Published in Volume 110, No. 21 of the Official Gazette dated May 26, 2014

Code of PNRI Regulations
Part 26

Security of Radioactive Sources

Nuclear Regulatory Division/PNRI
Rev. 1, February 2014

Published in Volume 110, No. 21 of the Official Gazette dated May 26, 2014

CPR Part 26

SECURITY OF RADIOACTIVE SOURCES

TABLE OF CONTENTS

V. RECORDING AND REPORTING REQUIREMENTS

VI. INSPECTION AND ENFORCEMENT

VII. EFFECTIVE DATE

Published in Volume 110, No. 21 of the Official Gazette dated May 26, 2014

Republic of the Philippines
Department of Science and Technology
PHILIPPINE NUCLEAR RESEARCH INSTITUTE
Commonwealth Avenue
Diliman, Quezon City

CPR Part 26

SECURITY OF RADIOACTIVE SOURCES

I. GENERAL PROVISIONS

Section 1. Purpose.

(a) The requirements in this Part are issued pursuant to:

(1) Section 2 of the Republic Act No. 5207, as amended, which provides as a matter of policy, to protect the public against the use of radioactive materials and associated facilities for unauthorized purposes; and
(2) Section 3(f)(3) of the Republic Act No. 9372, an act to secure the state and protect our people from terrorism also known as “Human Security Act of 2007”.

(b) The main objectives of this Part are:

(1) to achieve and maintain a high level of security of radioactive sources that is commensurate with the potential hazard posed by the radioactive sources, while recognizing the need to ensure appropriate use of the radioactive sources for beneficial purposes;
(2) to establish and maintain the security of radioactive sources throughout their entire life cycle; and
(3) to prevent unauthorized access or damage to, and loss, theft or unauthorized transfer of radioactive sources for malicious act.

(c) The requirements in this Part shall be used in conjunction with applicable Codes of PNRI Regulations (CPR) covering radiation safety, and with regard to the control of radioactive sources.

(d) Nothing in this Part shall be construed to limit actions as may be appropriate and necessary to protect the general public and the environment.

Section 2. Scope.

(a) The requirements in this Part shall apply to:

(1) adoption, introduction, conduct, discontinuance, or cessation of a practice involving radioactive sources; and
(2) design, manufacture, construction or assembly, acquisition, distribution, selling, loaning, locating, commissioning, processing, possession, use and operation, maintenance or repair, transfer or decommissioning, disassembly, storage, or disposal of the radioactive sources within a practice.

(b) The requirements in this Part shall also apply to radioactive sources within any practice to include disused sources or any other radioactive material as specified by the PNRI regulations, orders, or amendments of the requirements in this Part.

Section 3. Exemptions.

The requirements in this Part do not apply to:

(a) Radioactive waste material in general;

(b) Unsealed radioactive material, however PNRI may require, under specific circumstances, the security management of unsealed radioactive materials in accordance with this Part;

(c) Nuclear material as defined in the Convention on the Physical Protection of Nuclear Material except for radioactive sources incorporating Plutonium-239, such as in PuBe neutron sources.

Section 4. Definitions.

As used in this Part:

(a) **"Accounting"** means physically checking with an appropriate radiation survey that all radioactive sources are present in their expected location;

(b) **"Act"** means the Republic Act No. 5207, as amended, otherwise known as the "Atomic Energy Regulatory and Liability Act of 1968";

(c) **"Administrative Measures"** means the use of policies, procedures and techniques that direct personnel to securely and safely manage radioactive sources;

(d) **"Balanced Protection"** means adequate protection along all adversary pathways such that no easy path is created for the adversary;

(e) **"CPR"** means the Code of PNRI Regulations;

(f) **"Delay"** means the elements of a security system designed to increase the time required for an adversary to gain unauthorized access to or to remove or sabotage the radioactive sources, generally through barriers or other physical means;

(g) **"Defense-in-depth"** means the combination of multiple layers of systems and measures that have to be overcome or circumvented before security is compromised;

(h) **"Detection"** means a process in a security system that begins with sensing a potentially malicious or other unauthorized act and that is completed with the assessment of the cause of the alarm;

(i) **"Deterrence"** means security measures designed to dissuade an individual from undertaking a malicious act;

(j) **"Disposal"** means the emplacement of the radioactive sources in an appropriate facility without the intention of retrieval;

(k) **"Disused Source"** means a radioactive source which is no longer used, and is not intended to be used, for the practice for which a license has been granted;

(l) **"Graded approach"** means the application of security measures proportional to the potential consequences of a malicious act;

(m) **"Inventory"** means physically checking the identification of each individual radioactive source possessed by the licensee using appropriate means, such as serial numbers, manufacturer's name, size, dimension and activity;

(n) **"License"** means the authorization granted by PNRI on the basis of a safety and security assessment and accompanied by specific requirements and conditions to be completed by the licensee;

(o) **"Licensee"** means a holder of a specific PNRI license issued pursuant to the Code of PNRI Regulations or CPRs;

(p) **"Life cycle"** means the series of changes that happen with the radioactive source over the course of its useful life;

(q) **"Malicious Act"** means an act or attempt of unauthorized removal of the radioactive sources or sabotage;

(r) **"Orphan Source"** means a radioactive source which is not under regulatory control, either because it has never been under regulatory control, or because it has been abandoned, lost, misplaced, stolen or transferred without proper authorization;

(s) **"Person"** means (i) any individual, firm, partnership, association, trust, estate, private or public body, whether corporate or not, or government agency other than the Institute, any province, city, municipality, or any political entity within the Philippines and (ii) any legal successor, representative, agent or agency of the foregoing;

(t) **"PNRI"** means the Philippine Nuclear Research Institute and/or its duly authorized representative(s);

(u) **"Practice"** means any human activity that introduces additional sources of exposure or exposure pathways or extends exposure to additional people or modifies the network of exposure pathways from existing sources, so as to increase the exposure or the likelihood of exposure of people or the number of people exposed;

(v) **"Radioactive Source"** means a radioactive material that is permanently sealed in a capsule or closely bonded, in a solid form and which is not exempt from regulatory control. It shall also mean any radioactive material released if a radioactive source is leaking or broken, but does not mean material encapsulated for disposal, or nuclear material within the nuclear fuel cycles of research and power reactors;

(w) **"Radioactive Waste"** means material, whatever its physical form, remaining from practices or interventions and for which no further use is foreseen that contains or is contaminated with radioactive substances and has an activity or activity concentration higher than the level for clearance from regulatory requirements, and exposure to which is not excluded from the International Basic Safety Standards;

(x) **"Response"** means the actions undertaken following detection to prevent an adversary from succeeding or to mitigate potentially severe consequences. These actions, typically performed by security or law enforcement personnel, including

interrupting and subduing an adversary while the attempted unauthorized removal or sabotage is in progress, preventing the adversary from using the radioactive sources to cause harmful consequences, recovering the radioactive sources, or otherwise reducing the severity of the consequences.

