NATIONAL NUCLEAR REGULATOR

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

REGULATORY GUIDE

Guidance on Physical Protection Systems for Nuclear Facilities

RG-0006

Rev 0



UNRESTRICTED

5.19.2 Procedures should provide for when a radioactive source is unshielded, not located in a device or transport package.

5.19.3 Procedures should be in place for any radioactive source or device that has been abandoned.

5.20 Modifications and maintenance of PPS

5.20.1 A regular testing and maintenance programme should be established.

5.20.2 Before any authorised modifications and maintenance is undertaken, the holder should submit the modification and maintenance plan to the NNR.

5.20.3 Procedures should be in place for:

i. All modifications and maintenance on security measures or PPS to be authorised by senior management;
ii. Vendors providing maintenance or modifications to be authorised by recognised entity; and
iii. Maintenance or modifications on PPS and security measures to be reported to the NNR.

5.20.4 When any part of the intrusion detection systems or access control implemented for protecting special nuclear material, classified material, sensitive information and vital areas in general is out of service, complementary measures to be approved by the NNR should be put in place.

5.20.5 Preventive measures should be performed on the various subsystems and components constituting the IDS in accordance to the following factors:

i. Intrusion detection and assessment systems, and components to include tamper sensors, duress and response systems, and line supervision;
ii. Long range detection and assessment systems;
iii. Personnel and vehicle access control, entry/exit inspection equipment, and package and hand-held inspection equipment;
iv. Systems and equipment used by the security guard force for detection, assessment and communication;
v. Emergency power and auxiliary power supply;
vi. Lighting in any zone throughout the facility; and
vii. Security barriers and delay mechanisms.

5.20.6 The IDS and communication subsystems should be tested periodically to assess reliability and assurance of effectiveness and adequacy at least once every 12 months in accordance to the following factors:

i. Intrusion detection and assessment systems, and components to include tamper sensors, duress and response systems, and line supervision;
ii. Long range detection and assessment systems;
iii. Radio frequency communications;
iv. Personnel and vehicle access control, entry/exit inspection equipment, and package and hand-held inspection equipment;
v. Systems and equipment used by the security guard force for detection, assessment and communication, and communication capabilities with off-site response force;
vi. Emergency power and auxiliary power supply; and
vii. Lighting in any zone throughout the facility.

5.20.7 During testing, if there is indication of failure or degradation, repair and retesting protocol should be put in place.

5.20.8 Detection probability for the adequacy of the multiple sensor system comprising the IDS should be no less than 95%.

5.20.9 Newly installed intrusion detection systems should undergo an acceptance test, including a function test and performance test.

5.20.10 For a function test, the minimum design requirements should be in respect of the detection pattern and orientation within design limits.

5.20.11 A function test should be in conformance with the manufacturer's specification prior to acceptance of the installed system.

5.20.12 Testing should ensure that the alarm communication line or data link is capable of transmitting an alarm signal.

5.20.13 Testing should be able to isolate and indicate possible compromise of the IDS being tested.

5.20.14 Alarm system components should be tested by means of physical actuation at a frequency documented in the security plan.

5.20.15 Proper settings for high detection rates with lowest frequency or rate of nuisance alarm should be tested.

5.20.16 A performance test should be undertaken to ensure ability of the implemented PPS and associated IDS meet the regulatory requirements.

5.20.17 When conducting performance testing the following factors should be addressed:

i. Malevolent acts
ii. Pathways to the target
iii. Adversary manoeuvring and tactics
iv. Lowest lighting conditions.
v. Worst case light-to-dark ratio to determine shadows or dark spots in the field of view.
vi. Adverse weather and lighting conditions common to the local territory or environment.

5.21 Testing Criteria

5.21.1 Screening equipment such as explosive detectors, metal detectors and x-ray systems should be capable of detecting prohibited and controlled items before entering the facility.

5.21.2 Performance testing procedures for metal detectors should respond to presence of weapons, firearms, knives and non-ferromagnetic material including stainless steel, aluminium and steel material.

5.21.3 X-ray machines should provide supplementary detection in addition to metal detectors and protective personal hand searches for personnel, visitors and service providers.

5.21.4 X-ray machines should show a discernible image of prohibited and controlled items.

5.21.5 Wires and other objects that may be electronic in nature should be discernible on the x-ray machine monitor.

5.21.6 Volumetric interior intrusion detection systems should be tested in respect to walk tests, voltage variation, temperature and humidity, electromagnetic susceptibility, vibration, standby power, and shock.

