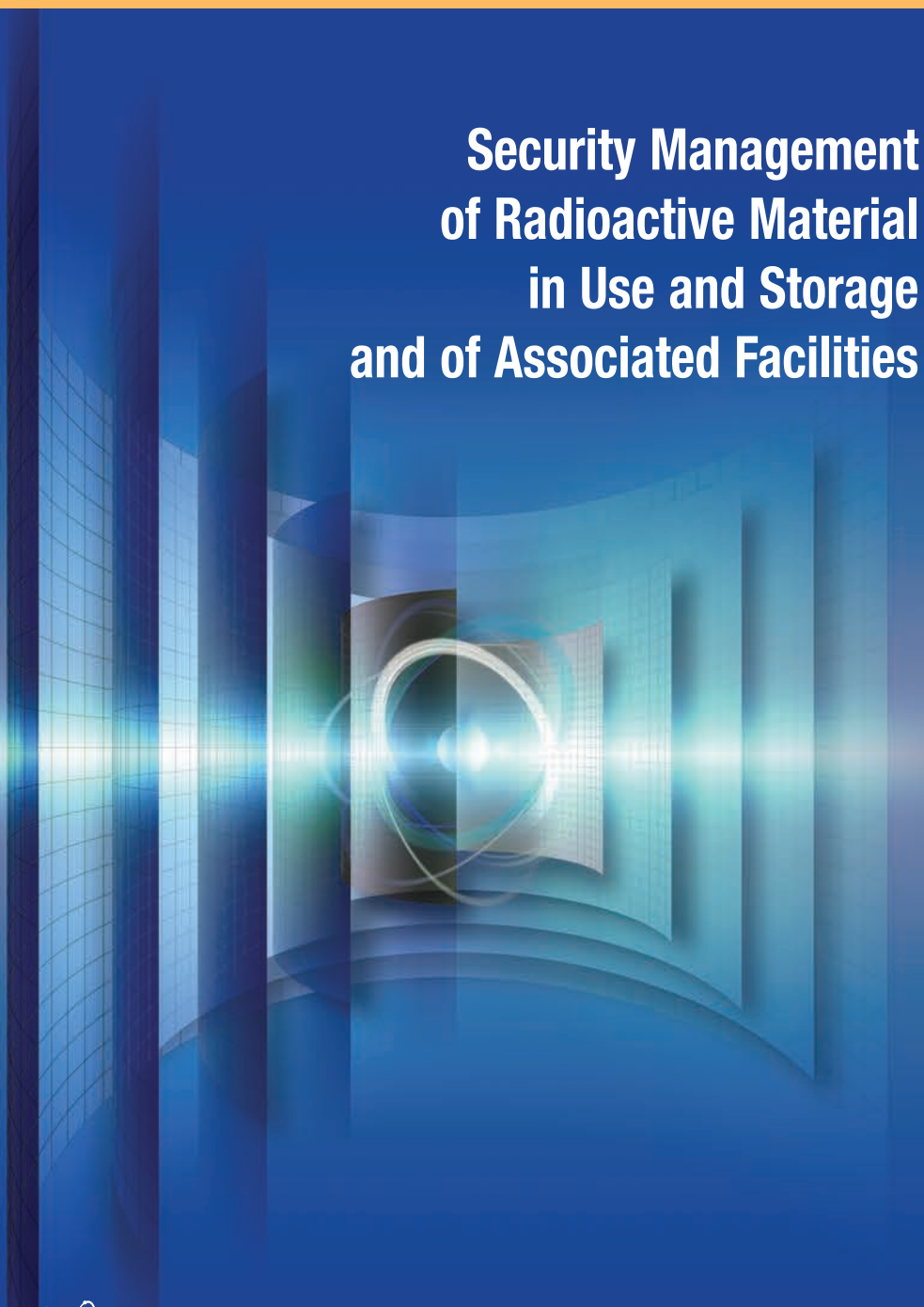
IAEA Nuclear Security Series No. 43-T

Technical Guidance

Security Management of Radioactive Material in Use and Storage and of Associated Facilities



IAEA
International Atomic Energy Agency

IAEA NUCLEAR SECURITY SERIES

Nuclear security issues relating to the prevention and detection of, and response to, criminal or intentional unauthorized acts involving, or directed at, nuclear material, other radioactive material, associated facilities or associated activities are addressed in the **IAEA Nuclear Security Series**. These publications are consistent with, and complement, international nuclear security instruments, such as the Convention on the Physical Protection of Nuclear Material and its Amendment, the International Convention for the Suppression of Acts of Nuclear Terrorism, United Nations Security Council resolutions 1373 and 1540, and the Code of Conduct on the Safety and Security of Radioactive Sources.

CATEGORIES IN THE IAEA NUCLEAR SECURITY SERIES

Publications in the IAEA Nuclear Security Series are issued in the following categories:

- **Nuclear Security Fundamentals** specify the objective of a State's nuclear security regime and the essential elements of such a regime. They provide the basis for the Nuclear Security Recommendations.
- **Nuclear Security Recommendations** set out measures that States should take to achieve and maintain an effective national nuclear security regime consistent with the Nuclear Security Fundamentals.
- **Implementing Guides** provide guidance on the means by which States could implement the measures set out in the Nuclear Security Recommendations. As such, they focus on how to meet the recommendations relating to broad areas of nuclear security.
- **Technical Guidance** provides guidance on specific technical subjects to supplement the guidance set out in the Implementing Guides. They focus on details of how to implement the necessary measures.

DRAFTING AND REVIEW

The preparation and review of Nuclear Security Series publications involves the IAEA Secretariat, experts from Member States (who assist the Secretariat in drafting the publications) and the Nuclear Security Guidance Committee (NSGC), which reviews and approves draft publications. Where appropriate, open-ended technical meetings are also held during drafting to provide an opportunity for specialists from Member States and relevant international organizations to review and discuss the draft text. In addition, to ensure a high level of international review and consensus, the Secretariat submits the draft texts to all Member States for a period of 120 days for formal review.

For each publication, the Secretariat prepares the following, which the NSGC approves at successive stages in the preparation and review process:

- An outline and work plan describing the intended new or revised publication, its intended purpose, scope and content;
- A draft publication for submission to Member States for comment during the 120 day consultation period;
- A final draft publication taking account of Member States' comments.

The process for drafting and reviewing publications in the IAEA Nuclear Security Series takes account of confidentiality considerations and recognizes that nuclear security is inseparably linked with general and specific national security concerns.

An underlying consideration is that related IAEA safety standards and safeguards activities should be taken into account in the technical content of the publications. In particular, Nuclear Security Series publications addressing areas in which there are interfaces with safety — known as interface documents — are reviewed at each of the stages set out above by relevant Safety Standards Committees as well as by the NSGC.

SECURITY MANAGEMENT OF RADIOACTIVE MATERIAL IN USE AND STORAGE AND OF ASSOCIATED FACILITIES

The following States are Members of the International Atomic Energy Agency:

AFGHANISTAN
ALBANIA
ALGERIA
ANGOLA
ANTIGUA AND BARBUDA
ARGENTINA
ARMENIA
AUSTRALIA
AUSTRIA
AZERBAIJAN
BAHAMAS
BAHRAIN
BANGLADESH
BARBADOS
BELARUS
BELGIUM
BELIZE
BENIN
BOLIVIA, PLURINATIONAL STATE OF
BOSNIA AND HERZEGOVINA
BOTSWANA
BRAZIL
BRUNEI DARUSSALAM
BULGARIA
BURKINA FASO
BURUNDI
CAMBODIA
CAMEROON
CANADA
CENTRAL AFRICAN REPUBLIC
CHAD
CHILE
CHINA
COLOMBIA
COMOROS
CONGO
COSTA RICA
CÔTE D'IVOIRE
CROATIA
CUBA
CYPRUS
CZECH REPUBLIC
DEMOCRATIC REPUBLIC OF THE CONGO
DENMARK
DJIBOUTI
DOMINICA
DOMINICAN REPUBLIC
ECUADOR
EGYPT
EL SALVADOR
ERITREA
ESTONIA
ESWATINI
ETHIOPIA
FIJI
FINLAND
FRANCE
GABON
GEORGIA
GERMANY
GHANA
GREECE
GRENADA
GUATEMALA
GUYANA
HAITI
HOLY SEE
HONDURAS
HUNGARY
ICELAND
INDIA
INDONESIA
IRAN, ISLAMIC REPUBLIC OF
IRAQ
IRELAND
ISRAEL
ITALY
JAMAICA
JAPAN
JORDAN
KAZAKHSTAN
KENYA
KOREA, REPUBLIC OF
KUWAIT
KYRGYZSTAN
LAO PEOPLE'S DEMOCRATIC REPUBLIC
LATVIA
LEBANON
LESOTHO
LIBERIA
LIBYA
LIECHTENSTEIN
LITHUANIA
LUXEMBOURG
MADAGASCAR
MALAWI
MALAYSIA
MALI
MALTA
MARSHALL ISLANDS
MAURITANIA
MAURITIUS
MEXICO
MONACO
MONGOLIA
MONTENEGRO
MOROCCO
MOZAMBIQUE
MYANMAR
NAMIBIA
NEPAL
NETHERLANDS
NEW ZEALAND
NICARAGUA
NIGER
NIGERIA
NORTH MACEDONIA
NORWAY
OMAN
PAKISTAN
PALAU
PANAMA
PAPUA NEW GUINEA
PARAGUAY
PERU
PHILIPPINES
POLAND
PORTUGAL
QATAR
REPUBLIC OF MOLDOVA
ROMANIA
RUSSIAN FEDERATION
RWANDA
SAINT LUCIA
SAINT VINCENT AND THE GRENADINES
SAMOA
SAN MARINO
SAUDI ARABIA
SENEGAL
SERBIA
SEYCHELLES
SIERRA LEONE
SINGAPORE
SLOVAKIA
SLOVENIA
SOUTH AFRICA
SPAIN
SRI LANKA
SUDAN
SWEDEN
SWITZERLAND
SYRIAN ARAB REPUBLIC
TAJIKISTAN
THAILAND
TOGO
TRINIDAD AND TOBAGO
TUNISIA
TURKEY
TURKMENISTAN
UGANDA
UKRAINE
UNITED ARAB EMIRATES
UNITED KINGDOM OF GREAT BRITAIN AND NORTHERN IRELAND
UNITED REPUBLIC OF TANZANIA
UNITED STATES OF AMERICA
URUGUAY
UZBEKISTAN
VANUATU
VENEZUELA, BOLIVARIAN REPUBLIC OF
VIET NAM
YEMEN
ZAMBIA
ZIMBABWE

The Agency's Statute was approved on 23 October 1956 by the Conference on the Statute of the IAEA held at United Nations Headquarters, New York; it entered into force on 29 July 1957. The Headquarters of the Agency are situated in Vienna. Its principal objective is "to accelerate and enlarge the contribution of atomic energy to peace, health and prosperity throughout the world".

IAEA NUCLEAR SECURITY SERIES No. 43-T

SECURITY MANAGEMENT OF RADIOACTIVE MATERIAL IN USE AND STORAGE AND OF ASSOCIATED FACILITIES

TECHNICAL GUIDANCE

INTERNATIONAL ATOMIC ENERGY AGENCY
VIENNA, 2022

COPYRIGHT NOTICE

Marketing and Sales Unit, Publishing Section
International Atomic Energy Agency
Vienna International Centre
PO Box 100
1400 Vienna, Austria
fax: +43 1 26007 22529
tel.: +43 1 2600 22417
email: sales.publications@iaea.org
www.iaea.org/publications

Printed by the IAEA in Austria
March 2022
STI/PUB/1951

IAEA Library Cataloguing in Publication Data

Names: International Atomic Energy Agency.
Title: Security management of radioactive material in use and storage and of associated facilities / International Atomic Energy Agency.
Description: Vienna : International Atomic Energy Agency, 2022. | Series: IAEA nuclear security series, ISSN 1816–9317 ; no. 43-T | Includes bibliographical references.
Identifiers: IAEAL 21-01472 | ISBN 978–92–0–118221–0 (paperback : alk. paper) | ISBN 978–92–0–118321–7 (pdf) | ISBN 978–92–0–118421–4 (epub)
Subjects: LCSH: Radioactive substances — Security measures. | Nuclear facilities — Security measures. | Radioactive substances — Storage.
Classification: UDC 620.267:343.852 | STI/PUB/1951

FOREWORD

by Rafael Mariano Grossi
Director General

The IAEA Nuclear Security Series provides international consensus guidance on all aspects of nuclear security to support States as they work to fulfil their responsibility for nuclear security. The IAEA establishes and maintains this guidance as part of its central role in providing nuclear security related international support and coordination.

The IAEA Nuclear Security Series was launched in 2006 and is continuously updated by the IAEA in cooperation with experts from Member States. As Director General, I am committed to ensuring that the IAEA maintains and improves upon this integrated, comprehensive and consistent set of up to date, user friendly and fit for purpose security guidance publications of high quality. The proper application of this guidance in the use of nuclear science and technology should offer a high level of nuclear security and provide the confidence necessary to allow for the ongoing use of nuclear technology for the benefit of all.

Nuclear security is a national responsibility. The IAEA Nuclear Security Series complements international legal instruments on nuclear security and serves as a global reference to help parties meet their obligations. While the security guidance is not legally binding on Member States, it is widely applied. It has become an indispensable reference point and a common denominator for the vast majority of Member States that have adopted this guidance for use in national regulations to enhance nuclear security in nuclear power generation, research reactors and fuel cycle facilities as well as in nuclear applications in medicine, industry, agriculture and research.

The guidance provided in the IAEA Nuclear Security Series is based on the practical experience of its Member States and produced through international consensus. The involvement of the members of the Nuclear Security Guidance Committee and others is particularly important, and I am grateful to all those who contribute their knowledge and expertise to this endeavour.

The IAEA also uses the guidance in the IAEA Nuclear Security Series when it assists Member States through its review missions and advisory services. This helps Member States in the application of this guidance and enables valuable experience and insight to be shared. Feedback from these missions and services, and lessons identified from events and experience in the use and application of security guidance, are taken into account during their periodic revision.

I believe the guidance provided in the IAEA Nuclear Security Series and its application make an invaluable contribution to ensuring a high level of nuclear security in the use of nuclear technology. I encourage all Member States to promote and apply this guidance, and to work with the IAEA to uphold its quality now and in the future.

EDITORIAL NOTE

CONTENTS

1. INTRODUCTION

BACKGROUND

1.1. The IAEA Nuclear Security Series provides guidance for States to assist them in implementing national nuclear security regimes as well as in reviewing and, when necessary, strengthening their regimes. The Series also serves as guidance for States in fulfilling their obligations and commitments with respect to binding and non-binding international instruments adopted under the IAEA and other auspices.