(y) **"Sabotage"** means any deliberate act directed against the radioactive sources or associated facility or activity that could directly or indirectly endanger the health and safety of personnel, the public and the environment by exposure to radiation or release of radioactive material;

(z) **"Safety"** means measures intended to minimize the likelihood of accidents involving radioactive sources and, should such an accident occur, to mitigate its consequences;

(aa) **"Safety Culture"** means the assembly of characteristics and attitudes in organizations and individuals which establishes that, as an overriding priority, protection and safety issues receive the attention warranted by their significance;

(bb) **"Security"** means the prevention and detection of, and response to, a malicious act;

(cc) **"Security Culture"** means the assembly of characteristics, attitudes and behaviors of individuals, organizations and institutions which serves as means to support, enhance and sustain nuclear security;

(dd) **"Security Contingency Plan"** means sets of actions for response to unauthorized acts indicative of attempted unauthorized removal or sabotage, including threats thereof, designed to effectively counter such acts;

(ee) "**Security Goal"** means the overall result that the security system must be capable of providing for a given security level and only addresses unauthorized removal. Achievement of the goals will reduce the likelihood of a successful act of sabotage;

(ff) **"Security Management"** means measures addressing access control, trustworthiness, information protection, preparation of a security plan, training and qualification, accounting, inventory and security event reporting. The stringency of required security management measures should vary as appropriate based on the graded approach;

(gg) **"Security Plan"** means a document prepared by the licensee that presents a detailed description of the security arrangements in place at a facility;

(hh) **"Security System"** means an integrated set of security measures intended to prevent a threat from completing a malicious act;

(ii) **"Storage"** means the holding of radioactive sources in a facility that provides for their containment with the intention of retrieval in the future;

(jj) **"Technical Measures"** means the physical barriers to the radioactive sources, device or facility to separate these from unauthorized personnel and to deter, or to prevent inadvertent or unauthorized access to, or removal of, the radioactive sources;

(kk) **"Timely Detection"** means detection of any unauthorized access, which together with delay measures is sufficient to enable guards or response forces to interdict the intruder;

(ll) **"Transfer"** means a process that involves the changes of responsibilities and accountability of the safety and security of the source from one licensee to another.

(mm) **"Threat"** means a person or group of persons with motivation, intention and capability to commit a malicious act.

Note: Terms defined in the Act and in other Parts of the CPR shall have the same meaning when used in this Part to the extent that such terms are not specifically defined in this Part.

Section 5. Interpretation.

Except as specifically authorized by the Director in writing, no interpretation of the meaning of the regulations by any officer or employee of the PNRI other than a written interpretation by the Director will be recognized to be binding upon the PNRI.

Section 6. General Obligation.

No person shall engage in the activities involving radioactive sources except as authorized in a license issued by PNRI pursuant to the specific requirements of this Part.

Section 7. Access to Premises and Information.

For purposes of implementing its licensing and regulatory functions pursuant to the Act, authorized representatives of PNRI may have immediate access to premises and facilities in which authorized practices are conducted or sources are located, in order to obtain information about the status of source security and verify compliance with regulatory requirements of this Part.

Section 8. Resolution of Conflicts.

PNRI may initiate the appropriate steps towards its resolution if a conflict exists between the requirements in this Part and other laws and regulations.

Section 9. Additional Requirements.

PNRI may impose additional requirements by regulation, order, or conditions of a license, in addition to those established in the requirements of this Part, as it deems appropriate or necessary to protect health; minimize risk from radiation hazards; or protect the national interest.

Section 10. Communication.

All communications and reports concerning the requirements of this Part shall be addressed to the Director, Philippine Nuclear Research Institute, Commonwealth Avenue, Diliman, Quezon City, Metro Manila.

II. ADMINISTRATIVE REQUIREMENTS

Section 11. Responsibilities of Licensees.

(a) The licensee shall designate a security manager and other qualified individuals in key assignments related to the security of the radioactive sources and/or facility. Other individuals' assigned tasks that substantially affect the security of the radioactive sources and/or the facility shall also be identified.

(b) The licensee shall bear the responsibility for establishing and implementing the administrative and technical measures that are needed for ensuring security for the authorized radioactive sources and facilities and for compliance with all applicable requirements in this Part and conditions of the license.

(c) The licensee shall ensure that only authorized individuals by reference in the license shall be permitted to fulfill such required assignments and tasks.

(d) The licensee shall ensure that such individuals meet the requirements for training and trustworthiness specified in the requirements in this Part.

(e) The licensee shall notify PNRI of the intentions to introduce any modification to facilities or activities affecting the security of the radioactive sources for which they are licensed, and shall not carry out any such modification unless specifically authorized by PNRI.

(f) The licensee shall ensure that security measures do not compromise the safety of individuals or the protection of the environment.

(g) The licensee shall notify PNRI of any intention to introduce any amendment to an authorized practice, which could have implications to security, and shall not carry out such amendment unless specifically authorized by PNRI.

Section 12. Responsibilities of a Security Manager.

(a) The Security Manager shall be responsible in the development and overall implementation of the security plan and procedures to provide valuable insights for improving the consideration of safety and security risks in a system-integrated way.

(b) The Security Manager shall provide advice and analysis to ensure that security requirements are being implemented in a manner that does not compromise safety.

