Nuclear Security Management for Research Reactors and Related Facilities

IAEA
International Atomic Energy Agency

IAEA NUCLEAR SECURITY SERIES AND RELATED PUBLICATIONS

IAEA guidance on 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 is provided in the **IAEA Nuclear Security Series**. Publications in this series 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.

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.

Other publications on nuclear security, which do not contain IAEA guidance, are issued outside the IAEA Nuclear Security Series.

RELATED PUBLICATIONS

The IAEA also establishes standards of safety for protection of health and minimization of danger to life and property, which are issued in the **IAEA Safety Standards Series**.

The IAEA provides for the application of guidance and standards and makes available and fosters the exchange of information relating to peaceful nuclear activities and serves as an intermediary among its Member States for this purpose.

Reports on safety and protection in nuclear activities are issued as **Safety Reports**, which provide practical examples and detailed methods that can be used in support of the safety standards.

Other safety related IAEA publications are issued as **Emergency Preparedness and Response** publications, **Technical Reports** and **TECDOCs**. The IAEA also issues reports on radiological accidents, training manuals and practical manuals, and other special safety and security related publications.

The **IAEA Nuclear Energy Series** comprises informational publications to encourage and assist research on, and the development and practical application of, nuclear energy for peaceful purposes. It includes reports and guides on the status of and advances in technology, and on experience, good practices and practical examples in the areas of nuclear power, the nuclear fuel cycle, radioactive waste management and decommissioning.

NUCLEAR SECURITY MANAGEMENT FOR RESEARCH REACTORS AND RELATED 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
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
ETHIOPIA
FIJI
FINLAND
FRANCE
GABON
GEORGIA
GERMANY
GHANA
GREECE
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
NORWAY
OMAN
PAKISTAN
PALAU
PANAMA
PAPUA NEW GUINEA
PARAGUAY
PERU
PHILIPPINES
POLAND
PORTUGAL
QATAR
REPUBLIC OF MOLDOVA
ROMANIA
RUSSIAN FEDERATION
RWANDA
SAN MARINO
SAUDI ARABIA
SENEGAL
SERBIA
SEYCHELLES
SIERRA LEONE
SINGAPORE
SLOVAKIA
SLOVENIA
SOUTH AFRICA
SPAIN
SRI LANKA
SUDAN
SWAZILAND
SWEDEN
SWITZERLAND
SYRIAN ARAB REPUBLIC
TAJIKISTAN
THAILAND
THE FORMER YUGOSLAV REPUBLIC OF MACEDONIA
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".

NUCLEAR SECURITY MANAGEMENT FOR RESEARCH REACTORS AND RELATED FACILITIES

INTERNATIONAL ATOMIC ENERGY AGENCY
VIENNA, 2016

For further information on this publication, please contact:

Nuclear Security of Materials and Facilities Section
International Atomic Energy Agency
Vienna International Centre
PO Box 100
1400 Vienna, Austria
Email: Official.Mail@iaea.org

NUCLEAR SECURITY MANAGEMENT FOR RESEARCH REACTORS AND RELATED FACILITIES
IAEA-TDL-004
ISBN 978-92-0-111315-3

Printed by the IAEA in Austria
March 2016

FOREWORD

States have responded to the risk that nuclear or other radioactive material could be used for malicious purposes by engaging in a collective commitment to strengthen the protection and control of such material and to effectively respond to nuclear security events. They have agreed to strengthen existing international legal instruments, and have established new ones, to enhance nuclear security around the world. Nuclear security management is fundamental to the use of nuclear technologies and to applications where nuclear or other radioactive material is used or transported in ways that are consistent with these commitments.

This publication is intended for use by persons responsible for the implementation of nuclear security management at research reactors and related facilities. It provides a single source of advice on developing and maintaining an effective and comprehensive nuclear security programme covering all management aspects of nuclear security for all nuclear and other radioactive material, and associated facilities on the site.

In aiming to cover all nuclear security considerations as applied to research reactors and related facilities, this publication may repeat or interpret guidance from IAEA Nuclear Security Series publications. The intention is to provide usable, comprehensive information and advice on security management in the context of research reactors and related facilities.

This publication focuses primarily on assisting operators in implementing an effective nuclear security management system, and in demonstrating the effectiveness of their nuclear security programme to the competent authority. The competent authority may also find it useful in supporting the licensing and inspection of an operator’s nuclear security systems.

The information in this publication dealing with nuclear security management at research reactors and related facilities is based on national experience and practices as well as publications in the field of nuclear security management. The advice is provided for consideration by States, competent authorities and operators.

This publication was prepared in a series of nine consultancy meetings, with input from more than 12 experts from ten Member States.

EDITORIAL NOTE

This publication has been prepared from the original material as submitted by the contributors and has not been edited by the editorial staff of the IAEA. The views expressed remain the responsibility of the contributors and do not necessarily represent the views of the IAEA or its Member States.

Neither the IAEA nor its Member States assume any responsibility for consequences which may arise from the use of this publication. This publication does not address questions of responsibility, legal or otherwise, for acts or omissions on the part of any person.

The use of particular designations of countries or territories does not imply any judgement by the publisher, the IAEA, as to the legal status of such countries or territories, of their authorities and institutions or of the delimitation of their boundaries.

The mention of names of specific companies or products (whether or not indicated as registered) does not imply any intention to infringe proprietary rights, nor should it be construed as an endorsement or recommendation on the part of the IAEA.