1.2. IAEA Nuclear Security Series No. 20, Objective and Essential Elements of a State's Nuclear Security Regime [1], provides the objective and essential elements for a nuclear security regime. IAEA Nuclear Security Series No. 14, Nuclear Security Recommendations on Radioactive Material and Associated Facilities [2], provides recommendations for States and competent authorities on developing, enhancing, implementing and maintaining a nuclear security regime for radioactive material, associated facilities and associated activities. IAEA Nuclear Security Series No. 11-G (Rev. 1), Security of Radioactive Material in Use and Storage and of Associated Facilities [3], provides guidance to States and their competent authorities on how to implement the recommendations contained in Ref. [2].

1.3. This publication supplements Ref. [3] by providing detailed guidance on security management, including details on the development of a security plan for radioactive material in use and storage and for associated facilities.

OBJECTIVE

1.4. The objective of this publication is to provide guidance to States, competent authorities and operators on how to implement and maintain security management measures, including details on the development of a security plan, for radioactive material in use and storage and for associated facilities.

1.5. This publication is also intended to assist regulatory bodies in establishing regulations and guidance on security management and to assist operators in meeting these regulatory requirements.

SCOPE

1.6. This publication applies to security management of radioactive material in use and storage and of associated facilities.

1.7. This publication covers radioactive material that includes sealed radioactive sources and unsealed radioactive material under regulatory control, including radioactive material over which regulatory control has been gained or regained.

1.8. The term ‘radioactive material’ is used throughout this publication, but the application of this guidance to radioactive material other than sealed radioactive sources will depend on national context and priorities.

1.9. This publication is intended primarily for application at facilities that use and store Category 1, 2 and 3 radioactive sources, as defined in the Code of Conduct on the Safety and Security of Radioactive Sources [4], and other radioactive material. Although this publication does not specifically address the security management of Category 4 and 5 radioactive sources, a State might choose to apply the security management concepts and measures outlined in this Technical Guidance to such material.

1.10. This publication does not cover preparedness and response to a nuclear or radiological emergency triggered by a nuclear security event, which are addressed in IAEA Safety Standards Series No. GSR Part 7, Preparedness and Response for a Nuclear or Radiological Emergency [5].

1.11. This publication also does not address security management relating to the transport of radioactive material, other than transport that is incidental to the use of mobile or portable radioactive material. The topic of transport of radioactive material is addressed in IAEA Nuclear Security Series No. 9-G (Rev. 1), Security of Radioactive Material in Transport [6].

1.12. This publication does not address security measures relating to radioactive material out of regulatory control.

STRUCTURE

1.13. Section 2 explains the role and purposes of security management. Section 3 provides guidance on implementing security sub-goals and measures. Section 4 provides additional guidance and good practices for security management.

Section 5 provides guidance on the contents of a facility security plan for radioactive material in use and storage. The annexes provide examples of documentation referred to in the main text.

2. ROLE AND PURPOSES OF SECURITY MANAGEMENT

2.1. Security management of radioactive material in use and storage and of associated facilities includes the establishment and implementation of policies, plans, procedures and processes that provide personnel with the needed authority and resources to establish and maintain an effective security system. Security management should be a component of the operator's overall management system.

2.2. Security should be integrated into the overall management system in a manner that avoids, or at least minimizes, conflicts with other elements of the management system, such as nuclear and radiation safety, and takes advantage of potential synergies. In particular, the operator should ensure that, as far as possible, security measures and safety measures do not conflict with one another and are mutually supportive.

2.3. Security management has the following three main purposes:

(a) Ensuring the effectiveness and sustainability of the security system;
(b) Ensuring that personnel, procedures and equipment function effectively as a system (integration);
(c) Promoting a robust nuclear security culture.

In the following subsections, each of these purposes is presented in more detail.

EFFECTIVENESS AND SUSTAINABILITY

2.4. The first purpose of security management is to ensure that the security system is effective and sustainable. To achieve this, the security system should be reliably operated and maintained, should be evaluated, should function as intended and should meet regulatory requirements.

2.5. The operating organization's leadership should provide staff responsible for security with the requisite authority, support and resources to achieve this purpose, including by doing the following:

(a) Ensuring that the security system provides protection against the threat at a level commensurate with the potential consequences of malicious acts, is appropriate to the specific conditions at the facility and meets the regulatory requirements;
(b) Establishing and implementing policies and procedures governing the operation of the security system, the training of individuals responsible for security and the regular evaluation of regulatory compliance and security system performance;
(c) Maintaining security equipment to manufacturer specifications, promptly repairing equipment malfunctions and designing and implementing compensatory measures that meet or exceed applicable security requirements in the event of equipment failures or outages.

INTEGRATION

2.6. The second purpose of security management is to ensure that personnel, procedures and equipment function effectively as a system. The operator should take measures to ensure that personnel, procedures and equipment operate interdependently and in an integrated manner.

NUCLEAR SECURITY CULTURE

2.7. The third purpose of security management is to promote a robust nuclear security culture. Nuclear security culture is the "assembly of characteristics, attitudes and behaviour of individuals, organizations and institutions which serves as a means to support and enhance nuclear security" [7]. Security management policies, plans, processes and procedures should promote a robust nuclear security culture by the following:

(a) Demonstrating leadership commitment to security at the highest level of the organization;
(b) Providing personnel responsible for security with the requisite authority to perform their duties;
(c) Ensuring sufficient resources are available to effectively implement security measures;

(d) Building security awareness and cultivating a sense of shared responsibility for security among all staff;
(e) Holding staff and management accountable for security;
(f) Embedding a robust security culture within the overall organizational culture.

3. SECURITY MANAGEMENT SUB-GOALS AND MEASURES

3.1. An effective security system should display an adequate level of performance for security management as well as for each of the security functions of detection, delay and response. This adequate level of performance can be expressed via 'sub-goals', as per the method for establishing a regulatory programme for the security of radioactive material set out in sections 5 and 6 of Ref. [3]. These sub-goals are also presented in Table 1 (reproduced from Ref. [3]), with accompanying security measures that could be used to meet the individual sub-goals.

3.2. The following subsections provide additional guidance on implementing these sub-goals.

ACCESS MANAGEMENT

3.3. The first four security sub-goals — access authorization, trustworthiness assessment, access control and information protection — are arrangements through which the operator limits access to radioactive material and sensitive information only to those individuals who have been authorized for such access, based on a demonstration of their operational need for such access and verification of their trustworthiness and reliability.

3.4. These four sub-goals are grouped together as access management in this publication in order to emphasize their interdependency.

TABLE 1. SECURITY MANAGEMENT MEASURES

Security sub-goal	Security measures
Establish a process for granting individuals authorized unescorted access to radioactive material and/or access to sensitive information	Procedures for determining the individuals who need access, verifying that such individuals are trustworthy and reliable and have received necessary training, authorizing access, withdrawing access as appropriate and maintaining documentation
Ensure trustworthiness and reliability of authorized individuals	Background checks for all personnel authorized for unescorted access to radioactive material and/or for access to sensitive information
Provide access controls that effectively restrict unescorted access to radioactive material to authorized persons only	Identification and verification measures
Identify and protect sensitive information	Procedures to identify sensitive information and protect it from unauthorized disclosure
Provide a security plan	A security plan which addresses required topics, is submitted or made available to the regulatory body and is periodically exercised, evaluated and revised as appropriate
Ensure training and qualification of individuals with security responsibilities	Assessment of necessary knowledge, skills and abilities; provision of corresponding training; procedures for documenting and updating training
Conduct accounting and inventory of radioactive material	Procedures and documentation for verifying presence of radioactive material at prescribed intervals; establishment and maintenance of a radioactive material inventory
Conduct evaluation for compliance and effectiveness, including performance testing	Process for verifying that all applicable security requirements are met and for assessing the effectiveness of the security system, employing performance tests as appropriate
Establish a capability to manage and report nuclear security events	Response plan addressing security related scenarios and procedures for timely reporting of nuclear security events

3.5. Access control measures or separation of duties should be used to ensure that no single person or part of the operating organization has authority over all measures used to manage the access to radioactive material or sensitive information. For example, the operator of a storage facility may require that authorization be received from two persons from two different units in order for an access authorization to be granted.

Access authorization

3.6. Certain personnel need to have unescorted access to radioactive material and/or access to sensitive information in order to discharge their operational or security related responsibilities. Access authorization is the process of granting permission to only these specific personnel for unescorted access to radioactive material and/or for access to sensitive information.

3.7. Regulatory bodies should require operators to limit unescorted access to radioactive material and access to sensitive information to staff with a demonstrated need for such access to perform their jobs, whose trustworthiness has been verified and who have received appropriate security training, to reduce the potential risk posed by insider threats.

3.8. Unescorted access to radioactive material and sensitive information should only be permitted if an access authorization is granted by the operator. The granting of access authorization should be limited to the minimum necessary number of personnel.

3.9. The operator's management should implement a process for granting access authorization, including establishing and implementing procedures that provide for the following:

(a) Determining that an individual needs such access in order to discharge his or her responsibilities and defining the scope of his or her access, for example by limiting it to specific locations, specific hours or circumstances during which access is permitted or specific types of information that may be accessed;
(b) Obtaining verification that the individual is trustworthy and reliable (see paras 3.12–3.18);
(c) Obtaining verification that the individual has received the necessary security training (paras 3.45–3.52);
(d) Authorizing access using the processes described in (a), (b) and (c);
(e) Withdrawing access as appropriate, for example when an individual's responsibilities change or when employment is terminated;

(f) Maintaining current documentation of the results of this process and providing it to those responsible for access control as needed.

Documentation of access authorization could include, for example, the names of personnel with access authorization, their positions, the date of completion of their background checks and security training, the scope of the access authorization, the date from which that access is or was authorized and the date and reason for which access was withdrawn, if applicable.

3.10. Individuals who are not authorized for unescorted access should be allowed access to areas where radioactive material is present only if they are escorted or observed by personnel authorized for such access, or if compensatory measures for the security of the radioactive material have been implemented. This should apply not only to visitors but also to individuals that may access the facility on a regular basis, including maintenance, cleaning and repair staff and contractors.

3.11. More detailed guidance on this topic can be found in IAEA Nuclear Security Series No. 8-G (Rev. 1), Preventive and Protective Measures against Insider Threats [8].

Trustworthiness assessment

3.12. Trustworthiness assessments are used to provide an initial assessment (during the hiring process) and ongoing assessments (occurring periodically throughout the employment period) of an individual's integrity, honesty and reliability [8]. Such a determination is in addition to any identification verification or background checks performed by the operator upon the initial hiring of employees.

3.13. Laws or regulations may define the minimum requirements, standards and scope for the trustworthiness assessments or establish penalties for misrepresenting material facts during the background check. The regulatory bodies and/or other competent authorities should also establish a framework that enables to search criminal and counterterrorism databases as part of the background check. The details of these arrangements will vary depending on the State's legislation and regulations in this area. Example elements of a background check are provided in Annex I.

3.14. The regulatory body should require the operator to establish policies and procedures, on the basis of the category of the radioactive material and following a graded approach, to ensure that the trustworthiness and reliability of all individuals authorized for unescorted access to radioactive material or access to sensitive information have been confirmed through a trustworthiness assessment.

The regulatory body should ensure the availability of arrangements to enable operators to implement this requirement, such as referral to law enforcement or other external agencies for conduct of the review. In some States, this referral process might require facilitation by the regulatory body. Moreover, as noted in para. 4.18 of Ref. [8], "National laws might restrict the scope or conduct of identity verification, personal document verification and trustworthiness assessments in a State".

3.15. The operator should establish policies and procedures for obtaining trustworthiness assessments, documenting the results and managing the privacy of information. The extent of the assessment should be proportional to the sensitivity of the individual's responsibilities, in accordance with applicable regulations. The depth of the assessment should also account for the planned extent of the individual's access to radioactive material or sensitive information and the security level of the radioactive material the individual would access.

3.16. The assessments should review the individual's observance of the law and adherence to the facility rules, as well as any behaviour or motivational factors of concern. For example, the assessment should seek to identify motivational factors such as financial problems or pressures (e.g. debts, wage cuts), adherence to an ideology of concern, desire for revenge (e.g. a perceived injustice against the individual), physical dependency (e.g. drugs, alcohol, sex), psychological or psychiatric characteristics, severe dissatisfaction with private or professional life and other factors due to which an individual could be coerced to commit a malicious act. These motivational factors may be identified by a review of information such as criminal records, personal and professional references, past work history, financial records, on-line and other social networks, medical records and job performance reports, as well as information from colleagues about observed behaviour [8].

3.17. Depending on the State's laws and regulations, trustworthiness checks may be performed only by the competent authority or entirely or partially by the operator. When the operator takes part in this process, the regulatory body and/or other competent authorities should consider developing a standard questionnaire for the trustworthiness assessment, to ensure the consistency of the type of information gathered by operators. Unwillingness to provide information and concealment or misstatement of facts in the personal history disclosure are factors that can raise serious concern when determining trustworthiness for access to radioactive material or sensitive information.

3.18. The trustworthiness assessment for each individual should be carefully documented and protected as sensitive information and retained for possible inspection by the regulatory body. This documentation is also subject to national legislation relevant to trustworthiness assessments, information security and privacy of information.

Access control

3.19. Access control is intended to limit access to locations where radioactive material or security sensitive information is present to authorized persons. Access control typically consists of allowing authorized persons to temporarily disable physical barriers such as a locked door only upon verification of the person's identity and access authorization [3]. Robust implementation of access control rules and procedures can minimize the potential that an insider adversary has access to sensitive material, systems and equipment.

3.20. The operator should establish and document strict access control rules and procedures to limit unescorted access of persons without authorized access to radioactive material, equipment used for processing or handling radioactive material and systems relevant to safety or security.

3.21. The operator should define all facility areas to which unescorted access will be limited to authorized persons. Each such area should consist of a physical space that provides three dimensional containment, such as a locked room with no easily defeated entry points (e.g. windows, false ceilings), and should be configured to minimize the number of personnel who need access in order to perform their jobs. For example, such an area for a teletherapy unit would generally consist of the treatment room and sometimes an anteroom.

3.22. Once the areas are defined to which unescorted access is limited to authorized persons, the operator should select and install barriers (e.g. locked doors) that can be temporarily disabled by authorized persons during working hours to allow entry. Some type of access credentials (e.g. keys, identification cards or a combination of methods) should be needed to enable entry, and a method for verifying the authorized person's credentials should be implemented. The operator should install the necessary equipment, issue access media to authorized individuals, develop access control procedures for entry to the area, provide training on their use for authorized individuals and conduct regular tests and maintenance.

3.23. According to para. 4.55 of Ref. [8], "Access control records should also be maintained of all persons…who have access to, or are in possession of, keys, key

cards and other credentials relevant for accessing other systems, including computer systems that control access". Procedures should be developed and implemented for documenting and maintaining information on the access authorizations of persons permitted to enter areas to which unescorted access is limited.

3.24. Access credentials should be returned and/or deactivated when access authorization is no longer needed. In addition, physical access credentials such as keys and cards should also be audited and access credentials should be changed periodically. When it is discovered, reported or suspected that access credentials have been lost or compromised, immediate action should be taken to prevent unauthorized access, for example by changing locks, combinations or system programming.