(c) The Security Manager shall coordinate with the licensee's Radiation Safety Officer in matters related to safety of radioactive sources.

(d) The Security Manager shall communicate and coordinate with the law enforcement agency in matters related to security incidents.

Section 13. Security Culture.

(a) The licensee shall promote security culture and establish a management system, commensurate with the security levels described in Table 1, to ensure that:

(1) policies and procedures are established;
(2) problems affecting security are promptly identified and corrected;
(3) the responsibilities of each individual for security are clearly identified and each individual is suitably trained and qualified;
(4) clear lines of authority for decisions on security are defined;
(5) organizational arrangements and lines of communications are established that result in an appropriate flow of information on security at, and between, the various levels in the entire organization of the licensee;
(6) sensitive information relative to the security of radioactive sources is identified and protected according to the requirements in this Part; and
(7) security of radioactive sources is managed in accordance with a security plan commensurate with the security level of the radioactive sources.

Section 14. Confidentiality and Information Security.

(a) The licensee shall establish information management systems, commensurate with the security level of the radioactive sources, which ensure that:

(1) the confidentiality of information received in confidence from another party is protected; and
(2) the confidentiality of information, the unauthorized disclosure of which could compromise security measures.

(b) Information or documents that can be used to identify specific locations, specific security measures or weaknesses in the licensee's system of management of sources shall be controlled and distributed only to individuals authorized to receive the information on a need to know basis. This information includes, as appropriate:

(1) specific locations of the radioactive sources;
(2) the facility's security plan and security system associated with the radioactive sources;
(3) temporary or permanent weaknesses in the security system;
(4) radioactive source utilization log;
(5) transport security plan;
(6) proposed dates and times of shipment of radioactive sources; and
(7) security contingency plans.

Section 15. Trustworthiness of Authorized Individuals.

(a) The licensee shall take measures to determine and periodically review the trustworthiness of authorized individuals with access to sensitive information in accordance with Section 14 of this Part or have unescorted access to radioactive sources in accordance with Section 30 of this Part.

(b) The licensee shall cause its authorized individuals to take psychological examinations and undergo appropriate background checks.

(c) The means of determining and reviewing trustworthiness shall be commensurate to the security level of the authorized practices or sources within the practice.

Section 16. Training Requirements.

(a) The licensee shall ensure that all personnel responsible for the security plan are given appropriate training, including the effective implementation of security measures.

(b) The licensee shall ensure that the personnel responsible for the security of radioactive sources:

(1) are instructed in the licensee's security plan and implementing procedures, their responsibilities, and the appropriate response to security incidents;
(2) receive training on security awareness that addresses the nature of security related threats that includes:
(i) security plan including security contingency plan; and
(ii) other associated plans commensurate with the responsibilities of personnel and their roles in implementing the plans.

(c) The licensee shall train the dedicated security personnel in the timely notification of concerned local law enforcement agency during emergencies.

(d) Personnel subject to the training requirements of this Part shall complete the training before being allowed unescorted access to radioactive sources.

(e) The licensee shall require personnel responsible for the security of radioactive sources to undertake periodic refresher training especially when significant changes have been made to the security plan. The training, as applicable for Security Levels A and B, shall address:

(1) any significant change in the security plan;
(2) reports on relevant security issues, problems or lessons learned;
(3) relevant results from readiness reviews and inspections by PNRI or other responsible groups or organizations; and
(4) relevant results from the licensee's own reviews and evaluations.

(f) Training programs shall be routinely evaluated and updated as necessary.

Section 17. Quality Assurance.

(a) The licensee shall establish a quality assurance program that provides, as appropriate:

(1) adequate assurance that the specified requirements relating to security are satisfied;
(2) assurance that the components of the security system are sufficient for their tasks; and
(3) quality control mechanisms and procedures for reviewing and assessing the overall effectiveness of security measures.

(b) The quality assurance program for radioactive sources in Security Levels A and B shall include annual drills and exercises, and evaluation of security plans including security contingency plans with subsequent revision as necessary.

Section 18. Performance Testing and Verification of Compliance.

The licensee shall conduct performance testing and preventive maintenance of security systems to verify compliance with the requirements in this Part and the conditions of the license. Performance testing shall include drills and exercises in which personnel exhibit their understanding and ability to perform their required tasks.

III. TECHNICAL REQUIREMENTS

Section 19. Security System and Security Functions.

The licensee shall ensure that a security system is designed and installed to protect radioactive sources from an adversary intent of committing a malicious act. The design shall allow the security system to perform the basic security functions: detection, delay, response, and security management.

Section 20. Design and Evaluation of Security Systems.

The licensee shall ensure that their security system integrates measures to perform the basic security functions in accordance with Section 19 of this Part consistent with the security concepts that shall include the following:

(a) deterrence cannot be measured;

(b) detection before delay;

(c) detection requires assessment;

(d) balanced protection;and

(e) defense-in-depth.

Section 21. Transfer of Radioactive Sources.

The licensee shall not transfer radioactive sources to another person unless:

(a) licensed by PNRI;

(b) the recipient possesses a valid license for the sources; and

(c) the recipient is provided with all relevant technical information to permit the safe and secure management of the sources.

Section 22. Transport Requirements.

The licensee transporting radioactive sources either domestically or internationally shall comply with the requirements of CPR Part 4, “Regulations for the Safe Transport of Radioactive Material in the Philippines”, CPR Part 27, “Security Requirements on the

Transport of Radioactive Material", and other applicable transport requirements including the UN Recommendations on the Transport of Dangerous Goods.

Section 23. Security During Storage and Disposition of Disused Sources.

(a) Disused sources that are on long-term storage or disposal in facilities shall be categorized according to the aggregation within a conditioned container or storage location as described in Section 24 of this Part.

(b) Facilities specifically licensed for long-term storage of radioactive sources shall meet the requirements for the highest security level for which they have been authorized.

(c) The licensee shall dispose of the disused sources within the period fixed by PNRI after determining that extended or long-term storage of disused sources will pose unacceptable risk to the safety and security of the radioactive sources.

IV. SECURITY PERFORMANCE REQUIREMENTS

Section 24. Categorization of Radioactive Sources.