5.21.7 Volumetric sensors should be able to detect a person walking at a rate of 30 centimetres per second within the total field of view of the sensor and its plane of detection.

5.21.8 Balanced magnetic switches should trigger an alarm when attempt is made to substitute an external magnetic field.

5.21.9 Balanced magnetic switches should trigger an alarm whenever the edge of the door is over 2.5 centimetres from the door jamb and when the back edge clears the jamb.

5.21.10 All personnel and contractors to be associated with testing and maintenance of IDS and the various components of the PPS should have applicable security clearances.

6 TRAINING, REPORTING, PROCEDURES AND RECORDS

6.1 Training

6.1.1 Management and security officers should be trained on the necessary radiation and radiation protection aspects.

6.1.2 Management and security officers should be trained on required legislative provisions.

6.1.3 Procedure should be in place to determine use of the various types of weapons such as batons, automatic rifles, pepper spray or guns.

6.1.4 Approved training procedures for the contracted security vendor or for the facility providing its own security personnel should be authorised.

6.1.5 All security personnel and management should be certified by an authorised body.

6.1.6 Security officers and management should be trained on what actions to take when responding to a radioactive source, device, transport package or radioactive material that has been recovered or intercepted.

6.1.7 Schedules and programs for training of the physical protection personnel should make provision for adequate response during extraordinary situations.

6.2 Reporting of nuclear security events or incidents

6.2.1 Reporting of nuclear security events or incidents shall be as per section 5.13 of the General Nuclear Security Regulations.

6.3 Review of procedures

6.3.1 Security procedures should be reviewed every 2 years or as and when required to do so.

6.4 Record keeping

6.4.1 Procedures should be in place for security records to be kept for at least 40 years by the facility.

6.4.2 Records of incidents including testing and maintenance should be documented on-site in accordance to approved management procedures.

6.4.3 Security records should be accessible to authorised and cleared individuals on need-to-know basis.

7 REFERENCES

The following references were consulted during the compilation of this document:

[1] Act No. 47, 1999, National Nuclear Regulator Act

[2] Convention on the Physical Protection of Nuclear Material (INFCIRC/ 274/ Rev.1) and the 2005 Amendment (GOV/INF/2005/10-GC(49)/INF/6).

[3] United Nations Security Council Resolutions 1373 (2001), 1540 (2004), 1673 (2006) and 1887 (2009)

[4] International Convention for the Suppression of Acts of Nuclear Terrorism (UNGA Resolution 59/290) (2005)

[5] IAEA Handbook on Nuclear Law- Implementing legislation

[6] IAEA INSAG-24 The Interface Between Safety and Security at Nuclear Power Plants

[7] IAEA Technical Guidance on Engineering Safety Aspects of the Protection of Nuclear Power Plants against Sabotage (Nuclear Security Series No. 4)

[8] IAEA Implementing Guide on Nuclear Security Culture (Nuclear Security Series No. 7)

[9] IAEA Implementing Guide on Preventive and Protective Measures against Insider Threats (Nuclear Security Series No. 8)

[10] IAEA Implementing Guide on Security in the Transport of Radioactive Material (Nuclear Security Series No. 9)

[11] IAEA Implementing Guide on Development, Use and Maintenance of the Design Basis Threat (Nuclear Security Series No. 10)

[12] IAEA Nuclear Security Recommendations on the Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Rev.5) (Nuclear Security Series No. 13)

[13] IAEA Nuclear Security Recommendations on Radioactive material and associated facilities (Nuclear Security Series No. 14).

[14] IAEA Technical Guidance on Identification of Vital Areas at Nuclear Facilities (Nuclear Security Series No. 16)

[15] IAEA Technical Guidance on Computer Security at Nuclear Facilities (Nuclear Security Series No. 17)

[16] IAEA Physical Protection Objectives and Fundamental Principles (GC(45)/INF/14)

[17] IAEA Implementing Guide on Establishing the Nuclear Security Infrastructure for a Nuclear Power Programme (Nuclear Security Series No. 19)

[18] IAEA Nuclear Security Fundamentals on Objective and Essential Elements of a State's Nuclear Security Regime (Nuclear Security Series No. 20)