3.25. Rules and procedures for the operation and management of electronic access control systems should also be put into place, if applicable.

3.26. The operator should designate personnel to develop and implement access control procedures, to manage and operate access and entry control systems and to design, install and operate physical access control measures. Management should also provide resources, awareness, training and support to enforce policies and procedures throughout the operating organization.

3.27. Access control rules should be defined for visitors, escorts and for abnormal conditions such as response to emergencies and system outages [8]. The access control rules should state that authorized individuals are responsible for escorting individuals who do not have access authorization for the limited access area. Persons without authorized access should be permitted to enter the limited access area only if they have a specific need to do so, such as treatment, maintenance or janitorial activities. Authorized individuals should accompany escorted persons at all times that they are in the limited access area or should maintain constant visual surveillance of the unescorted persons, for example through video monitoring. Upon exit of escorted persons, authorized personnel should ensure the limited access area is again secure or should maintain visual surveillance of the entry until it is secured.

3.28. Further information on access control can be found in Ref. [8].

Information protection

3.29. Paragraph 1.1 of IAEA Nuclear Security Series No. 23-G, Security of Nuclear Information [9], states that "Sensitive information is information, in whatever

form, including software, the unauthorized disclosure, modification, alteration, destruction, or denial of use of which could compromise nuclear security". The same applies to the security of radioactive material. Such information could include, for example, the design of a security system, a list of staff with unescorted access to the radioactive material, or details of an organization's response capabilities to a particular threat. Securing sensitive information is necessary because easy access to inadequately secured information can help adversaries to plan or commit malicious acts with relatively little effort or risk [9]. The operator's security policies and procedures direct information security activities. The security plan is the primary tool to document these activities.

3.30. Paragraph 6.15 of Ref. [9] states that "Personnel security, including trustworthiness checks, ensures that those who have access to sensitive information are deemed by the State to be suitably trustworthy to do so". Personnel should protect sensitive information from unauthorized disclosure and report any actual or suspected unauthorized release, compromise or failure to protect sensitive information. Support of the leadership within the operating organization is needed to provide the resources and training to enforce policies and procedures regarding sensitive information throughout the organization.

3.31. Paragraph 3.4 of Ref. [9] states:

> "The State's relevant competent authorities should develop and issue policy and requirements specific to the security of sensitive information at nuclear material and other radioactive material associated facilities and activities. These are usually based on, and in accordance with, any national security policy and requirements issued by the national security authorities, but taking into account the special nature of the activities that involve such materials".

3.32. In accordance with Ref. [9], information protection measures should be considered for information of at least the following types, which could affect nuclear security:

(a) Details of physical protection systems and any other security measures in place for nuclear material, other radioactive material, associated facilities and activities, including information on guard and response forces;
(b) Information relating to the quantity and form of radioactive material in use or storage, including accounting information;
(c) Details of computer systems, including communication systems, that process, handle, store or transmit information that is directly or indirectly important to safety and security;

(d) Security plan and information on the liaison with local law enforcement agencies;
(e) Contingency and response plans for nuclear security events;
(f) Personal information about employees, vendors and contractors;
(g) Threat assessments and security alert information;
(h) Details of sensitive technology;
(i) Details of vulnerabilities or weaknesses that relate to the above topics;
(j) Historical information on any of the above topics.

3.33. Some of the above information, such as personal information, may also be subject to specific security requirements under other national laws or company policies [9].

SECURITY PLAN

3.34. The security plan enables operators to demonstrate to the regulatory body their compliance with security requirements. A security plan is an important tool for documenting the activities associated with establishing, implementing and maintaining an effective, sustainable and integrated security system that demonstrates the operator's nuclear security culture.

3.35. Paragraph 4.20 of Ref. [2] states that "*Operators* should be required to develop, implement, test, periodically review, revise as necessary a security plan and comply with its provisions". Similarly, the Code of Conduct [4] states that:

> "Every State should ensure that the regulatory body established by its legislation has the authority to […] require those who intend to manage radioactive sources to seek an authorization, and to submit […] a security plan or assessment as appropriate".

3.36. Paragraph 3.33 of Ref. [2] states that "The *regulatory body* should ensure that the *operator's* security plan includes measures to effectively respond to a *malicious act* consistent with the *threat*". The security plan should describe the security systems that are planned or are in place to protect radioactive material in use and storage and associated facilities. It should also include descriptions of the security management measures that are planned or are in place.

3.37. Each facility should develop its own security plan on the basis of applicable regulations and facility policies and practices.

3.38. Applicable regulatory requirements for security, as well as any other applicable national or local requirements, should be documented in the security plan. Regulatory compliance should also be documented, including a description of measures taken by the operator, where appropriate. The plan should set out any policies and procedures established by the operator responsible for the radioactive material that affect the security or the security management of the radioactive material, as well as how these policies and procedures are implemented.

3.39. Senior management should designate individual(s) who will be responsible for preparing and internally approving the security plan. Upon regulatory approval, management should also provide sufficient resources for the implementation of the plan. The designated individual(s) should be responsible for the drafting, implementing, reviewing and updating of the security plan.

3.40. All staff with a defined role in the security plan should be aware of their responsibilities, including any security procedures that apply to them. In particular, response forces, both on-site and off-site, should be consulted during the development of the security plan to ensure that their roles and responsibilities are appropriately understood and documented.

3.41. The security plan should be coordinated with the facility's emergency plans and procedures to ensure consistency, and emergency response personnel should be consulted during the development of the security plan.

3.42. Security plans contain sensitive information and should be protected as such. Some information (e.g. threat information, vulnerability assessment information) might be particularly sensitive and should be included in appendices to which access is further limited to specific individuals with a need to know this information in order to perform their duties.

3.43. The security plan should include a list of references used or referred to in the body of the security plan. The security plan should include appendices (such as procedures) that contain information that is too detailed or too sensitive to include in the main body of the security plan.

3.44. Detailed guidance on a proposed format and contents of a security plan following this approach is provided in Section 5 of this publication as well as in appendix II of Ref. [3].

TRAINING AND QUALIFICATION OF PERSONNEL

3.45. All personnel should have sufficient security awareness to enable them to understand the need for and importance of the security of radioactive material. They should also be able to recognize a nuclear security event and know what to do and who to contact if such an event occurs. Regular security awareness training should be provided to all personnel. Personnel who have specific security responsibilities or perform a particular security function — such as controlling access media (e.g. cards, keys) — or are involved in the response to a security event should be adequately qualified and have specialized training. These individuals may include both staff and contractors.

3.46. Training is used to provide staff with the knowledge, skills and abilities to effectively execute their responsibilities for security as well as to update their knowledge, skills and abilities. Qualification is used to ensure that staff with specific security responsibilities are capable of performing their assigned security responsibilities to an acceptable standard. The contents and delivery of training at each facility should take into account facility specific conditions and qualification of personnel.

3.47. The operator should identify needs for training and qualification of personnel. These should be based on an evaluation of the knowledge, skills and abilities that individuals with security responsibilities need in order to effectively perform their roles. Training and qualification should be documented, and training records should be maintained.

3.48. The operator should establish and deliver a training programme for new personnel and identify needs and timelines for conducting periodic refresher or re-qualification training (see para. 3.49). Development and delivery of security training can be performed by qualified staff, external experts or a combination of the two. All training should include a participant assessment to ensure that learning objectives have been satisfied.

3.49. The content and methods of delivery of courses within the training programme should consider the level of knowledge, skills and abilities needed by the operator or required by the competent authority for personnel in specific roles. The courses should include the following training content:

(a) Security awareness for all facility personnel;
(b) Security system and functions for personnel with specified security responsibilities;

(c) Specialized or advanced training, such as for response personnel;
(d) Specific on-the-job training involving procedures or equipment instructions;
(e) Refresher training.

3.50. All training courses and materials should be regularly reviewed by the operator for relevance of content and effectiveness of delivery. Suggested key learning areas and their topics are provided in Annex II.

3.51. The operator's qualification needs for personnel with specific security responsibilities should generally include minimum educational and previous experience and may also include physical and psychological aspects as well as experience or training in the operation specific security equipment. The management should assess each individual's knowledge, skills and abilities as well as other qualifications against the applicable needs before assigning that individual to a position with security responsibilities. The competence of such staff to perform their assigned duties should also be periodically re-assessed (re-qualification).

3.52. The qualification process should also involve an assessment or verification of the knowledge, skills and abilities needed by the operator. Performance testing provides an additional means to evaluate or validate the application of knowledge and skills of the staff during the performance of their duties (see paras 4.19–4.23).

ACCOUNTING AND INVENTORY

3.53. An inventory is a current list of all radioactive material or items containing radioactive material that an operator is authorized to possess. Accounting processes are used to verify that all radioactive material in an operator's inventory is present at its authorized location, providing a means to detect the loss or unauthorized removal of any radioactive material.

3.54. The regulatory body should specify accounting and inventory requirements in its regulations for the security of radioactive material.

3.55. The operator should verify the presence of radioactive material at its authorized location through such means as the following:

(a) Physical checks;
(b) Remote video monitoring;
(c) Examination of seals or other tamper indicating devices;

(d) Radiation measurements at designated measurement points.

The verification should take place at intervals prescribed by the regulatory body, in accordance with a graded approach and following specific procedures. The intervals at which this verification should take place for various types of material are presented in Ref. [3].

3.56. The regulatory body should require the operator to maintain records indicating the results of each accounting verification, including the date, the individual who carried out the verification and the means used to verify the presence of the radioactive material. If the presence of the radioactive material cannot be verified, the operator should be required to report the loss or unauthorized removal to the regulatory body and/or other competent authorities in a manner and within a time prescribed by the regulatory requirements and to initiate efforts to locate and regain control of the material.

3.57. The operator should establish an inventory of all radioactive material it possesses, noting for each radioactive material in the inventory the following information:

(a) The location of the material;
(b) The radionuclide;
(c) The activity on a specified date;
(d) The serial number or unique identifier;
(e) The chemical and physical forms;
(f) The material use history, including movement into, within and out of the operator's facility;
(g) Receipt, transfer or disposal of the material;
(h) Other information, as appropriate, to enable the material to be identifiable and traceable.

This inventory should be established as prescribed by the regulatory body and in accordance with specific procedures summarized in the security plan.

3.58. The operator should also be required to adjust the inventory following any transfers and receipts within a period of time specified by the regulatory body. Annually or more frequently, as specified by the regulatory body, the operator should be required to verify that the inventory is complete and accurate in all respects and to adjust the inventory to reflect any discrepancies identified. The operator should be required to report the results of these activities to the regulatory body for inclusion in the national registry of radioactive material.

3.59. The operator should assign to one or more individuals the responsibility for performing periodic accounting activities and for verifying the inventory of radioactive material.

EVALUATION FOR COMPLIANCE AND EFFECTIVENESS

3.60. During an evaluation process, the operator should perform a self-assessment to verify that the facility is in compliance with all applicable security requirements. The operator should also assess the effectiveness of the security system to identify any weaknesses that should be corrected and identify any opportunities for improvement, including the development of more effective protection measures.

3.61. Evaluation helps to ensure that the operator's security system is reliably operated and maintained, functions as intended, is effective and continues to meet the regulatory requirements. Evaluation also assists the facility to prepare for regulatory inspections and thus to avoid negative inspection results and possible enforcement action. It may also identify opportunities for improving the cost effectiveness of the security system. If the operator lacks the capability to perform an evaluation of its system, the evaluation could be conducted by specialized security subcontractors or by competent authorities, such as law enforcement.

3.62. The operator's management should establish a process and schedule for conducting evaluations and assign roles and responsibilities for their conduct. Depending on the size of the facility and the complexity of the evaluation, participants can include the following:

(a) An evaluation team leader with overall responsibility for the evaluation;
(b) Evaluation team members responsible for specific assigned evaluation topics;
(c) A facility representative who serves as liaison between the evaluation team and other facility staff;
(d) The facility safety officer who ensures that security evaluation activities, such as performance tests, do not compromise safety.

All facility staff should cooperate as requested in the conduct of these evaluations.

3.63. As described in Ref. [3], performance tests are an especially useful means of evaluating security measures to determine whether these measures can actually perform as expected and produce the desired results. Guidance on performance testing, which should be integral to the evaluation process, is provided in Section 4.

3.64. Over time, the operator should track trends and patterns in the evaluation results to identify emerging problems and opportunities for improvement. The operator should also incorporate evaluation results (both positive and negative), as appropriate, into security awareness training for all staff, as well as in specific training for staff with assigned security responsibilities.

3.65. The details of the evaluation process should be flexible and tailored to the facility's particular needs and constraints. The remainder of this subsection describes an example of how an evaluation should be implemented.

Implementation of an evaluation

3.66. The operator's management should define the scope of the evaluation and identify the security requirements against which compliance is to be verified, such as regulatory requirements, licence conditions and provisions of the facility security. The scope should include the security system and security management elements to be evaluated. Evaluation criteria and methods of evaluation should be agreed with the regulatory body.

3.67. Once the scope of the evaluation is defined, the operator's management should assign a team leader to assume overall responsibility for the planning and conduct of the evaluation. The team leader should prepare an evaluation plan which sets out the evaluation method to be used for each topic to be addressed. Evaluation methods might include: document review (e.g. review of accounting records, access control procedures, training records), interviews (e.g. asking questions of radiation protection officers), observations (e.g. watching personnel entering the secured area) and security analysis tools and models, supported by performance testing (e.g. testing of equipment, personnel or procedures[1]). The results of the evaluation should be integrated for analysis.

3.68. The evaluation plan should include assigned roles and responsibilities for conducting the assessment, including, if appropriate, evaluation team members, facility representatives, facility safety officers and facility staff responsible for matters subject to the evaluation. For each evaluation team member, the plan should specify the topics to be assessed by the team member, the requirements applicable to each assigned topic, any good practices applicable to the topic which have been followed by the operator, the methods to be employed for evaluating

[1] Because of their key role in evaluations, performance tests are addressed separately in paras 4.18–4.23. However, performance testing will be conducted as an integral part of the evaluation process.

each topic and the schedule for preparing, performing and reporting on the evaluation of each assigned topic.

3.69. Following the completion of the evaluation, the team leader should compile the results and prepare an evaluation report. This report could, as applicable, include the following:

(a) The scope and type of the evaluation;
(b) The topics evaluated;
(c) The requirements and the effectiveness of the measures or the good practices applicable to each topic;
(d) The methods employed for evaluation with respect to each topic;
(e) The conclusions reached with respect to each topic with specific reference to the basis for each conclusion;
(f) Recommendations for any follow-up actions.

The evaluation team leader should review the results with the operator's management and adjust any follow-up actions as directed. The operator's management could prepare a prioritized action plan to correct any problems identified in the evaluation.

3.70. The regulatory body should consider if the findings necessitate changes in the facility security system. If so, the findings arising from the evaluation of the effectiveness of the security system should be incorporated into the operator's nuclear security plan to gain regulatory approval for changes to the security system.