The licensee shall categorize radioactive sources based on their potential to cause harm, including aggregation of sources in a given location, as described in Table 2. The following shall apply to:

(a) Category 1, 2, and 3 Radioactive Sources:

(1) A single radioactive source shall be categorized and assigned to the applicable security level based on the practice in which it is used or the calculated A/D value, as provided in Table 3, whichever requires higher security level; and

(2) An aggregation of sources shall be categorized and assigned to the applicable security level on the basis of the summation of the activity of each radionuclide divided by the corresponding D-value or based on the practice whichever requires higher security level. The calculated sum of A/D values shall be compared to the A/D values and the appropriate security level as provided in Table 3.

(b) Category 4 and 5 Radioactive Sources:

(1) Categories 4 and 5 sources shall be provided control measures with sufficient level of security taking into account the national threat, as appropriate, where the approach is summarized in Table 3.

(c) Sources that are no longer used in a practice listed in Table 3 shall be assigned to a security level on the basis of the ratio of the activity of the source divided by the corresponding D-value. The calculated A/D value shall be compared to the A/D values and the appropriate security level assigned in Table 3.

Section 25. Determination of Applicable Security Level of a Given Source.

The licensee shall determine the security level commensurate to the categorization of the radioactive sources as shown in Table 3. Each security level has a corresponding security goal.

Section 26. Security Levels, Goals and Objectives.

(a) The licensee shall ensure that the security systems meet the overall security goal for each security level and corresponding objectives as prescribed in Table 1.

(b) The licensee shall perform tests, assessments or inspections to determine the overall effectiveness of the facility's security system and evaluate against the applicable security goals and objectives. The security system design shall be reviewed based upon the results of any test, assessment or inspection and modified as necessary.

Section 27. Security Measures.

The licensee shall implement the security measures that are applicable to the security level of the authorized radioactive sources as specified in Tables 4, 5, and 6.

Section 28. Requirements for a Security Plan.

(a) The licensee shall establish a security plan, commensurate with the security level as described in Tables 4, 5, and 6. The security plan shall:

(1) contain, as a minimum, the information in Appendix I and II (Form and Content of Security Plan) of this Part; and
(2) be tested and evaluated annually against the applicable security goal and objectives and shall be reviewed based upon the results of the test.

(b) Identified deficiencies in the plan or security systems shall be promptly remedied and reported in accordance with Section 34.

Section 29. Compensatory or Alternative Measures for Mobile Devices Containing Radioactive Sources.

(a) In cases where the required security measures stated in the license cannot be fully met during field or offsite operations, the licensee may propose alternative compensatory measures that will provide an equivalent level of security.

(b) Such measures shall be approved by PNRI at least fifteen (15) days before commencing a field or offsite operation.

(c) Alternative compensatory measures shall be valid only for the period indicated in the specific authorization, after which the security measures prescribed in the license will be re-established.

Section 30. Access Control Requirements.

(a) The licensee shall control access to radioactive sources and devices containing radioactive sources at all times and limit access only to individuals whose duties require such access and who have prior written approval from the licensee.

(b) Access to radioactive sources, devices, and source locations shall be commensurate with the security level of the radioactive sources, practice or facility, and kept to the minimum necessary, while still allowing the sources to be used for their intended purpose, as provided in Tables 4, 5, and 6.

(c) Only individuals who have been determined to be trustworthy shall have unescorted access.

(d) The licensee shall maintain current a list of individuals who are granted unescorted access to radioactive sources and devices that contain radioactive sources and shall document the basis of approved individual's trustworthiness and reliability.

(e) Individuals whose trustworthiness have not been determined shall be escorted by, or kept under continuous surveillance of, an individual with authorized unescorted access.

(f) The identity of all individuals accessing the source location shall be verified and be issued with appropriate registered passes or badges.

(g) Authorized individuals with access shall be reviewed periodically as to the need for access and continued fitness for authorization.

(h) Authorization shall be withdrawn from individuals who no longer require access to perform their duties or no longer employed by the licensee or did not pass the periodic trustworthiness examination.

(i) Key control measures shall be commensurate with the security level of the radioactive sources, practice or facility.

(j) A record shall be kept of all authorized individuals having access to, or possession of keys concerned with the security of radioactive sources.

Section 31. Security Contingency Plans.

(a) The licensee with radioactive sources in Security Levels A or B shall have specific security contingency plans and procedures, in addition to the safety requirement to have an emergency plan pursuant to the corresponding requirements of this Part for the particular security level.

(b) The licensee with radioactive sources in Security Level C are not required to have specific security contingency plans, but shall be included in a licensed facility's emergency plan.

(c) The security contingency plans shall be appropriate to the type, magnitude and number of radioactive sources. As a minimum, specific contingency plans shall include:

(1) pre-arranged procedures with law enforcement agency for response;

(2) notifications in the event of a loss of a source, including an immediate report to PNRI in accordance with Section 34 of this Part;
(3) initial measures to recover lost or stolen sources;
(4) measures to quickly secure previously unaccounted for sources, found orphan sources, or lost or stolen sources that are recovered;
(5) response to a specific or increased security threat in accordance with Section 32 of this Part; and
(6) media release procedures.

(d) Security contingency plans and procedures shall be exercised, evaluated and updated at least once a year.

Section 32. Specific or Increased Security Threat.

(a) If a licensee with radioactive sources in Security Levels A or B becomes aware, or suspects that there is a specific threat targeting a source or source storage location, security measures shall be increased in accordance with the threat, and may include:

(1) immediately returning the source to its secure storage location if it is in use;

(2) providing a twenty-four (24) hour guard, using additional video camera observation, or an additional intrusion alarm;
(3) ensuring that law enforcement agency and PNRI are made aware of the suspected threat; and
(4) reviewing security procedures, facility layout, and radiation safety practices with the law enforcement and emergency response personnel.

(b) The licensee shall closely cooperate with PNRI for any response planning to an increased threat of malevolent use regarding their radioactive sources, practice or facility.

(c) The licensee shall follow pre-arranged procedures with the law enforcement agency regarding intelligence information and use of appropriately reliable and secure communications as well as their actions to an increased threat.

(d) Increased security measures shall be continued until such time as it is determined that the specific threat is no longer present.

