gates and entry control points should be justified that they may or may not be manned.
7) All intrusion detection systems should be supported by a guard response to investigate alarm events or conditions.
8) Visual inspections of the process area to identify access by unauthorized personnel, unauthorized access to the process systems and components or other anomalous conditions should be made possible.
9) Security surveillance and assessment needed during normal operations and maintenance activities should be in accordance to critical or vital and/or non-vital areas.
10) Physical barriers that restrict access to the vital areas to authorized personnel should ensure balanced protection.
11) Tamper indicating devices to detect unauthorized access to controlled and/or vital areas should be in use.
12) Where applicable access controls should be a combination of administrative procedures, electronic personnel identification and/or camera surveillance.
13) There should be defined measures and procedures that provide for response and investigation to specific alarms or detected anomalies.

7.2 Key and Lock Control Measures

1) Keys which allow access to enclosures should be controlled and secured against unauthorised use or duplication.
2) Locks used for the protection of enclosures should be of good quality, incorporating features that offer resistance to forcible attack.
3) The implemented key and lock control measures should ensure that safety and security do not compromise each other.

7.3 Illumination Measures

1) Effective illumination should be provided to enhance visibility and reliability of assessment of activity internally and externally.

2) Adequate illumination should be provided to deter intruders, unauthorised activities and assist patrolling response personnel.

7.4 Communication Measures

1) Security personnel at all levels should be provided with effective and reliable forms of communication.
2) Communication between patrols, fixed posts and the local reporting or security control centre should be made available.
3) In the event of extra-ordinary security events or security incidents, communication to / rephrase made available.
4) Transporters or carriers should be able to communicate with the shipper and/or operator and to any response agencies.
5) Communication systems should be provided with diverse and redundant capability when required.

7.5 Materials Management and Inventory Control Measures

1) Accurate, timely, complete, and reliable information on the locations, quantities, and characteristics of the radioactive material and/or uranium in the facility's possession should be maintained.
2) Continuous implementation of measures to deter and detect unauthorized removal should be ensured.
3) In the event of unauthorized removal of uranium prompt investigation and resolution of any anomaly indicating a possible loss of radioactive material and/or uranium should be provided for.
4) Capability for detecting insider activities related to radioactive material and/or uranium should be put in place.
5) Self-assessments of the materials management and inventory control program to sustain effective performance of physical protection systems should be conducted.
6) Access to controlled material or equipment should be allowed to individuals on a need to know.

7.6 Transport Security

1) Transporters (consignors, carriers, and consignees) engaged in the transport of radioactive material or uranium should develop a transport security plan using a graded approach.
2) Responsibility for and ownership of the transport security plan should be clearly established.
3) The security plan should provide for designated responsibilities to appropriately competent individuals or entities.
4) Transport security should be accounted for on the basis of current operations and assessment of vulnerability, including intermodal transfer, storage in transit, handling and distribution as appropriate.
5) Transported material should be tracked to monitor the location of the shipment at any given time.
6) Distribution of sensitive transport information should be controlled and maintained in accordance to information security policy.

7.7 Maintenance, Modifications and Security Systems Testing

1) The performance of camera surveillance and monitors should be regularly assessed to ensure reliable and good quality display of imagery.
2) Physical protection systems including intrusion detection systems should be tested for performance upon installation and maintained at regular intervals.
3) The NNR should be informed of maintenance and systems testing on a monthly basis.
4) All modifications or changes made to physical protection systems including information security programmes should be reported to the NNR.
5) Record of maintenance and systems testing should be kept.

7.8 Protection of Computer Systems and/or Cyber Security

1) Protection of computer systems and/or cyber security should be provided to address as a minimum the following aspects:
   a) Inventory systems/records
   b) Industrial processes
   c) Instrumentation/Industrial and Control System
   d) Physical access control

e) Security monitoring
f) Defence in depth
g) Maintenance and sustainability programme
h) Developing network security architecture

8 REFERENCES

[1] Act No. 47 of 1999, National Nuclear Regulator Act
[2] Regulations in terms of section 36, of the National Nuclear Regulator Act, 1999 (Act no. 47 of 1999), on Safety Standards and Regulatory Practices (GN R388).
[3] Draft General Nuclear Security Regulations (Section 36 of NNR Act) (2015 revised edition)
[4] IAEA Implementing Guide on Nuclear Security Culture (Nuclear Security Series No. 7)
[5] IAEA Implementing Guide on Preventive and Protective Measures against Insider Threats (Nuclear Security Series No. 8)
[6] IAEA Implementing Guide on Security in the Transport of Radioactive Material (Nuclear Security Series No. 9)
[7] IAEA Nuclear Security Recommendations on Radioactive material and associated facilities (Nuclear Security Series No. 14).
[8] IAEA Nuclear Security Fundamentals on Objective and Essential Elements of a State's Nuclear Security Regime (Nuclear Security Series No. 20)