MANAGEMENT OF NUCLEAR SECURITY EVENTS

3.71. Management measures related to nuclear security events consist of the operator's policies, plans and procedures to prepare for, respond to and report on nuclear security events. These policies, plans and procedures should be well defined and exercised.

3.72. The facility's response plan should address management and reporting of nuclear security events. Paragraph 3.124 of Ref. [3] states:

> "The regulatory body should require the operator to establish, test and implement measures to detect and respond to nuclear security events, using a graded approach and in cooperation with State and local level emergency

and response plans. These measures should be documented in the operator's security plan or in a stand-alone response plan".

3.73. The operator's response plan should take into account facility circumstances (e.g. its location) and business operations, as well as the roles of the operating personnel, external security response personnel, emergency response organizations and the regulatory body. In developing the facility response plan, the operator along with the external response organizations should determine the following:

(a) The types of nuclear security event to be addressed (such as suspected or threatened malicious acts, unauthorized access to a limited access area, attempted malicious acts and successful malicious acts);
(b) The means by which each type of nuclear security event might be identified (such as detection and assessment of an alarm);
(c) The roles and responsibilities of the operating personnel in the initial phase of each type of nuclear security event, including communications, as appropriate, with the operator's management, external response forces and the regulatory body;
(d) Arrangements with external security response forces for their deployment in response to each type of nuclear security event, including, as appropriate, arrangements regarding the forces' familiarity with the facility and targets, estimated response times, capabilities, strategy and tactics;
(e) Communication methods to be used by operating personnel and external security response forces;
(f) Procedures for reporting of nuclear security events to the regulatory body as well as for notifying external response forces and emergency response organizations, as appropriate, including timeframes for notification and reporting commensurate with the significance of the event.

The operator should confer with the regulatory body to determine when and how the regulatory body will be informed of and involved in the response to a nuclear security event.

3.74. While the operator is responsible for developing, implementing and regularly exercising the response plan, in most cases, the portion of the response aimed at interrupting the adversary will be provided by external security response forces, such as the local law enforcement. Accordingly, the operator should jointly develop, implement and exercise the response plan in conjunction with the organization responsible for the external response forces in order to ensure that the planned response and division of responsibilities is agreed and coordinated. The operator should also include emergency response organizations in the

development, implementation and exercise of the response plan for events that might initiate a nuclear or radiological emergency. The regulatory body might need to engage with the response force organization to facilitate the necessary communications and coordination with the operator.

3.75. The operator should document arrangements with external organizations, such as response force organizations, in memoranda of understanding or other arrangements. The operator should make the response plan available in draft form to the organization providing the external response and the regulatory body for their review and comment, if required or requested.

3.76. The operator should exercise the response plan on a regular basis (at least annually), with the participation of external security response personnel and others, such as the regulatory body, as appropriate. The exercises should also address nuclear security events that might initiate a nuclear or radiological emergency, in order to evaluate the integration of the security response forces with the emergency response organizations. Such exercises could be conducted either as tabletop exercises or as field exercises, depending on the situation and availability of resources. The regulatory body should facilitate the involvement of external security response personnel and other external entities as necessary and appropriate.

3.77. The operator along with external response personnel should review the exercise results and modify the response plan as necessary to address any identified deficiencies.

4. ADDITIONAL GUIDANCE ON SECURITY MANAGEMENT

4.1. In addition to the security management sub-goals and measures identified in Ref. [3] and presented in Section 3, there are a number of other good practices for security management, five of which are presented in the subsections to follow.

4.2. The operator's management should support the promotion and strengthening of nuclear security culture and the evaluation and continuous improvement of nuclear security, including by doing the following:

(a) Establishing clear lines of responsibility and accountability for the implementation of nuclear security requirements imposed by the regulatory body;
(b) Setting security objectives and security performance goals;
(c) Periodically evaluating the management system for the security of radioactive material;
(d) Allocating sufficient resources to guarantee the implementation of security requirements;
(e) Conveying the importance of nuclear security and of fulfilling legal and regulatory obligations;
(f) Creating and sustaining opportunities for learning and development for all personnel;
(g) Encouraging feedback, both positive and negative, from facility personnel.

4.3. The operator's management should continuously promote nuclear security culture and a sustainable security system in which personnel turnover, organizational changes or competing organizational priorities do not lead to a loss of core competencies or weaken security culture. This effort should include systematic knowledge management and succession planning.

ROLES AND RESPONSIBILITIES

4.4. The operator should assign roles and responsibilities for security and ensure that the personnel are familiar with the equipment and procedures needed for these roles and responsibilities to be carried out. In assigning roles and responsibilities for security, the operator should ensure that the security system is effective and that the personnel are held accountable for the proper performance of their duties.

4.5. The operator should analyse the security system to identify activities associated with designing, implementing, operating and maintaining the security system. On the basis of this analysis, the operator should then define, assign and document all roles and responsibilities associated with the performance of each activity. Roles and responsibilities should be described in a manner that is clear, understandable, unambiguous, specific and complete, and the roles and responsibilities should be clearly assigned to appropriate parts of the organization or personnel. The assignment of roles and responsibilities should be summarized

in the security plan as well as in other documents that are accessible to facility personnel with a need to know but without access to the security plan.

4.6. The operator should ensure that the facility personnel possess the authority, training and resources needed to fulfil the responsibilities assigned to them. Once roles and responsibilities have been assigned, performance expectations should be established and assigned staff should be held accountable to them. The operator should clearly convey to the personnel their roles and responsibilities related to security and overall facility operations.

MAINTENANCE PROGRAMME

4.7. A maintenance programme is used to ensure that all security equipment is kept in operational condition and that any security equipment that is malfunctioning is identified as such and restored to its normal operating mode. Most modern security system components have a lifecycle of several years. An effective maintenance programme supports the sustainability of an operator's security system.

4.8. The operator should establish and implement a maintenance programme that defines steps, procedures and schedules for ensuring that all components of the security system are operating effectively. The maintenance programme should also ensure that any components that are not operating effectively are repaired as soon as possible and should include procedures for tracking and reporting system faults. These procedures should include timelines for responding to component or system failures. Until systems are returned to effective operation, the operator should implement additional temporary security measures to ensure that overall security effectiveness is not degraded.

4.9. The maintenance programme should be integrated as much as possible into the overall management system of the facility, while recognizing the sensitive nature of the security system.

4.10. The maintenance programme should address both preventive and corrective maintenance. Security equipment should receive periodic routine preventive maintenance to ensure reliable operation. The maintenance programme should also include arrangements for corrective actions when a system or component fails during normal operation or during testing.

4.11. Activities performed by security maintenance personnel should include the following:

(a) Developing a schedule for preventive maintenance on the basis of manufacturer specifications and experience with the equipment;
(b) Conducting preventive maintenance tasks, including development of maintenance schedules and inspection of existing security equipment;
(c) Correcting faults and failures in a timely manner;
(d) Repairing, modifying or replacing faulty security equipment;
(e) Managing equipment and parts inventory;
(f) Keeping maintenance and warranty records;
(g) Interacting with technical support resources within the organization, security equipment vendor or manufacturer.

4.12. More sophisticated systems, such as those that incorporate biometric sensors or other special detection means, might need more frequent attention.

4.13. The maintenance programme can be carried out by qualified facility technicians, suitable external contractors or a combination of the two. The description of roles and responsibilities summarized in the security plan should include information indicating which personnel have the overall responsibility for maintenance as well as which personnel have the authority for conducting each particular type of maintenance. If an external contractor is employed for the maintenance of security equipment, the description should identify the contract and the major tasks the contractor is to perform. If a combination of facility technicians and external contractors performs maintenance tasks, then the respective section of the security plan should describe explicitly which tasks are assigned to facility technicians and which to external contractors.

4.14. All facility staff should be held responsible for noticing and immediately reporting security equipment that does not function effectively or is not being used properly.

BUDGET ALLOCATION AND RESOURCE PLANNING

4.15. Security budget allocation and resource planning should reflect the priority given to security within the overall facility management system. Budget allocation ensures that necessary funds are available for and dedicated to operating, maintaining and continuously improving the security system. Resource planning

involves a detailed plan to identify, obtain and properly use financial and human resources, training, equipment, and infrastructure for security.

4.16. The operator's budget allocation and resource planning process should include the following activities:

(a) Establishing objectives and goals for the security system that are consistent with the policies of the organization;
(b) Determining the resources necessary to ensure the effectiveness of the security system;
(c) Ensuring that all individuals with security responsibilities are trained and competent to perform their duties;
(d) Providing the necessary resources to operate the security system;
(e) Establishing metrics to ensure the effective use of budget and resources;
(f) Reviewing regularly the expenditure of resources against budget and resource projections and ensuring that action is taken to address deviations.

The information and knowledge of individuals within the organization should also be managed as a resource so that it is retained over time.

4.17. Staff with security responsibilities should provide input into the budget and planning process, as appropriate, as well as use resources efficiently.

PERFORMANCE TESTING

4.18. Paragraph 6.57 of Ref. [3] states:

> "Performance testing, which should be integral to the evaluation process, includes the investigation, measurement, validation or verification of one or more of the following:
>
> — Personnel, to verify that they understand the security system, follow procedures and use the system properly and as intended;
> — Procedures, to verify that the procedures produce the desired result and that personnel understand and properly follow them;
> — Equipment, to verify that equipment functions as intended and is effective."

Paragraph 6.58 of Ref. [3] states that "The regulatory body should require the operator to develop and implement an evaluation process that includes

performance tests, as appropriate". Facility personnel, contractors or a combination thereof should be assigned the responsibility for scheduling and implementing performance tests as part of the evaluation process.

4.19. The operator should conduct appropriate performance tests that include both limited scope tests that focus on one component or a few components at a time and system-wide tests of the entire security system. For example, performance tests may be conducted when the functionality or effectiveness of a particular security system component or security management element is in question. The results of all performance tests conducted should feed into the ongoing evaluation process. Corrective action should be taken when performance testing indicates that any of these items are defective or not performing adequately.

4.20. There are several types of performance tests, such as those testing the following:

(a) Operability, to confirm the operability and functionality of an individual component or system;
(b) Effectiveness, to determine how well the component or system performs;
(c) Simulated adversary testing, to test how a component, group of components or the entire system performs against a specified threat scenario.

4.21. For each performance test, a specific plan should be developed, including the following:

(a) Test objective(s) indicating what is to be accomplished by conducting the performance test;
(b) References to the manufacturer's performance specifications;
(c) The conditions for conducting the performance test;
(d) The test control measures taken to ensure the performance test is valid;
(e) A description of the resources that are needed to conduct the performance test;
(f) Any coordination needs, such as who approves or acknowledges the conduct of the performance test;
(g) The procedure for conducting the performance test;
(h) Criteria for evaluation of the results of the performance test.

An example of a performance test plan is provided in Annex III.

4.22. After conducting a performance test, the operator should document the results, identify any deficiencies and determine corrective actions to address them. The operator should retain all documentation relating to the performance tests.

4.23. Regular performance testing and the review of the results of sequential performance tests can help to identify trends that might need to be addressed to maintain system effectiveness.

RECEIPT AND TRANSFER PROCEDURES

4.24. The regulatory body should specify requirements for receipt and transfer of radioactive material as part of its regulations for the security of radioactive material, including requirements for radioactive material to be transferred only to persons authorized by the regulatory body to receive the material. These requirements may be included as part of general regulations or safety regulations. These requirements are intended to prevent security from being compromised when radioactive material is transferred outside the facility, a stage at which it is especially vulnerable.

4.25. Procedures should be in place to ensure continuity of regulatory control when radioactive material is received from or prepared for shipment. The operator should develop, follow and document compliance with procedures to ensure that the security and control of radioactive material is maintained when it is being received from or prepared for shipment outside the facility and that it is only transferred to persons authorized to receive it.[2]

4.26. These procedures should ensure at a minimum that the operator performs the following actions:

(a) Determines in advance when radioactive material will be received or transferred;

---

[2] International transfers are addressed by export controls consistent with the supplementary Guidance on the Import and Export of Radioactive Sources [10], which is beyond the scope of this Technical Guidance. Transport security, including preparation of radioactive material for transport and development of transport security plans has to be addressed by measures consistent with IAEA Nuclear Security Series No. 9-G (Rev. 1), Security of Radioactive Material in Transport [6], which is also beyond the scope of this Technical Guidance.

(b) Verifies that the recipient of any radioactive material to be transferred is or will be authorized to receive it before the material is shipped;
(c) Identifies any security measures that will not be fully effective when the radioactive material is being accepted or prepared for shipment and any associated vulnerabilities;
(d) Establishes and implements compensatory security measures that address any vulnerabilities identified;
(e) Restores normal security measures as soon as possible when acceptance or transfer is complete;
(f) Updates the facility inventory and reports to the regulatory body that the radioactive material has been received or transferred to another licensed facility, to allow for updating of the national registry.

5. CONTENTS OF A SECURITY PLAN FOR RADIOACTIVE MATERIAL IN USE AND STORAGE

5.1. This section contains guidance on the preparation of a security plan for radioactive material in use and storage, including on the proposed structure and contents of the plan. This section is structured under seven subsections, corresponding to the sections of a facility security plan. This structure builds on the guidance provided in appendix II to Ref. [3]. A detailed example facility security plan is provided in Annex IV.

5.2. The security plan should take into account any applicable national regulatory requirements. Each facility should develop its own security plan in accordance with applicable regulations and facility policies and practices.

INTRODUCTION

5.3. In this section of the security plan, the facility to which the security plan applies should be briefly identified, along with relevant background information for the security plan. The regulatory requirements on which the security plan is based should be described, as well as the objectives it satisfies and the scope of the security plan.

5.4. As part of the elaboration of the plan's scope, connections to other relevant documentation or plans should be described, such as management, operational,

radiation protection or emergency arrangements. Areas where security interacts with or impacts other management systems, especially those for safety, should be addressed.

5.5. The process for developing, approving and updating the security plan should also be described in this section, as well as how the security plan is reviewed and updated. It should be specified that reviews and updates are to be undertaken at a prescribed interval specified by the regulatory body, as applicable, and as necessary to address new threat information, changes in facility operations or any other development that could affect the effectiveness of the security system.

FACILITY DESCRIPTION

5.6. This section of the security plan should describe the purpose or mission of the facility and its operating organization, the activities involving radioactive material, the radioactive material to be protected as part of the plan, its location, the level of protection required by the regulatory body for the material and the physical and operational environment of the facility.

5.7. Information on the radioactive material and associated equipment or devices covered by the security plan should include the radionuclide(s), the current activity as well as the activity at the time that the source was imported with associated reference dates, chemical and physical forms, radioactive source or device serial number, equipment or device brand and model and manufacturer. Further, the categorization of the radioactive material and the associated security level should be identified, according to the applicable regulations, and the basis for this identification should be explained.

5.8. In addition, the physical features of the facility and its surrounding environment should be described in this section, including diagrams and scale floor and building drawings and photographs. The physical descriptions should indicate areas accessible to the public, roads and parking areas, nearest public thoroughfares, the central security office, the building and site perimeter, access points and physical barriers. In addition, the facility's surrounding environment should be described, including areas for industrial, commercial, residential or other uses, approximate distances to nearest police stations and other response services and the proximity to other buildings, roads and other features of security or operational interest, such as other facilities with hazardous materials. Security features should not be described in this section of the security plan, but rather in the security system section.