V. RECORDING AND REPORTING REQUIREMENTS

Section 33. Records and Inventory.

(a) The licensee shall keep/maintain and make available for PNRI inspection records of the following:

(1) performance testing of security system and verification of compliance including the results of tests carried out in accordance with the requirements of Section 18 of this Part;
(2) periodic inventory and accounting of each radioactive source;
(3) transfer of radioactive sources;

(4) annual inventory of radioactive sources that are not in routine use and have become disused;
(5) training records; and
(6) results of the review of security plan.

(b) Records of inventory and accounting shall be protected at a security level consistent with the radioactive sources included.

(c) Individual radioactive source records shall include the:

(1) location of the radioactive source;
(2) radionuclide;
(3) radioactivity on a specified date;
(4) model and serial number or unique identifier;
(5) chemical and physical form;
(6) utilization log, including recording all movements into and out of the storage location; and
(7) receipt, transfer, or disposal of the disused source.

(d) Training records shall be maintained for three (3) years and shall include syllabus of training, attendance sheet, training dates, and name of lecturers.

Section 34. Reporting Requirements.

(a) The licensee shall report to PNRI:

(1) Unusual events or incidents, such as:
(i) loss of control over the radioactive sources;
(ii) unauthorized access to, or unauthorized use of radioactive sources;
(iii) failures of equipment containing radioactive sources, which may have security implications;
(iv) discovery of any unaccounted radioactive source;
(v) receipt of specific or general malicious threats.
(2) Identified security system vulnerabilities and corrective actions taken to remedy the circumstances and to prevent a recurrence of similar situations.
(3) Any intention to introduce modifications to any practice with the radioactive sources whenever the modifications could have significant implications for security.

(b) Any violation of the requirements in this Part shall be communicated to PNRI not less than twenty-four (24) hours, and shall include the information required in Section 35.

(c) Reporting within one (1) hour of the following events is required for radioactive sources in Security Levels A and B:

(1) loss of control over the radioactive sources;
(2) actual or attempted theft or sabotage of radioactive sources; and
(3) receipt of a specific or general malicious threat.

(d) Unless otherwise specified, all reports required by this Part shall be made in writing within thirty (30) days.

Section 35. Non-Compliance and Incidents.

(a) In the event the licensee identifies a breach of any applicable requirement of this Part, the licensee shall, as appropriate:

(1) investigate the breach and its causes, circumstances and consequences;
(2) take appropriate action to remedy the circumstances and to prevent a recurrence of similar situations;
(3) report to PNRI within twenty-four (24) hours: the causes of the breach; its circumstances and consequences; and on the corrective or preventive actions taken or to be taken; and
(4) take whatever other actions are necessary as required by this Part.

(b) Failure to take corrective or preventive actions within a reasonable time as determined by PNRI shall be a ground for enforcement.

Section 36. Feedback of Operating Experiences.

The licensee shall ensure that information on operational performance, abnormal conditions, and events that may affect the security of the radioactive sources are made available whenever deemed necessary by PNRI.

VI. INSPECTION AND ENFORCEMENT

Section 37. Inspections.

(a) The licensee shall permit PNRI representative immediate access to premises and facilities where radioactive sources are located in order to obtain information about the status of security and verify compliance with regulatory requirements.

(b) The licensee shall afford to PNRI representative at all reasonable times opportunity to conduct its own performance testing of security measures.

(c) The licensee shall make available to PNRI, for review and inspection upon reasonable notice, information and records pertaining to the security of radioactive sources.

Section 38. Notice of Violation.

(a) A notice of violation shall be issued by PNRI to the licensee who may be found to have violated the requirements of this Part or any term or condition of the license issued hereunder.

(b) The licensee shall develop and implement lasting actions that will not only prevent recurrence of the subject violation, but will be appropriately comprehensive, given the substance and complexity of the violation to prevent occurrence of violations with similar root causes.

Section 39. Modification, Suspension or Revocation of License.

(a) PNRI may modify, suspend or revoke the license to use the radioactive sources, or prohibit the possession of the radioactive sources, upon finding a lapse in security or non-compliance with the requirements of this Part.

(b) Any person who willfully violates, attempts to violate or conspires to violate any rule or regulation or order issued hereunder, may be guilty of a crime, and upon conviction, may be punished by a fine or imprisonment or both as provided by Sections 64 and 65 of Republic Act No. 5207.

VII. EFFECTIVE DATE

Section 40. Effective Date.

This Part shall take effect fifteen (15) days following the publication in the Official Gazette.

Approved:

(Sgd.) ALUMANDA M. DELA ROSA, Ph. D.
Director, PNRI

Date: 28 February 2014

TABLE 1. SECURITY LEVELS AND SECURITY OBJECTIVES.

SECURITY FUNCTION	SECURITY OBJECTIVES[a]		
	Security Level A Goal: Prevent unauthorized removal	Security Level B Goal: Minimize likelihood of unauthorized removal	Security Level C Goal: Reduce likelihood of unauthorized removal
Detect	Provide immediate detection of any unauthorized access to the secured area/source location		
	Provide immediate detection of any attempted unauthorized removal of the radioactive sources, including by an insider	Provide detection of any attempted unauthorized removal of the radioactive sources	Provide detection of unauthorized removal of the radioactive sources
	Provide immediate assessment of detection		
	Provide immediate communication to response personnel		
	Provide a means to detect loss of radioactive sources through verification		
Delay	Provide delay after detection sufficient for response personnel to interrupt the unauthorized removal	Provide delay to minimize the likelihood of unauthorized removal	Provide delay to reduce the likelihood of unauthorized removal
Response	Provide immediate response to assessed alarm with sufficient resources to interrupt and prevent the unauthorized removal	Provide immediate initiation of response to interrupt the unauthorized removal	Implement appropriate action in the event of unauthorized removal of the radioactive sources
Security management	Provide access controls to source location that effectively restrict access to authorized persons only		
	Ensure trustworthiness of authorized individuals		
	Identify and protect sensitive information		
	Provide a security plan		
	Ensure a capability to manage security events covered by security contingency plan (see the Definitions) sabotage.		
	Establish security event reporting system		

[a] Achievement of these goals will also reduce the likelihood of a successful act of sabotage.