5.9. Finally, a description of the facility operations should be provided, including working and non-working hours, the number and type of staff involved in the facility's operations and the typical number, type and frequency of visits of non-staff in the facility during scheduled operations or at any other time. Non-staff could include visitors, members of the public, patients, customers, service personnel or contractors.

SECURITY MANAGEMENT

5.10. This section of the security plan should describe the security management measures in place and the duties of management and staff that ensure the effective implementation of these measures. This should include information on roles and responsibilities, access authorization, trustworthiness assessment, information protection, budget allocation and resource planning, evaluation for compliance and effectiveness, and the maintenance programme for the security system. Further information on these topics is provided in paras 5.11–5.19.

5.11. The assignment of all roles and responsibilities relevant to the security of radioactive material should be documented in the security plan, including the roles and responsibilities of the following:

(a) Leadership, management and supervisors;
(b) Staff directly responsible for the security of radioactive material;
(c) Staff with responsibility for regulatory matters, including the licensee, radiation protection officer(s), security personnel, advisers, guards and staff in positions specifically required by regulation.

These roles and responsibilities should be presented in the form of a table.

5.12. In addition, an organizational chart showing the staffing structure with lines of authority and supervision should be included that demonstrates how the security organization and responsibilities fit within the overall facility organization.

5.13. The process for authorizing personnel who need unescorted access to radioactive material, secured areas and/or security sensitive information in order to perform their duties (which might or might not be directly related to nuclear security) should be described in the security plan, including information on how to do the following:

(a) Identify which positions need unescorted access;

(b) Verify that the individuals holding the identified positions have the necessary qualifications and training (see para. 5.14);
(c) Verify that the individuals holding the identified positions are trustworthy (see para. 5.15);
(d) Perform the timely withdrawal of access for individuals who no longer need it;
(e) Conduct periodic review and re-evaluation for particular circumstances;
(f) Maintain up-to-date records of personnel authorized for unescorted access.

5.14. The information on how to verify that individuals holding positions that need unescorted access have the necessary qualifications and training should cover the following, drawing on the information on positions with security responsibilities from paras 3.45–3.52:

(a) The established specifications for qualification of staff with security responsibilities, including any qualifications required by the regulations or licence conditions;
(b) The training to be provided to each individual, including the needed initial, specialized, advanced or refresher training for each position with security responsibilities;
(c) Security awareness training for all staff and any other relevant specific on-the-job training, such as training involving procedures and work instructions;
(d) The provider(s) of the identified training and how frequently each training is to be conducted;
(e) The training records that document satisfactory completion of all security related training.

This information can be presented in the form of a table.

5.15. The security plan should clearly describe the process that is used to verify that individuals holding positions that need unescorted access are trustworthy, including any requirements for periodic review or re-evaluation for particular circumstances. This description should cover the following:

(a) Identification of the individuals whose trustworthiness is to be assessed, on the basis of their need for access authorization;
(b) Identification of the applicable requirements for trustworthiness in the regulations for the security of radioactive material, licence conditions or elsewhere, including any requirements that vary depending on the security level or other factors;

(c) Indication of the method by which each individual is assessed;
(d) Stating which records are maintained and kept confidential as part of the trustworthiness assessment.

5.16. Information that needs to be protected based on regulatory body requirements or facility management policies should also be described. Examples of such information include the following:

(a) Location and inventory of the radioactive material;
(b) Access authorization and access control measures;
(c) Security system design, equipment details and diagrams;
(d) Lock combinations and key codes;
(e) Information on the threat and vulnerability assessments;
(f) Temporary or long term weaknesses in the security system;
(g) Security staffing arrangements;
(h) The means of response to events or alarms;
(i) Planned dates, routes, and mode of shipment or transfer of radioactive material;
(j) Security plan and procedures, response plans and related arrangements and measures;
(k) Private information relating to individuals' background checks.

5.17. In addition, measures used to protect this information should be described, such as the following:

(a) How the protected information is identified, such as the use of markings or other designators to ensure all users of this information recognize it as needing protection;
(b) The particular forms of the protected information, such as paper documents, electronic media or closed-circuit television (CCTV) recordings;
(c) Where the protected information is stored and who has custody of it;
(d) Who has access to sensitive information and how that access is determined (e.g. Is the information required to perform someone's job? Do they have an appropriate level of trustworthiness?);
(e) Which protection measures are in place to prevent unauthorized access when the information is being used or is being stored (e.g. physical protection, encryption);
(f) Which requirements are in place for preventing unauthorized access when the protected information is being reproduced or transmitted within or outside the facility;

(g) How the protected information is destroyed to prevent recovery when no longer needed, including who is authorized to destroy it and by which means the various forms of information will be destroyed.

5.18. Finally, the methods for conducting and implementing resource planning for security should be summarized, including descriptions of how the objectives and goals for the security system are established in accordance with the policies of the organization and how the resources necessary to ensure the effectiveness of the security system are determined and provided. All security related activities of the security system should be considered, including human resources, training, operational costs and equipment maintenance. In addition, a description of how metrics are established to ensure the effective use of budget and other resources should be included, as well as of how the expenditure of resources is reviewed against budget and resource projections and how it is ensured that actions are taken to address any deviations.

5.19. Instead of describing in detail the methods for conducting and implementing resource planning for security in the security plan, references to appropriate documentation can be considered to be sufficient. The process for verifying that the facility security system is in compliance with all applicable security requirements should be described, as well as the process for assessing the effectiveness of the documented security system to identify any weaknesses that should be corrected and any opportunities for continuous improvement, including arrangements for performance testing.

SECURITY SYSTEM

5.20. This section of the security plan should include a description of how the current security system is designed and implemented, in accordance with the State's applicable regulations for the security of radioactive material. This should include any consideration given to the threat information provided to the facility and a description of the security assessment methodology and the security system design, including annotating layers of security on the facility layouts with their associated access control, detection and delay measures. Each of these topics is addressed in paras 5.21–5.26.

5.21. The threat information provided to the facility by the regulatory body or other competent authorities should be summarized as well as how and when this information was provided to the facility. To the extent that the threat information is provided to the facility by the regulatory body or other competent authorities,

this information should be summarized in the security plan to indicate how the security system is designed to protect against both external adversaries and insider threats. Information should also be included addressing which personnel at the facility are responsible for receiving threat information, including any notifications from the regulatory body or other competent authorities of a specific threat or of an increase in an existing threat, and how such information is to be appropriately shared with facility personnel who have a need to know.

5.22. The description of the security assessment methodology should include how the threat information provided to the facility is used in the assessment. The description of the methodology should also include the results of the initial security assessment that was used as input to the security system design, if applicable. The evaluation and vulnerability assessments should be periodically updated as part of any review or update of the security plan and in accordance with licensing requirements. The security plan should address how the evaluation and vulnerability assessments will be updated and how they will be adapted to address any new threat information, any changes in the facility operations or any other developments that could affect the security system performance or vulnerabilities.

5.23. The description of the security system design should note how a graded approach and the concepts of security design, for example, defence in depth, timeliness, robustness and balanced protection were taken into account including description of the layers of protection provided around each secured area identified in the facility layout.

5.24. The description of the security system design should include information on the detection, delay and response measures deployed and how these measures are implemented in an integrated and balanced way along security layers. The description should include the following, for each of the layers of protection around each secured area:

(a) The measures used to detect unauthorized access including, as applicable, both intrusion detection systems and observation by facility personnel;
(b) The measures used to assess the detection of unauthorized access, including personnel and equipment supporting the assessment;
(c) Any barriers or other delay measures used to increase the adversary task time relative to the response time.

5.25. The description of the security system design should also include access control measures across security layers, such as:

(a) How personnel are physically controlled at each access control point;
(b) Specific media used to authenticate the identity of authorized persons such as key cards, personal identification numbers, biometric devices or combinations of these;
(c) Procedures to be followed by authorized persons to access a secured area including, where relevant, the application of the two-person rule;
(d) Procedures to be followed for non-routine access (e.g. medical emergencies, fires, criticality alarms, security incidents);
(e) List of personnel who have access to radioactive material.

5.26. Threat information and the descriptions of the security assessment methodology and security system design can be placed in appendices to which access is limited to authorized personnel with a need to know.

SECURITY PROCEDURES

5.27. The written procedures that provide instructions to the personnel responsible for operating and maintaining the security measures should be summarized in the security plan. The procedures themselves should be separate documents and could be included individually as appendices to the security plan. These procedures include those for routine, off-shift and emergency response, for opening and closing the facility, for access control, for accounting and inventory and for receipt and transfer of radioactive material.

5.28. The summary of the procedures for routine, off-shift and emergency response should include information on how the assigned personnel, such as staff and contractors, will operate the security systems and discharge their other security related responsibilities during regular business hours, non-business hours (off-shift or after-hours operations when staff are not ordinarily present, generally at nights, on weekends, and during holidays), and during emergency response.

5.29. The summary of the procedures for the opening and closing of the facility should include general information on procedures used for opening and closing each secured area within the facility, particularly activities such as the unlocking and locking of doors and other barriers and communications with the central alarm station to deactivate and activate detection systems. The summary of the procedures should identify who within the organization is responsible for opening

and closing these areas and should note actions used to validate that other delay mechanisms have been appropriately secured.

5.30. The summary of the procedures for access control should include general information on the procedures used for control of keys, locks, combinations, passwords and related access control measures. The summary should note who is responsible for changing these access control measures and the specific conditions under which they are to be changed, such as the compromise of a combination or password, loss of a security key or termination of a staff member's access.

5.31. The summary of the procedures for accounting and inventory should address how periodic accounting for radioactive material is performed, as required by the applicable regulations, including the following:

(a) The accounting method used, such as physical checks, remote video monitoring, examination of seals or other tamper indicating devices or radiation measurements;
(b) The information contained in records that are generated, indicating the results of each verification and when, by whom and by what method verification was performed;
(c) Facility rules for the implementation of corrective actions and reporting if the presence of radioactive material cannot be verified;
(d) A description of how the facility's inventory of all radioactive material is established and maintained, as required by the applicable regulations.

Information should be included on procedures to notify the regulatory body of changes to the inventory within the prescribed period and to report the inventory to the regulatory body at prescribed intervals to verify that it is complete and accurate.

5.32. The summary of the procedures for receipt and transfer of radioactive material should include a summary of the procedures used to ensure that the operator maintains security and control of radioactive material when it is being received from outside the facility. Procedures used to ensure that the facility takes the necessary steps to make sure that radioactive material is provided only to a person authorized by the regulatory body to receive the material should also be summarized.

RESPONSE

5.33. The security plan should include information on the on-site and off-site response arrangements for nuclear security events, including how these arrangements are integrated with the response to nuclear or radiological emergencies. The security plan should include information on the following:

(a) The facility's arrangements with local law enforcement or other designated response authorities for responding to a nuclear security event, including attempted or actual theft or sabotage;
(b) Methods to be used by the operator for communicating with the regulatory body and local law enforcement or other designated competent authority within the time frame required by the regulatory body;
(c) Methods for reporting nuclear security events to the facility security organization, including how nuclear security events are documented, which personnel are responsible for documenting the event and any subsequent external reporting requirements (e.g. reporting to the regulatory body) as well as how plans and procedures are reviewed after an event in order to evaluate the effectiveness of the security plan and to identify corrective actions;
(d) Arrangements and actions to be taken during nuclear, radiological or other emergencies not initiated by a nuclear security event or other contingency situations in order to ensure the protection of the radioactive material at the facility, including any compensatory measures to be employed in the case of security system failures (such as loss of power);
(e) How notifications of an increased threat level are addressed by the facility.

REFERENCE DOCUMENTS

5.34. The security plan should include a list of reference documents. This could include specific regulations, regulatory licences, operating manuals and organizational policies, security response and emergency plans and other manuals that are referred to in the security plan, or that are needed to explain or expand on any details in the security plan.

REFERENCES

[1] INTERNATIONAL ATOMIC ENERGY AGENCY, Objective and Essential Elements of a State's Nuclear Security Regime, IAEA Nuclear Security Series No. 20, IAEA, Vienna (2013).

[2] INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Recommendations on Radioactive Material and Associated Facilities, IAEA Nuclear Security Series No. 14, IAEA, Vienna (2011).

[3] INTERNATIONAL ATOMIC ENERGY AGENCY, Security of Radioactive Material in Use and Storage and of Associated Facilities, IAEA Nuclear Security Series No. 11-G (Rev. 1), IAEA, Vienna (2019).

[4] INTERNATIONAL ATOMIC ENERGY AGENCY, Code of Conduct on the Safety and Security of Radioactive Sources, IAEA/CODEOC/2004, IAEA, Vienna (2004).

[5] FOOD AND AGRICULTURE ORGANIZATION OF THE UNITED NATIONS, INTERNATIONAL ATOMIC ENERGY AGENCY, INTERNATIONAL CIVIL AVIATION ORGANIZATION, INTERNATIONAL LABOUR ORGANIZATION, INTERNATIONAL MARITIME ORGANIZATION, INTERPOL, OECD NUCLEAR ENERGY AGENCY, PAN AMERICAN HEALTH ORGANIZATION, PREPARATORY COMMISSION FOR THE COMPREHENSIVE NUCLEAR-TEST-BAN TREATY ORGANIZATION, UNITED NATIONS ENVIRONMENT PROGRAMME, UNITED NATIONS OFFICE FOR THE COORDINATION OF HUMANITARIAN AFFAIRS, WORLD HEALTH ORGANIZATION, WORLD METEOROLOGICAL ORGANIZATION, Preparedness and Response for a Nuclear or Radiological Emergency, IAEA Safety Standards Series No. GSR Part 7, IAEA, Vienna (2015).

[6] INTERNATIONAL ATOMIC ENERGY AGENCY, Security of Radioactive Material in Transport, IAEA Nuclear Security Series No. 9-G (Rev. 1), IAEA, Vienna (2020).

[7] INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Culture, IAEA Nuclear Security Series No. 7, IAEA, Vienna (2008).

[8] INTERNATIONAL ATOMIC ENERGY AGENCY, Preventive and Protective Measures against Insider Threats, IAEA Nuclear Security Series No. 8-G (Rev. 1), IAEA, Vienna (2020).

[9] INTERNATIONAL ATOMIC ENERGY AGENCY, Security of Nuclear Information, IAEA Nuclear Security Series No. 23-G, IAEA, Vienna (2015).

[10] INTERNATIONAL ATOMIC ENERGY AGENCY, Guidance on the Import and Export of Radioactive Sources, 2012 Edition, IAEA/CODEOC/IMP EXP/2012, IAEA, Vienna (2012).

Annex I

EXAMPLE ELEMENTS OF A BACKGROUND CHECK

I–1. The security manager of the facility reviews and re-evaluates the background checks for the facility personnel. The nature and depth of background checks is proportionate to the security level of the radioactive material (i.e. more thorough background checks for radioactive material assigned to a higher security level) and in accordance with the State's regulations or as determined by the regulatory body. This annex provides an example of the elements of such a background check.