TABLE 2. TABLE OF D-VALUES.

a. For an aggregation of radioactive sources of a single radionuclide in a single storage or use location where radioactive sources are in close proximity, such as in storage facilities or manufacturing processes, the total activity shall be treated as one source for the purposes of assigning a category. If radioactive sources with several radionuclides are aggregated, then the sum of the A/D ratios shall be used to determine the category in accordance with the formula:

$$Aggregate \quad \frac{A}{D} = \sum_n \frac{\sum_i A_{i,n}}{D_n}$$

where:

$A_{i,n}$ = activity of each individual radioactive source *i* of radionuclide *n.*
D_n = D-value for radionuclide *n.*

b. Activity corresponding to a 'dangerous' source (D-value) for selected radionuclides and useful multiples thereof.

	Category 1		Category 2		Category 3			
Radionuclide	**1000 x D**		**10 x D**		**D**		**0.01 x D**	
	(TBq)	**(Ci)**	**(TBq)**	**(Ci)**	**(TBq)**	**(Ci)**	**(TBq)**	**(Ci)**
Am-241	6.0E+01	2.0E+03	6.0E-01	2.0E+01	6.0E-02	2.0E+00	6.0E-04	2.0E-02
Am-241/Be	6.0E+01	2.0E+03	6.0E-01	2.0E+01	6.0E-02	2.0E+00	6.0E-04	2.0E-02
Au-198	2.0E+02	5.0E+03	2.0E+00	5.0E+01	2.0E-01	5.0E+00	2.0E-03	5.0E-02
Cd-109	2.0E+04	5.0E+05	2.0E+02	5.0E+03	2.0E+01	5.0E+02	2.0E-01	5.0E+00
Cf-252	2.0E+01	5.0E+02	2.0E-01	5.0E-00	2.0E-02	5.0E-01	2.0E-04	5.0E-03
Cm-244	5.0E+01	1.0E+03	5.0E-01	1.0E+01	5.0E-02	1.0E+00	5.0E-04	1.0E-02
Co-57	7.0E+02	2.0E+04	7.0E+00	2.0E+02	7.0E-01	2.0E+01	7.0E-03	2.0E-01
Co-60	3.0E+01	8.0E+02	3.0E-01	8.0E+00	3.0E-02	8.0E-01	3.0E-04	8.0E-03
Cs-137	1.0E+02	3.0E+03	1.0E+00	3.0E+01	1.0E-01	3.0E+00	1.0E-03	3.0E-02
Fe-55	8.0E+05	2.0E+07	8.0E+03	2.0E+05	8.0E+02	2.0E+04	8.0E+00	2.0E+02
Gd-153	1.0E+03	3.0E+04	1.0E+01	3.0E+02	1.0E+00	3.0E+01	1.0E-02	3.0E-01
Ge-68	7.0E+02	2.0E+04	7.0E+00	2.0E+02	7.0E-01	2.0E+01	7.0E-03	2.0E-01
H-3	2.0E+06	5.0E+07	2.0E+04	5.0E+05	2.0E+03	5.0E+04	2.0E+01	5.0E+02
I-125	2.0E+02	5.0E+03	2.0E+00	5.0E+01	2.0E-01	5.0E+00	2.0E-03	5.0E-02
I-131	2.0E+02	5.0E+03	2.0E+00	5.0E+01	2.0E-01	5.0E+00	2.0E-03	5.0E-02
Ir-192	8.0E+01	2.0E+03	8.0E-01	2.0E+01	8.0E-02	2.0E+00	8.0E-04	2.0E-02
Kr-85	3.0E+04	8.0E+05	3.0E+02	8.0E+03	3.0E+01	8.0E+02	3.0E-01	8.0E+00
Mo-99	3.0E+02	8.0E+03	3.0E+00	8.0E+01	3.0E-01	8.0E+00	3.0E-03	8.0E-02
Ni-63	6.0E+04	2.0E+06	6.0E+02	2.0E+04	6.0E+01	2.0E+03	6.0E-01	2.0E+01
P-32	1.0E+04	3.0E+05	1.0E+02	3.0E+03	1.0E+01	3.0E+02	1.0E-01	3.0E+00
Pd-103	9.0E+04	2.0E+06	9.0E+02	2.0E+04	9.0E+01	2.0E+03	9.0E-01	2.0E+01
Pm-147	4.0E+04	1.0E+06	4.0E+02	1.0E+04	4.0E+01	1.0E+03	4.0E-01	1.0E+01
Po-210	6.0E+02	2.0E+03	6.0E-01	2.0E+01	6.0E-02	2.0E+00	6.0E-04	2.0E-02
Pu-238	6.0E+01	2.0E+03	6.0E-01	2.0E+01	6.0E-02	2.0E+00	6.0E-04	2.0E-02
Pu-239[d]/Be	6.0E+01	2.0E+03	6.0E-01	2.0E+01	6.0E-02	2.0E+00	6.0E-04	2.0E-02
Ra-226	4.0E+01	1.0E+03	4.0E-01	1.0E+01	4.0E-02	1.0E+00	4.0E-04	1.0E-02
Ru-106(Rh-106)	3.0E+02	8.0E+03	3.0E+00	8.0E+01	3.0E-01	8.0E+00	3.0E-03	8.0E-02
Se-75	2.0E+02	5.0E+03	2.0E+00	5.0E+01	2.0E-01	5.0E+00	2.0E-03	5.0E-02
Sr-90(Y-90)	1.0E+03	3.0E+04	1.0E+01	3.0E+02	1.0E+00	3.0E+01	1.0E-02	3.0E-01
Tc-99m	7.0E+02	2.0E+04	7.0E+00	2.0E+02	7.0E-01	2.0E+01	7.0E-03	2.0E-01
Tl-204	2.0E+04	5.0E+05	2.0E+01	5.0E+03	2.0E+01	5.0E+02	2.0E-01	5.0E+00
Tm-170	2.0E+04	5.0E+05	2.0E+02	5.0E+03	2.0E+01	5.0E+02	2.0E-01	5.0E+00
Yb-169	3.0E+02	8.0E+03	3.0E+00	8.0E+01	3.0E-01	8.0E+00	3.0E-03	8.0E-02

TABLE 3. CATEGORIES AND DEFAULT SECURITY LEVELS FOR COMMONLY USED SOURCES.