CONFIRMATION OF IDENTITY

I–2. Authenticate an individual's identity to confirm that the name and personal details of the individual in question are correct. Consider the following:

— Security concern: False or misleading identification information deliberately supplied by the applicant has to be considered a major, potentially disqualifying security concern.
— Potentially mitigating factors: Confusion created by legal name changes, marriages, divorces or cultural factors (e.g. concerning name conventions).

VERIFICATION OF EMPLOYMENT HISTORY AND EDUCATION

I–3. Verify education and periods of employment provided in the applicant's personal history. Where possible, interview previous employers and associates and seek to obtain information concerning the individual's honesty, character, conduct and reliability. Consider the following:

— Security concern: False or misleading identifying information deliberately supplied by the applicant has to be considered a major, potentially disqualifying security concern. Derogatory information obtained during interviews has to be corroborated before it is considered to be disqualifying.

REVIEW OF CRIMINAL HISTORY

I–4. Evaluate records contained in law enforcement criminal records databases or counter terrorism databases. Consider the following:

— Security concern: Past or current criminal activity creates doubts about a person's judgment, reliability, trustworthiness and willingness to follow the rules and regulations that protect radioactive material or sensitive information.
— Disqualifying security concerns might include records of a severe crime or various less significant offences or other violations of concern and/or failure to respond court trials to convincingly clarify any allegations.
— Conditions that could mitigate security concerns could include the time elapsed since the criminal behaviour happened, or whether it happened under such unusual circumstances that it is unlikely to recur and does not cast doubt on the individual's reliability, trustworthiness or good judgment. There could be a situation where the person was pressured or coerced into committing the act, and those pressures are no longer present in the person's life and the evidence of successful rehabilitation is obvious. Age and maturity of the person at the time of the criminal conduct could also be considered as a mitigating condition.

REVIEW OF FINANCIAL HISTORY

I–5. Evaluate the applicant's financial responsibility based on relevant information supplied by the applicant, for example credit history reports from established credit agencies. Poor financial history of an individual handling sensitive information or material might be a risk for being engaged in illegal acts to generate funds. Consider the following:

— Security concern: Meeting financial obligations leading to delinquency that can affect the individual's reliability, trustworthiness and ability to take care of classified information. Conditions that could raise a security concern might also include deceptive or illegal financial practices such as embezzlement, employee theft, check fraud and other intentional financial breaches of trust, and financial problems that are linked to drug abuse, alcoholism, gambling problems or other issues of security concern.
— Conditions that could mitigate security concerns include the occasional or very rare occurrence of financial problems under circumstances that are unlikely to recur; cases where the individual initiates good faith recovery efforts to maintain the necessary level of trustworthiness.

PERSONAL REFERENCES TO DETERMINE THE INTEGRITY, CHARACTER AND RELIABILITY OF EACH RELEVANT EMPLOYEE

I–6. Complete reference checks to determine the character and reputation of the individual who has applied for unescorted access. To the extent possible, obtain independent information to validate the information provided by the individual (e.g. seek references not supplied by the individual). Consider the following:

— Security concern: Derogatory information revealing personal or professional conduct involving questionable judgment, lack of candour, dishonesty or unwillingness to comply with rules and regulations can raise questions about an individual's reliability, trustworthiness and ability to protect radioactive material or sensitive information.
— Conditions that could raise a security concern and might be disqualifying include breach of confidentiality, unauthorized release of sensitive information relating to radioactive material and associated facilities, other inappropriate behaviours such as deliberate omission, concealment or falsification of relevant facts, or personal history disclosure used to determine employment qualifications or determine trustworthiness or eligibility for unescorted access.
— Conditions that could mitigate security concerns include restoration of trustworthiness while declining to act inadequately upon being aware of the consequences in doing so and cases where the individual has recognized to change the behaviour and is willing to take other positive steps to alleviate the circumstances or factors that caused the untrustworthy behaviour.

Annex II

EXAMPLE FACILITY TRAINING PROGRAMME FOR THE SECURITY OF RADIOACTIVE MATERIAL IN USE AND STORAGE

II–1. This annex provides a brief description of different types of training that could form part of a facility training programme for the security of radioactive material in use and storage and of associated facilities.

FACILITY SECURITY AWARENESS TRAINING

II–2. The audience for this training includes all staff who work at the facility and other staff who do not work at the facility, but interact regularly with the facility. It will be conducted annually. The prerequisite for attending this training is familiarity with the facility's operational context.

II–3. Proposed learning areas include the following:

(a) Threats and the need to protect radioactive material at the facility;
(b) Legal and regulatory requirements for the security of radioactive material;
(c) General concepts of security systems and examples of their application to the physical protection and security management at the facility;
(d) Outline of the security plan with emphasis on the facility security organization, the role of all staff in security and relevant operating procedures;
(e) Nuclear security culture.

TRAINING FOR FACILITY PERSONNEL WITH SPECIFIC ROLES AND RESPONSIBILITIES FOR SECURITY

II–4. The audience for this training includes staff with specific operational roles or responsibilities for or affecting security, usually as identified in the security plan and associated procedures. It will be conducted initially upon assignment to the position and then annually as a refresher. The prerequisites for this training are attendance at the facility security awareness training and assignment of a specific operational responsibility for security at the facility.

II–5. Proposed learning areas include the following:

(a) Overview of the design and operation of the security system;
(b) The functions of the physical protection measures at the facility and the operation of the equipment performing the functions, particularly for timely detection and response (on-the-job training in specific security procedures might be needed in addition);
(c) The application of each of the elements presented in Section 3 of this publication, including facility staff roles and responsibilities in the relevant procedures (on-the-job training in specific security procedures might be needed in addition);
(d) Topics covering the means to operationally ensure that the security system is effective and integrates equipment, people, plans and procedures, the role of the security plan and regulatory compliance in ensuring effectiveness and the development and maintenance of nuclear security culture.

TRAINING FOR SECURITY GUARDS AND OTHER RESPONSE PERSONNEL

II–6. The audience for this training includes the operator's security guards and the off-site response personnel of other organizations. It will be conducted initially upon assignment to the position and then annually as a refresher. The prerequisites for this training are attendance at the facility security awareness training, as well as requisite training and qualifications, such as those in guarding, self-defence, tactical response and use of response equipment.

II–7. Proposed learning areas include the following:

(a) Threats, threat assessment and the motivation and objectives of adversary groups (including classroom exercises);
(b) The facility's measures for access control and lock and key control;
(c) Assessment and response to facility alarm annunciations and other indications of intrusion and the application of the concept of timely detection and response;
(d) Guard and off-site response force organizations' roles, responsibilities, operations and communications in relation to, and arrangements with, the operating organization.

Annex III

EXAMPLE OF A PERFORMANCE TEST PLAN FOR KEY CONTROL

III–1. This annex provides an example of a performance test plan for key control for a security system for radioactive material in use and storage and of associated facilities.

TEST OBJECTIVE

III–2. The test objective is to determine whether security keys are being properly accounted for, controlled by the person responsible for the keys and inventoried to prevent loss or unauthorized use.

APPLICABLE REQUIREMENTS

III–3. The applicable requirements for the performance test plan for key control are the following:

— National regulations for the security of radioactive material [indicate applicable articles];
— Facility security plan [indicate applicable sections of the security plan].

TEST PROCEDURES AND CONDITIONS

III–4. This test will be conducted during operating hours. The assessor will review the security key inventory and will select a given number of keys. The status of each key will be noted (in secure storage or in possession of a custodian — that is, a person authorized to possess the key). The assessor and a facility representative will physically locate each selected key to verify the status of each key. If a custodian does not possess his or her assigned keys or if a key is not in secure storage, the assessor will begin an inquiry to determine the location of any missing keys.

III–5. The assessor will also select two custodians and will record the serial numbers of all security keys in their possession. The assessor will then compare

these serial numbers to the inventory to determine if a custodian is in possession of a security key that has not been properly documented on the inventory.

EVALUATION CRITERIA

III–6. All keys selected in the test have to be located (either in secure storage or in the possession of a custodian). If a key cannot be located, the result of the performance test will be considered as 'FAIL' (Table III–1). All keys have to be physically presented to the assessor.

TEST CONTROLS

III–7. Keys selected for this performance test will be selected at the time of the test. No advance notification will be provided to identify the keys to be selected for the test. No other controls are necessary.

RESOURCE NEEDS

III–8. Two key custodians are needed for the conduct of the test: one assessor and a facility representative.

TABLE III–1. EVALUATION CRITERIA FOR THE PERFORMANCE TEST FOR KEY CONTROL

Performance test	Result of performance test
All keys have been identified on the inventory and signed for by the correct custodian	PASS/FAIL
Each person responsible for the key possesses it and/or the key is properly secured	PASS/FAIL
A record exists that demonstrates a key has been returned	PASS/FAIL
All keys in the possession of a custodian are accounted for on the inventory record	PASS/FAIL

TEST COORDINATION NEEDS

III–9. Coordination will be needed from the following personnel:

— Assessment team leader;
— Facility representative;
— Facility safety officer.

APPROVAL

III–10. Signatures of the approvers:

Assessment Team Member: _____ Date: _____

Inspection Team Leader: _____ Date: _____

Facility Safety Officer: _____ Date: _____

APPENDICES

[Provide or list the procedures stated in the security plan, including their dates and version.]

Annex IV

EXAMPLE OF A SECURITY PLAN FOR A UNIVERSITY MEDICAL CENTRE

INTRODUCTION

IV–1. This security plan documents the security system that is designed to meet the regulatory requirements. It addresses design, operation and maintenance of the security system for the protection of radioactive material at a University Medical Centre, including security management measures.

Requirements

IV–2. This security plan has been prepared in accordance with [article or annex of applicable regulations]. All references to articles in this document refer to articles within the regulations on the security of radioactive material issued by the national regulatory body, unless otherwise specified.

Objective of the security plan

IV–3. The objective of this security plan is to describe the overall nuclear security system in place to protect the radioactive material, including the measures to address increased threat level, response to nuclear security events, and protection of sensitive information in order to demonstrate regulatory compliance.

Scope

IV–4. This security plan applies to all operations involving the use or storage of Category [1, 2 and/or 3, as applicable] radioactive sources at the University Medical Centre. In accordance with [article of applicable regulations], nothing in this security plan or within the security measures indicated by this security plan will be implemented to the detriment of other applicable radiation protection and safety measures, contained in safety and environmental regulations, as documented in [facility's health and safety plan and other applicable facility documents].

Preparing and updating the security plan

IV–5. This security plan was developed in accordance with the national regulations and reviewed and approved by the national regulatory body for radioactive material.

IV–6. The security plan will be updated as necessary to reflect circumstances affecting its continuing effectiveness, including when the type or location of radioactive material changes, when there are changes in facility operations or the security system, or when necessary to address new threat information or new security regulations.

IV–7. Updates to the security plan will be reviewed and approved by the regulatory body for radioactive material.

FACILITY DESCRIPTION

IV–8. This section describes the radioactive material that needs to be protected and its location at the University Medical Centre, the level of protection required, and the physical and operational environments that affect such protection.

Overview

IV–9. The University Medical Centre diagnoses and treats cancer patients with a variety of methods, including chemotherapy, teletherapy, brachytherapy and surgery. The radioactive material used by the facility is described in Table IV–1.

Radioactive material

(See Table IV–1.)

Categorization and security level of radioactive material

IV–10. The cobalt-60 teletherapy unit is assigned to Category 1 and the iridium-192 brachytherapy unit is assigned to Category 2, in accordance with [article or annex of applicable regulations], which requires that all teletherapy units have a high level of protection of radioactive material against unauthorized removal and that all high and medium dose rate brachytherapy units have an intermediate level of protection of radioactive material against unauthorized removal. Figure IV–1 describes the layout of the facility.

TABLE IV–1. RADIOACTIVE MATERIAL USED AT THE FACILITY

Device	Device serial number	Isotope	Source serial number	Initial activity (reference date)	Category and security level
Teletherapy unit	70008UFGY901	Cobalt-60	92356000HS65	150 TBq (15 January 2013)	Category 1 Security Level A
Brachytherapy unit	5492BJH87U99	Iridium-192	3817AL8HX09	0.44 TBq (Maximum activity)	Category 2 Security Level B

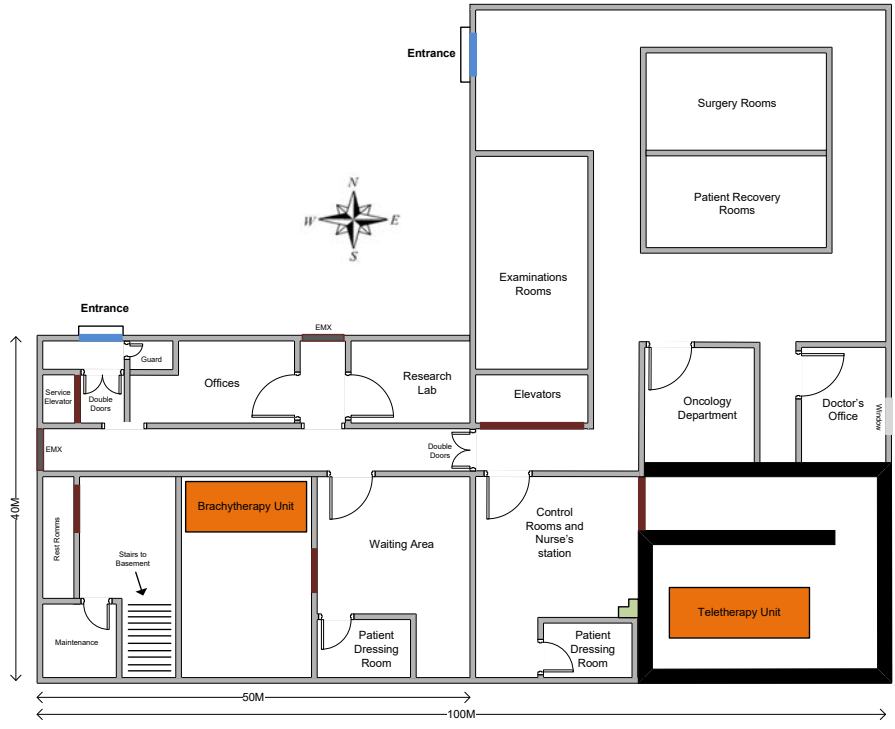


FIG. IV–1. [Name of facility] facility layout.

Physical description

IV–11. The layout of the surrounding environment of the [name of facility] is shown in Fig. IV–2.

Operational description

IV–12. The University Medical Centre is open 08:00–17:00 and Monday through Friday, with staff present in the facility 07:00–18:00 daily. The staff includes the centre director, two doctors, the security manager, four security guards, a radiation protection officer, four nurses, four medical technicians, and two receptionists. The clinic receives between 30 and 40 patients per day, usually with five patients in the facility per hour. Anyone from the public can walk into the facility, but it is rare to have non-patient visitors.

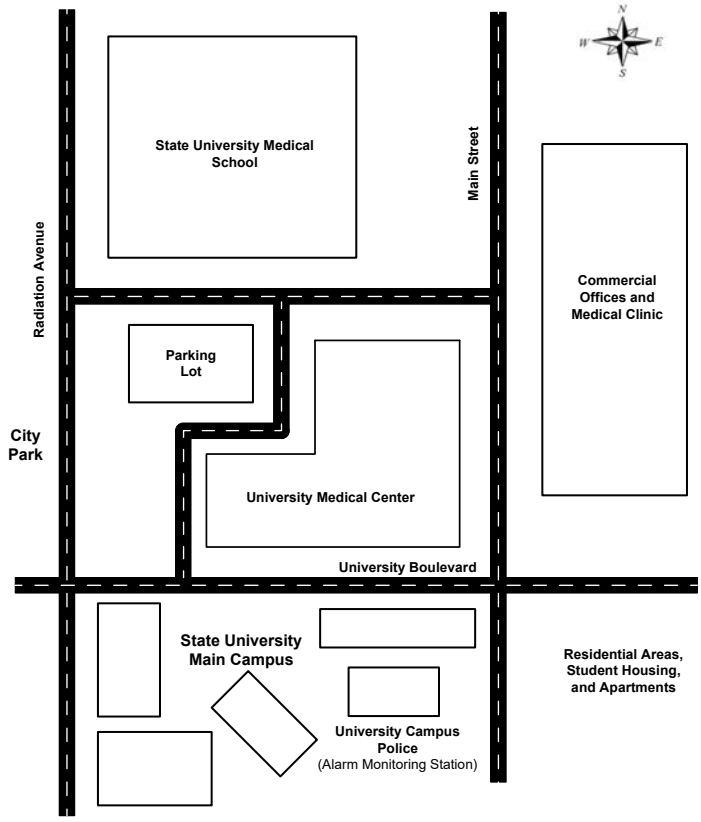


FIG. IV–2. Surrounding environment of the facility.

SECURITY MANAGEMENT

IV–13. This section describes the security management measures in place at the University Medical Centre and the security related duties of management and staff.

Roles and responsibilities

IV–14. Each person working at the University Medical Centre has a responsibility to be vigilant against potential threats, to understand all relevant security policies and procedures, to report any identified security risks to the proper entities, and to respond to security concerns defined in the University Medical Centre Security Policy and outlined in this security plan.

IV–15. Additional specific responsibilities of the staff with respect to security of radioactive material are described in Table IV–2, whereas Fig. IV–3 provides the security organization organogram.

TABLE IV–2. STAFF WITH SECURITY RESPONSIBILITIES

Position	Security responsibilities
Medical centre director	Establish security policy for the University Medical Centre Approve security processes and procedures Ensure that the University Medical Centre meets all applicable security requirements
Security manager	Develop all security processes and procedures according to security policies and regulatory requirements Recruit qualified staff and provide security training Prepare and periodically review, update and submit for approval the security plan Prepare the security response plan in conjunction with the local law enforcement commander Oversee design, day-to-day operation and sustainability of security system Supervise security guards
Security guards	Operate central alarm station Escort security contractors Conduct regular patrols Summon off-site response to security incident and take other actions in accordance with the security response plan

TABLE IV–2. STAFF WITH SECURITY RESPONSIBILITIES (cont.)

Position	Security responsibilities
Radiation protection officer	Oversee day-to-day operation of the radiotherapy programme Conduct and manage inventory of radioactive material Develop accounting processes and measures Supervise medical technicians and nurses
Medical technicians	Understand and follow applicable security procedures
Nurses	Understand and follow applicable security procedures

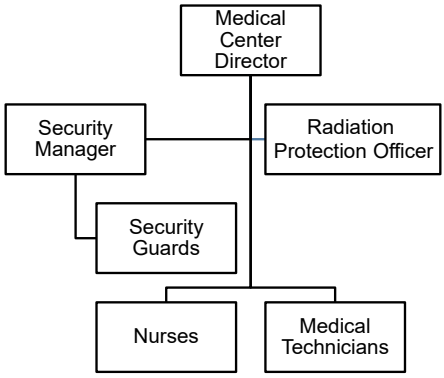


FIG. IV–3. Security organization of the facility.

Training and qualification

IV–16. Training types and frequencies of refresher trainings for the facility staff are presented in Table IV–3.

IV–17. The security manager is responsible for ensuring that each employee has the necessary qualifications before assumption of security related duties, that the necessary training is scheduled, conducted and successfully completed, and that records of the foregoing are maintained.

TABLE IV–3. QUALIFICATION AND TRAINING REQUIREMENTS FOR STAFF

Position	Security qualifications	Training type	Training frequency	Training provider
All staff	No specific security qualifications	Basic security awareness training	Annually	Security manager
Security manager	Certified physical security professional	Certified physical security professional refresher training Basic instructor training	Upon employment and as required to maintain certification	Certified training institute
Security guards	Two years in law enforcement or equivalent	Security guard training Central alarm station operation	Upon employment and annually thereafter	Vendor
Radiation protection officer	No specific security qualifications	Facility security training and awareness	Upon employment and annually thereafter	Security manager
Nurses	No specific security qualifications	Facility security and awareness training	Upon employment and annually thereafter	Security manager
Medical technicians	No specific security qualifications	Facility security and awareness training	Upon employment and annually thereafter	Security manager

Access authorization

IV–18. Unescorted access to radioactive source locations, secured areas and/or security sensitive information is limited to those who need such access to perform their duties. Unescorted access is only authorized when the security manager has verified that the individual has a need for unescorted access, has passed the relevant background check, and is up-to-date on the relevant training.

IV–19. Individuals in the following positions need unescorted access to the radioactive source location:

— Doctors;
— Radiation protection officer;
— Nurses;
— Medical technicians.

IV–20. Individuals in the following positions need unescorted access to the central alarm station:

— Security manager;
— Security guards.

IV–21. Individuals in the following positions need unescorted access to all security sensitive information:

— Director;
— Security manager;
— Radiation protection officer.

IV–22. The security manager will review and re-evaluate the training records and background checks annually to ensure that staff training is up-to-date and that no staff without proper authorization have unescorted access. This review will also be conducted on an as-needed basis when staff change jobs, staff have new job responsibilities or there is termination of employment.

IV–23. All computerized systems for access will be programmed to remove access every six months unless the security manager reconfirms that a given staff member still needs to have access.

Trustworthiness

IV–24. In accordance with article XXX of applicable regulations, the trustworthiness of all personnel identified as needing unescorted access to radioactive sources, secured areas and/or security sensitive information will be verified prior to grant of access and again every two years. The trustworthiness is verified by the following means, as outlined in procedure ABC.

— An identity verification;
— A review of record of previous employment;

— A criminal record check.

IV–25. Records of the individuals whose trustworthiness needs to be verified and the results of those verifications are retained for a minimum of five years and kept confidential.

Information protection

IV–26. In accordance with article XXX of applicable regulations, all information pertaining to the following topics is considered sensitive security information, whether in hard copy or electronic form:

— Employee background checks and their results;
— Security system design;
— Inventory of radioactive material;
— Security system weaknesses and results of security evaluations;
— Security plan.

IV–27. Procedure XYZ, established to protect sensitive information, outlines the following:

— Such information will be marked ‘CONFIDENTIAL’.
— Protected information will be stored in locked filing cabinets, which will remain locked at all times when they are not in use.
— When protected information is stored on a computer, each protected file will be encrypted or password protected and the computer will be programmed to automatically lock and request a password to unlock the computer.
— The computer will have installed a firewall and the latest version of antivirus software.
— Only those personnel having authorized access to security sensitive information will have access to that information and only so long as such information is necessary in order to perform their job.
— All electronic communications containing protected information will be encrypted or otherwise password protected. When transporting protected information in hard copy, the documents will have a cover page or will be in an envelope or folder to prevent unauthorized persons from seeing the contents.
— Protected information in paper form will be destroyed when it is no longer needed by the authorized person. All paper documents will be shredded. Electronic information will be destroyed.

Maintenance programme

IV–28. Security system maintenance is provided by ABC vendor. As provided in the maintenance contract, for the duration of the contract, the contractor checks all equipment to determine, on quarterly basis, whether the equipment works and replaces any item that is faulty.

IV–29. Contractor maintenance checks include the following:

(a) Inspecting electronic components and connections;
(b) Battery checks and replacements;
(c) Voltage checks and comparisons;
(d) Cleaning of appropriate electronic components;
(e) Performance testing of equipment;
(f) System adjustments for peak performance.

IV–30. If any equipment fails between quarterly visits, the contractor will replace that as well. In addition, the contractor provides the following services as provided in the contract:

(a) Unlimited replacement parts;
(b) Temporary substitution parts as needed (loaner parts);
(c) On-site response within 24 hours of notification;
(d) Unlimited local telephone support;
(e) Unlimited unplanned visits;
(f) Maintenance and warranty records for the site.

IV–31. All personnel are obligated, through security procedure AXY, to report observed problems with the security system to the security manager, who will notify the contractor.

Budget and resource planning

IV–32. The security manager establishes objectives and goals for the security system. Each year, the security manager determines the resources necessary for the effective operation and maintenance of the security system, including the following:

(a) Equipment purchase;
(b) Human resources;
(c) Training;

(d) Operational costs of the security system;
(e) Equipment maintenance;
(f) All other activities relating to the security of radioactive sources.

IV–33. The security manager submits a request to the centre director for the necessary financial and other resources.

IV–34. The centre director acts on this request through the regular budgeting and resource planning process of the organization.

IV–35. As part of the evaluation process described below, the security manager reviews the expenditure of resources against budget and resource projections and ensures that actions are taken to address any deviations that might arise.

Evaluation for compliance and effectiveness

IV–36. The security manager develops and implements an annual security evaluation for compliance with the applicable regulatory requirements and for effectiveness in protecting the facility's radioactive material.

IV–37. The scope of the evaluation addresses both the security system and security management measures.

IV–38. Following the completion of the evaluation, the security manager compiles the results and prepares an evaluation report that includes the following:

(a) The scope of the evaluation;
(b) The methods employed in the evaluation;
(c) The issues identified and their suspected causes;
(d) The conclusions of the evaluation;
(e) Recommendations for follow-up action.

IV–39. The recommendations for follow-up action will include the following:

(a) Any results that have to be reported immediately to the regulatory body;
(b) Other actions that have to be taken;
(c) Identification of who is responsible for each action;
(d) When each action has to occur;
(e) Responsibility for confirmation and documentation that each action has been taken.

IV–40. The security manager reviews the results with the centre director and adjusts any follow-up actions as directed.

SECURITY SYSTEM

IV–41. This section describes the security system designed and implemented at the University Medical Centre in order to protect the facility's radioactive material, consistent with national regulations for the security of radioactive material.

Threat information

IV–42. The regulatory body provides general information to the University Medical Centre regarding the threat that the security system has to be designed to protect against. If the security manager is notified about specific or increased threat, the security manager shares this information by secure means (usually an in-person meeting) with those facility staff who are authorized to receive security sensitive information and have a need to know.

IV–43. The regulatory body for the security of radioactive material has provided a representative threat statement. Based on this, the capabilities of the external and insider threats were addressed through the technical and administrative measures of the security system. Specifically, the response plan addresses the number of external adversaries and their weapons. The technical security measures were selected to counter the capabilities, tools, skills and training of the external and insider adversaries. Further, administrative measures were developed to adequately identify and report suspicious activity.

Security assessment methodology

IV–44. In order to design the security system, the following approach was employed:

(1) Security layers were selected around the targets to minimize access;
(2) Access controls were placed on the layers considering the threats and operations;
(3) Barriers were installed and balanced to strengthen the boundary of the layers to adequately delay any attempted penetration through the layers;
(4) Balanced detection and assessment were provided around the security layers to detect any attempted penetration (ensuring timeliness by preceding delay);

(5) All electronic information (i.e. access control, detection assessment) was routed to the central alarm station;
(6) Security procedures were developed and personnel were trained to ensure the smooth integration between people and equipment;
(7) Performance tests were conducted to assure that the equipment and people performed as intended.

Security system design

IV–45. Based on the regulations, the teletherapy and brachytherapy units required two layers of security. Therefore, two security layers enclosing two security areas were established around both the teletherapy and brachytherapy sources. The barriers comprising the boundary of the security layers around the teletherapy unit, in accordance with a graded approach as outlined in the regulations, are more robust than those surrounding the security layer for the brachytherapy unit. The security system designs for the teletherapy unit and the brachytherapy unit are shown in Figs IV–4, IV–5 and IV–6. Details of access control, detection, delay and response measures and security procedures are described in the subsequent text.

Access control

IV–46. In accordance with article XXX of the applicable regulations for the security of radioactive material, the following access control measures are in place and are documented in procedure YZZ.

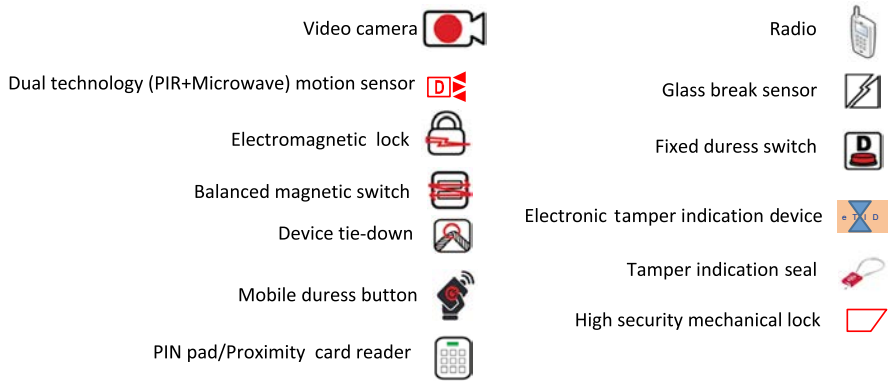


FIG. IV–4. Security measures employed in the security system.

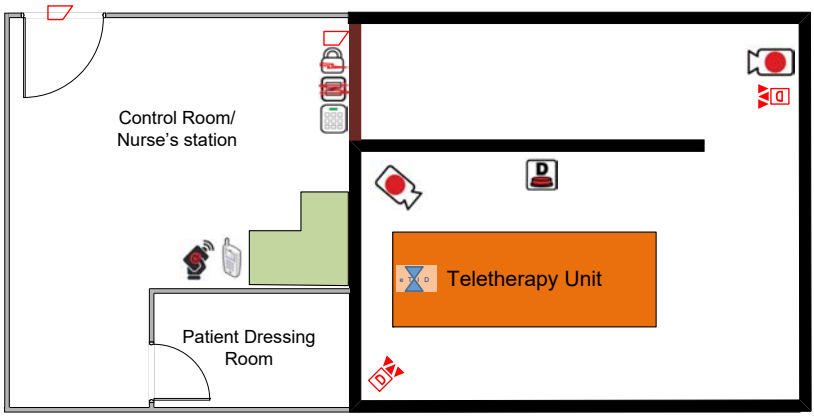


FIG. IV–5. Security system protecting the teletherapy unit.