CATEGORY	SOURCES AND PRACTICES[a]	A/D[b]	SECURITY LEVEL
1	Irradiators teletherapy sources Fixed multibeam teletherapy (e.g. gamma knife) sources	A/D > 1000	A
2	Industrial gamma radiography sources High/medium dose rate brachytherapy sources	1000 > A/D > 10	B
3	Fixed industrial gauges that incorporate high activity sources[c] Well logging gauges	10 > A/D > 1	C
4	Low dose rate brachytherapy (except eye plaques and permanent implants) Industrial gauges that do not incorporate high activity sources Bone densitometers Static eliminators	1 > A/D > 0.01	Apply measures as described in relevant Code of PNRI Regulations (CPRs)[e].
5	Low dose rate brachytherapy eye plaques and permanent implant sources XRF devices Electron capture devices Mossbauer spectrometry sources Positron emission tomography (PET) check sources	0.01 > A/D and A >exempt[d]	

[a] Factors other than A/D alone have been taken into consideration in assigning the sources to a category (Categorization of Radioactive Sources, IAEA Safety Standards Series No. RS-G-1.9, IAEA, Vienna (2005), Annex I).

[b] This column can be used to determine the category of a source purely on the basis of A/D. This may be appropriate, for example, if the facilities and activities are not known or are not listed, if sources have a short half-life and/or are unsealed, or if sources are aggregated (Categorization of Radioactive Sources, IAEA Safety Standards Series No. RS-G-1.9, IAEA, Vienna (2005), paragraph 3.5).

[c] Examples are given in (Categorization of Radioactive Sources, IAEA Safety Standards Series No. RS-G-1.9, IAEA, Vienna (2005), Annex I).

[d] Exempt quantities as stipulated in Appendix I of CPR Part 3, Standards for Protection Against Radiation, published in the Official Gazette on 6 September 2004.

[e] For Categories 4 and 5, refer to the relevant CPRs.

TABLE 4. SECURITY MEASURES FOR SECURITY LEVEL A.
(Goal: prevent unauthorized removal)

SECURITY FUNCTION	SECURITY OBJECTIVE	SECURITY MEASURES
Detect	Provide immediate detection of any unauthorized access to the secured area/source location.	Electronic intrusion detection system and/or continuous surveillance by licensee personnel.
	Provide immediate detection of any attempted unauthorized removal of the source, including by an insider.	Electronic tamper detection equipment and/ or continuous surveillance by licensee personnel.
	Provide immediate assessment of detection.	Remote monitoring of CCTV or assessment by licensee / response personnel.
	Provide immediate communication to response personnel.	Rapid, dependable, diverse means of communication such as phones, cell phones, pagers, radios.
	Provide a means to detect loss through verification.	Daily checking through physical checks, CCTV, tamper indicating devices, etc.
Delay	Provide delay after detection sufficient for response personnel to interrupt the unauthorized removal.	System of at least two layers of barriers (e.g. walls, cages) which together provide delay sufficient to enable response personnel to interdict
Response	Provide immediate response to assessed alarm with sufficient resources to interrupt and prevent the unauthorized removal.	Capability for immediate response with size, equipment, and training to interdict.
Security management	Provide access controls to source location that effectively restrict access to authorized persons only.	Identification and verification, for example, lock controlled by swipe card reader and personal identification number, or key and key control.
	Ensure trustworthiness of authorized individuals.	Background checks for all personnel authorized for unescorted access to the source location and for access to sensitive information.
	Identify and protect sensitive information.	Procedures to identify sensitive information and protect it from unauthorized disclosure
	Provide a security plan.	A security plan which conforms to regulatory requirements and provides for response to increased threat levels.
	Ensure a capability to manage security events covered by security contingency plans.	Procedures for responding to security-related scenarios.
	Establish security event reporting system.	Procedures for timely reporting of security events.

TABLE 5. SECURITY MEASURES FOR SECURITY LEVEL B.
(Goal: minimize the likelihood of unauthorized removal)

SECURITY FUNCTION	SECURITY OBJECTIVE	SECURITY MEASURES
Detect	Provide immediate detection of any unauthorized access to the secured area/source location	Electronic intrusion detection equipment and/or continuous surveillance by licensee personnel
	Provide detection of any attempted unauthorized removal of the source	Tamper detection equipment and/ or periodic checks by licensee personnel
	Provide immediate assessment of detection	Remote monitoring of CCTV or assessment by licensee / response personnel
	Provide immediate communication to response personnel	Rapid, dependable means of communication such as phones, cell phones, pagers, radios
	Provide a means to detect loss through verification	Weekly checking through physical checks, tamper detection equipment, etc.
Delay	Provide delay to minimize the likelihood of unauthorized removal	System of two layers of barriers (e.g. walls, cages)
Response	Provide immediate initiation of response to interrupt unauthorized removal	Equipment and procedures to immediately initiate response
Security management	Provide access controls to source location that effectively restrict access to authorized persons only	One identification measure
	Ensure trustworthiness of authorized individuals	Background checks for all personnel authorized for unescorted access to the source location and for access to sensitive information
	Identify and protect sensitive information	Procedures to identify sensitive information and protect it from unauthorized disclosure
	Provide a security plan	A security plan which conforms to regulatory requirements and provides for response to increased threat levels
	Ensure a capability to manage security events covered by security contingency plans	Procedures for responding to security-related scenarios Establish security event reporting system Procedures for timely reporting of security events

TABLE 6. SECURITY MEASURES FOR SECURITY LEVEL C.
(Goal: reduce the likelihood of unauthorized removal)