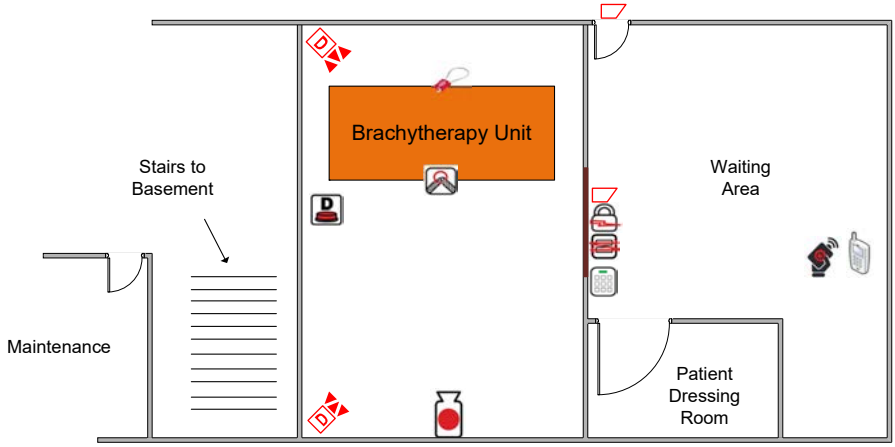


FIG. IV–6. Security system protecting the brachytherapy unit.

(a) Teletherapy unit:

(i) The teletherapy door is a steel plated lead lined security door with protected high security hinges and mechanical steel bolts thrown into the steel door jamb and ceiling. Further a high security electromagnetic lock secures the door.

(ii) For access to the teletherapy unit, the mechanical bolts are released by a mechanical level handle that is secured with a high security key. The electromagnetic lock is released upon receipt of an authorized personal identification number (PIN) and proximity card.

(iii) During non-business hours, the door to the teletherapy treatment room is locked by both high security mechanical and electromagnetic locks that demand the use of a high security key, a proximity card and a PIN to allow access. A balanced magnetic switch on the door and an internal motion sensor are activated to detect unauthorized entry.

(iv) During business hours, the door to the teletherapy treatment room is unlocked, but is under continuous observation by trained staff equipped with a mobile duress button. Patients and other non-authorized persons may enter only if accompanied by staff with authorized access.

(b) Brachytherapy unit:

(i) During non-business hours, the door to the brachytherapy treatment room is also locked by high security mechanical lock and electromagnetic lock that demand the use of a high security key, a proximity card and a PIN to allow access. During non-business hours, a balanced magnetic switch on the door and an internal motion sensor are activated to detect unauthorized entry.

(ii) During business hours, the door to the brachytherapy treatment room is unlocked, but is under continuous observation by trained staff equipped with a mobile duress button. Patients and other non-authorized persons may enter only if accompanied by staff with authorized access.

Detection (including assessment) and delay measures

IV–47. The security systems consist of the following detection, assessment and delay measures (see procedures X, Y and Z):

(a) Teletherapy unit:

(i) Detection: During non-business hours, detection of unauthorized access to the teletherapy treatment room is provided by a balanced magnetic switch on the door and a dual technology motion sensor located inside the treatment room. During business hours, detection is provided through continuous observation by trained staff equipped with a mobile duress button and a radio transmitter. The electronic tamper indication device remains armed 24 hours. A fixed duress switch is also installed in the treatment room.

(ii) Assessment: During non-business hours alarms from the sensors are communicated to the central alarm station of the University Medical Centre. The security guard at the central alarm station views the video images from the cameras located in the treatment room to determine whether an intruder might be present. If so, the security

guard summons the local police. During business hours, assessment is provided by staff concurrently with detection by observation. If an intruder is present, the staff member summons the police by the mobile duress button, radio or fixed duress switch.

(iii) Delay: Means of delay include the hardened door to the treatment room equipped with an electromagnetic lock and the housing of the teletherapy unit itself (which has to be partially disassembled to remove the radioactive source).

(b) Brachytherapy unit:

(i) Detection: During non-business hours, detection of unauthorized access to the brachytherapy treatment room is provided by a balanced magnetic switch on the door and a dual technology motion sensor located inside the treatment room. During business hours, detection is provided through continuous observation by trained staff equipped with a mobile duress button and a radio transmitter. A fixed duress switch is also installed in the treatment room.

(ii) Assessment: During non-business hours, alarms from the sensors are communicated to the central alarm station of the centre. The security guard at the central alarm station views the video images from the cameras located in the treatment room to determine whether an intruder might be present. If so, the security guard summons the local police. During business hours, assessment is provided by staff concurrently with detection by observation. If an intruder is present, the staff member summons the police by the mobile duress button, radio or fixed duress switch.

(iii) Delay: Means of delay include the hardened door to the treatment room equipped with an electromagnetic lock and a fastening of the brachytherapy unit to the floor.

SECURITY PROCEDURES

IV–48. In addition to the procedures for the actions described above, this section summarizes the procedures used by staff to operate and maintain the security system. The full written procedures are included in separate documents issued to assigned staff.

Routine, off-shift and emergency response

IV–49. Assigned staff have different responsibilities and follow different procedures during business hours, non-business hours and emergency response.

During business hours, sensors are deactivated and medical staff assume the primary responsibility for detecting and assessing the presence of intruders and summoning a response. During non-business hours, sensors are activated and alarm monitoring staff are responsible for assessing the cause of an alarm and summoning a response.

Opening and closing of facility

IV–50. At the beginning of each business day, two security guards open the doors to the teletherapy and brachytherapy treatment rooms and deactivate the sensors. They then conduct an examination of the treatment room and the device to verify the absence of any signs of intrusion or tampering with delay mechanisms or the device, confirm that the assigned medical staff responsible for controlling access during business hours are present and are properly equipped with the necessary communications equipment and report these actions to the central alarm station.

IV–51. At the end of each business day, two security guards confirm that the medical staff no longer have the need to access the treatment room and verify that the device is appropriately secured. They then activate the sensors, lock the treatment room doors and report these actions to the alarm monitoring station.

Key and lock control

IV–52. Upon determination by the security manager that a staff member is authorized for unescorted access to radioactive material locations and/or secured areas, the security manager will issue the staff member a proximity card and a PIN. All user PINs are reset every 12 months, or more frequently in the event of a compromise of a combination or a PIN, loss of a security key or termination of a staff member's access.

IV–53. The security manager is responsible for collecting proximity cards when a staff member's access authorization changes. In addition, the security manager needs to verify every six months that each user qualifies for continued access to the facility so that the proximity card and PIN can continue to be valid. In the event that continued access is not verified within six months, the system is programmed to deny personnel access until their authorization for access is confirmed.

Accounting and inventory

IV–54. In accordance with article XXX of applicable regulations, the University Medical Centre performs periodic accounting for radioactive material and establishes and maintains a radioactive material inventory as follows:

(a) Accounting: The [radiation protection officer or other designated position] verifies the presence of the teletherapy source daily and the presence of the brachytherapy sources weekly. These verifications are performed by examination of the device to confirm the absence of tampering and by review of radiation monitoring measurements. The [radiation protection officer or other designated position] enters the results of each check on a hard copy accounting log for the source immediately after performing the verification. If the presence of the radioactive source cannot be verified, the radiation protection officer immediately notifies the security manager, the regulatory body and the local police or other designated response authority.

(b) Inventory: The [radiation protection officer] maintains an inventory of radioactive sources at the University Medical Centre, which contains the following information on each radioactive source:
    (i) Location of the source;
    (ii) Radionuclide;
    (iii) Radioactivity on a specified date;
    (iv) Serial number or unique identifier;
    (v) Chemical and physical form;
    (vi) Radioactive source use history and any internal movements, as applicable;
    (vii) Date and origin or destination of receipt, transfer or disposal of the radioactive source.

IV–55. The radiation protection officer verifies the accuracy of the inventory annually and adjusts the information on each radioactive source within 30 days of any change.

Receipt and transfer

IV–56. When receiving or transferring radioactive material, the security manager will arrange for compensatory security measures appropriate for the category of the material. Such measures might include the staffing of additional security guards to protect the material while outside a secured facility location or transport vehicle, and coordination with the local police force so that they are aware the transfer is being made. When transferring radioactive material to an

outside entity, the security manager will first verify with the regulatory body that the entity has the necessary authorization to handle that material.

RESPONSE

IV–57. This section describes arrangements for responding to a nuclear security event.

Security events

IV–58. The security manager has overall responsibility for making arrangements for the response to a security event and has made the following arrangements:

(a) Contacted the police with the assistance of the regulatory body and arranged a visit to the University Medical Centre for familiarization with the facility's radioactive material and associated equipment and devices, security system and security management measures.
(b) Confirmed the means by which the facility will notify the police following detection and assessment of an alarm.
(c) In coordination with the regulatory body, discussed with the police the threat that responders have to be prepared to counter.
(d) Obtained from the police the estimated response time and modified the security system as necessary to provide sufficient delay to enable a timely response.
(e) Reached agreement with the police on any specific actions to be taken by facility staff to facilitate a response.
(f) Arranged for exercises of these arrangements for response to a security event.

Communications

IV–59. The University Medical Centre employs the following means to communicate with the police:

(a) Phones;
(b) Fixed duress switches;
(c) Radios;
(d) Landline telephones;
(e) Cell phones.

IV–60. All of these are programmed to enable immediately communication to [local law enforcement or other designated response authority] that a nuclear security event is or might be occurring at the facility.

Security event reporting

IV–61. Following a security event, the security manager is responsible for drafting a report on what occurred. The report is provided to the regulatory body within 60 days after the incident, as required by article XXX of the applicable regulations. The security manager will work together, with the response or security organization as necessary, to understand how the security event occurred and to determine what improvements have to be made to the security of the facility.

Nuclear security during emergencies and contingencies

IV–62. To the extent feasible without endangering personnel safety, in the event of a non-security conventional emergency such as fire, earthquake, flood or hurricane, [designated staff with access to the radioactive source] will ensure that all the teletherapy and brachytherapy devices are appropriately secured and the treatment room doors are locked.

IV–63. In the event of failures in the security system, responsible staff will implement the compensatory measures.

Increased threat level

IV–64. In accordance with article XXX of applicable regulations, when the facility becomes aware of a heightened threat level, the security manager will determine what immediate steps can be taken to increase security in order to meet the increased threat level. Immediate measures might include deploying additional security guards, changing PINs, alerting staff to additional risks, testing security equipment and meeting with local police to develop and review response plans. Modification of the security system will also be considered as necessary, such as installing additional security cameras, new and/or additional locks, new and/or additional alarm systems or other measures, such as structural changes to the facility to better secure sources. The measures will be adopted as quickly as possible.

IAEA
International Atomic Energy Agency

No. 26

ORDERING LOCALLY

IAEA priced publications may be purchased from the sources listed below or from major local booksellers.

Orders for unpriced publications should be made directly to the IAEA. The contact details are given at the end of this list.

NORTH AMERICA

Bernan / Rowman & Littlefield
15250 NBN Way, Blue Ridge Summit, PA 17214, USA
Telephone: +1 800 462 6420 • Fax: +1 800 338 4550
Email: orders@rowman.com • Web site: www.rowman.com/bernan

REST OF WORLD

Please contact your preferred local supplier, or our lead distributor:

Eurospan Group
Gray's Inn House
127 Clerkenwell Road
London EC1R 5DB
United Kingdom

Trade orders and enquiries:
Telephone: +44 (0)176 760 4972 • Fax: +44 (0)176 760 1640
Email: eurospan@turpin-distribution.com

Individual orders:
www.eurospanbookstore.com/iaea

For further information:
Telephone: +44 (0)207 240 0856 • Fax: +44 (0)207 379 0609
Email: info@eurospangroup.com • Web site: www.eurospangroup.com

Orders for both priced and unpriced publications may be addressed directly to:

Marketing and Sales Unit
International Atomic Energy Agency
Vienna International Centre, PO Box 100, 1400 Vienna, Austria
Telephone: +43 1 2600 22529 or 22530 • Fax: +43 1 26007 22529
Email: sales.publications@iaea.org • Web site: www.iaea.org/publications

OBJECTIVE AND ESSENTIAL ELEMENTS OF A STATE'S NUCLEAR SECURITY REGIME
IAEA Nuclear Security Series No. 20
STI/PUB/1590 (15 pp.; 2013)
ISBN 978-92-0-137810-1 Price: €20.00

NUCLEAR SECURITY RECOMMENDATIONS ON RADIOACTIVE MATERIAL AND ASSOCIATED FACILITIES
IAEA Nuclear Security Series No. 14
STI/PUB/1487 (27 pp.; 2011)
ISBN 978-92-0-112110-3 Price: €22.00

SECURITY OF RADIOACTIVE MATERIAL IN USE AND STORAGE AND OF ASSOCIATED FACILITIES
IAEA Nuclear Security Series No. 11-G (Rev. 1)
STI/PUB/1840 (105 pp.; 2019)
ISBN 978-92-0-110018-4 Price: €50.00

PREVENTIVE AND PROTECTIVE MEASURES AGAINST INSIDER THREATS
IAEA Nuclear Security Series No. 8-G (Rev. 1)
STI/PUB/1858 (37 pp.; 2020)
ISBN 978-92-0-103419-9 Price: €24.00

SECURITY OF RADIOACTIVE MATERIAL IN TRANSPORT
IAEA Nuclear Security Series No. 9-G (Rev. 1)
STI/PUB/1872 (102 pp.; 2020)
ISBN 978-92-0-105119-6 Price: €42.00

NATIONAL NUCLEAR SECURITY THREAT ASSESSMENT, DESIGN BASIS THREATS AND REPRESENTATIVE THREAT STATEMENTS
IAEA Nuclear Security Series No. 10-G (Rev. 1)
STI/PUB/1926 (39 pp.; 2021)
ISBN 978-92-0-131020-0 Price: €31.00

ENHANCING NUCLEAR SECURITY CULTURE IN ORGANIZATIONS ASSOCIATED WITH NUCLEAR AND OTHER RADIOACTIVE MATERIAL
IAEA Nuclear Security Series No. 38-T
STI/PUB/1874
ISBN 978-92-0-105319-0 (206 pp.; 2021) Price: €69.00

This publication provides guidance to States, competent authorities and operators on the security management for radioactive material in use and storage and of associated facilities, including the establishment and implementation of policies, plans, procedures and processes to ensure that the security systems is effective, reliably operated and maintained. This technical guidance sets forth security management as an essential tool to verify that personnel, procedures and equipment operate interdependently and in an integrated manner; as well as to assist leadership and personnel responsible for security to demonstrate high commitment towards promoting a robust nuclear security culture. This publication is also intended to assist regulatory bodies in establishing regulations and guidance on security management measures and to assist operators in meeting these regulatory requirements.

INTERNATIONAL ATOMIC ENERGY AGENCY
VIENNA