SECURITY FUNCTION	SECURITY OBJECTIVE	SECURITY MEASURES
Detect	Provide detection of unauthorized removal of the source.	Tamper detection equipment and/or periodic checks by licensee personnel.
	Provide immediate assessment of detection.	Assessment by licensee / response personnel.
	Provide a means to detect loss through verification.	Monthly checking through physical checks, tamper indicating devices, or other checks to confirm the presence of the source.
Delay	Provide delay to reduce the likelihood of unauthorized removal of a source.	One barrier (e.g. cage, source housing) or under observation by licensee personnel.
Response	Implement appropriate action in the event of unauthorized removal of a source.	Procedures for identifying necessary actions in accordance with contingency plans
Security management	Provide access controls to source location that effectively restrict access to authorized persons only.	One identification measure.
	Ensure trustworthiness of authorized individuals.	Appropriate methods for determining the trustworthiness of authorized individuals with unescorted access to radioactive sources and access to sensitive information.
	Identify and protect sensitive information.	Procedures to identify sensitive information and protect it from unauthorized disclosure.
	Provide a security plan.	Documentation of security arrangements and reference procedures.
	Ensure a capability to manage security events covered by security contingency plans.	Procedures for responding to security related scenarios.
	Establish security event reporting system.	Procedures for timely reporting of security events.

APPENDIX I. FORM AND CONTENT OF SECURITY PLAN FOR SECURITY LEVELS A AND B

A security plan should include all information necessary to describe the security approach and system being used for protection of the radioactive sources. The level of detail and depth of content should be commensurate with the security level of the radioactive sources covered by the plan. The following topics should typically be included:

1. Chapter 1 INTRODUCTION
   - 1.1. Background
   - 1.2. Objective
   - 1.3. Scope
   - 1.4. National Regulatory and Other Guidance Documents

2. Chapter 2 FACILITY DESCRIPTION
   - 2.1. Description of Facility and Surrounding Environment
   - 2.2. Description of Radioactive Source(s) and its use
   - 2.3. Determination of Categorization of the Radioactive Sources and Applicable Security Levels

3. Chapter 3 SECURITY MANAGEMENT
   - 3.1. Roles and Responsibilities/Structure of Security Organization
   - 3.2. Training Program
   - 3.3. Performance Testing
   - 3.4. Verification of Compliance
   - 3.5. Maintenance Program
   - 3.6. Budget and Resource Plan
   - 3.7. Background Checks
   - 3.8. Confidentiality and Information Protection

4. Chapter 4 SECURITY SYSTEM DESIGN
   - 4.1. Definition of Security Functions
   - 4.2. Access Control Measures
   - 4.3. Description of Technical Barriers

5. Chapter 5 SECURITY PROCEDURES
   - 5.1. Routine, Off Shift and Emergency Operations
   - 5.2. Opening and Closing of Facility
   - 5.3. Key and Lock Control Measures
   - 5.4. Source Accounting Measures
   - 5.5. Local Security Procedures
   - 5.6. Procedures to address Increased Threat Level

6. Chapter 6 RESPONSE PLANNING
   - 6.1. Security Communications Plan
   - 6.2. Security Contingency Plan
   - 6.3. Security Event Reporting

APPENDIX II. FORM AND CONTENT OF SECURITY PLAN FOR SECURITY LEVEL C

A security plan should include all information necessary to describe the security arrangements and procedures for protection of the radioactive sources. The following topics should typically be included:

1. Objective
2. Description of Facility and Surrounding Environment
3. Description of Radioactive Sources and its use
4. Roles and Responsibilities/Structure of Security Organization
5. Background Checks
6. Description of Technical Barriers
7. Access Control Measures
8. Key and Lock Control Measures
9. Source Accounting Measures
10. Emergency Plan

REFERENCES.

[1] Code of PNRI Regulations Part 26, Security of Radioactive Sources, published in the Official Gazette on 1 January 2007.
[2] Code of PNRI Regulations Part 2, Licensing of Radioactive Material, published in Official Gazette on 16 July 1990.
[3] Code of PNRI Regulations Part 3, Standards for Protection Against Radiation, published in the Official Gazette on 6 September 2004.
[4] Code of PNRI Regulations Part 11, Licenses for Industrial Radiography and Radiation Safety Requirements for Radiographic Operations, published in the Official Gazette on 8 February 2010.
[5] Code of PNRI Regulations Part 12, Licenses for Medical Use of Radioactive Sources in Teletherapy, published in the Official Gazette on 20 October 2008.
[6] Code of PNRI Regulations Part 14, Licenses for Medical Use of Radioactive Sources in Brachytherapy, published in the Official Gazette on 4 January 2010.
[7] Code of PNRI Regulations Part 16, Licenses for the Use of Sealed Sources Contained in Industrial Devices, published in the Official Gazette on 16 August 1999.
[8] IAEA Nuclear Security Series No. 11 (NSS 11), Security of Radioactive Sources, Vienna, 2009.
[9] IAEA Safety Guide No. RS-G-1.9, Categorization of Radioactive Sources, Vienna, 2005.
[10] PNRI Administrative Order No. 2, Series of 2011, Regulatory Criteria in Determining Severity of Violation(s).

CONTRIBUTORS.

(a) **COMMITTEE ON THE REVISION OF CODE OF PNRI REGULATION PART 26**

CARL M. NOHAY, Chairman
SSRS, Radiological Impact Assessment Section, NRD
TERESITA G. DE JESUS, Member
SSRS, Regulatory Development and Standards Section, NRD
SYLVIA S. BUSINE, Member
SSRS, Nuclear Safeguards and Security Section, NRD
THELMA P. ARTIFICIO, Member
SSRS, Licensing Review and Evaluation Section, NRD
LUZVIMINDA L. VENIDA, Member
SSRS, Inspection and Enforcement Section, NRD

(b) **JULIETTA E. SEGUIS**
Head, Nuclear Safeguards and Security Section, NRD
(c) **MARIA VISITACION B. PALATTAO**
Head, Regulations and Standards Development Section, NRD
(d) **VANGELINE K. PARAMI, Ph.D.**
Head, Licensing Review and Evaluation Section, NRD
(e) **EDGAR G. RACHO**
Head, Inspection and Enforcement Section, NRD
(f) **ALFONSO A. SINGAYAN**
SSRS, Regulations and Standards Development Section, NRD
(g) **NELSON P. BADINAS**
SSRS, Inspection and Enforcement Section, NRD