Security related terms are to be understood as defined in the publication in which they appear, or in the guidance that the publication supports. Otherwise, words are used with their commonly understood meanings.

An appendix is considered to form an integral part of the publication. Material in an appendix has the same status as the body text. Annexes are used to provide practical examples or additional information or explanation. Annexes are not integral parts of the main text.

The IAEA has no responsibility for the persistence or accuracy of URLs for external or third party Internet web sites referred to in this publication and does not guarantee that any content on such web sites is, or will remain, accurate or appropriate.

CONTENTS

1. INTRODUCTION

1.1. BACKGROUND

Existing IAEA Nuclear Security Series (NSS) publications do not provide specific guidance for Research Reactors and Related Facilities (RRRF). Implementing Guides address technical areas such as nuclear security culture, measures against insider threat, design basis threat (DBT) and computer security; but these are typically meant as general guidance for nuclear facilities rather than having specific application to research reactors. RRRF operators would therefore need to apply a graded approach to the general nuclear security guidance on several different topics and to take account of the particular characteristics of research reactors.

The term ‘research reactor’ is used to describe a diverse range of non-power reactors and also includes a wide variety of co-located facilities. These overall facilities are referred to as RRRF and may include: nuclear reactors; radioisotope production facilities; fuel research and fabrication facilities; storage facilities for fresh fuel, spent fuel, or radioactive sources; radioactive waste storage and disposal facilities; laboratories and hot cells; irradiation facilities; and other non-nuclear related facilities and activities.

Research reactors therefore comprise a wide variety of facilities in terms of objectives, power levels, fuel and complexity. This variety introduces different security concerns and considerations when compared with other types of nuclear facility. These concerns and considerations include, but are not limited to:

— **Diversity of designs**: Research reactors are designed to meet specific operational objectives. Sometimes, these objectives result in designs that complicate the security system.

— **Power levels**: Most research reactors have much lower thermal energies and fission product inventories than power reactors and so, typically, do not present the same hazards or risks.

— **Fuel enrichment**: Research reactors typically use a form of uranium that is more highly enriched than that used for power reactors, which may be a more attractive target for theft.

— **Ageing**: More than 70% of research reactors worldwide are more than 30 years old. Many were built with older technology that did not consider security in their initial design and construction, and many are now in a state of extended shutdown.

— **Utilization**: Research reactors are often part of a larger enterprise (e.g. medical isotope production or training facilities for universities) or are part of a larger research campus of unrelated activities. In addition, the uses of research reactors are often such that ease of access to the reactor facility is essential.

— **Stakeholders**: Most research reactors are owned and/or supported by a number of organizations, often of different types. This may influence the reliability of funding due to the presence of competing priorities, particularly with respect to security.

— **Culture**: Research reactor staff may lack an effective nuclear security culture; in particular, there may be a belief that the needs of research can take priority over compliance with safety and security regulatory requirements.

1.2. OBJECTIVE

This publication is intended to provide a single source guidance to assist those responsible for the implementation of nuclear security measures at a RRRF in developing and maintaining an effective and comprehensive programme covering all aspects of nuclear security (for all nuclear and other radioactive material and the related facilities) on the site.

In aiming to cover all nuclear security considerations as applied to RRRF, this publication may repeat or interpret guidance from thematic guidance publications. The intention is to provide a comprehensive set of information and guidance that RRRF security management can use effectively and to present it in the context of how it applies to RRRF.

This publication focuses primarily on assisting an operator (operator-centric) to implement an effective nuclear security management system, and in demonstrating the effectiveness of their nuclear security programme to the competent authority. The competent authority may also find this publication useful in supporting the licensing and inspection of the operator's nuclear security systems.

1.3. SCOPE

Existing IAEA Nuclear Security Series (NSS) publications do not provide specific guidance for RRRF. Implementing Guides address technical areas such as nuclear security culture, measures against insider threat, design basis threat (DBT) and computer security; but these are typically meant as general guidance for nuclear facilities rather than having specific application to research reactors.

This document builds on the recommendations of NSS publications No. 13 Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Rev5) and No.14 Nuclear Security Recommendations on Radioactive Materials and Associated Facilities.

RRRF operators would therefore need to apply a graded approach to the general nuclear security guidance on several different topics and to take account of the particular characteristics of research reactors.

The guidance in this publication applies to RRRF located on the same site. It does not address other types of facility or the off-site transport of nuclear or other radioactive material. The scope includes security operations, security processes, security forces as well as integrated management system interfaces and their relationship with the State's nuclear security regime.

The guidance in this publication applies to RRRF located on the same site. It does not address other types of facility or the off-site transport of nuclear or other radioactive material. The scope includes security operations, security processes, and security forces and their relationship with the State's nuclear security regime.

1.4. STRUCTURE

Section 1 provides an introduction and Section 2 describes the particular challenges to establishing and sustaining effective nuclear security systems and measures at RRRF. Section 3 addresses the particular risks, targets and threats associated with RRRF. Section 4 describes the objectives of a facility programme to establish nuclear security systems and measures to counter the threats, and Sections 5 and 6 address, respectively, the different types of nuclear security measure and the management processes and procedures needed to implement and complement those measures. Section 7 describes the considerations in developing a security

plan, and Section 8 provides guidance on preparing for regulatory inspections. Appendices I–III provides more detail on specific topics covered in the guidance.

2. CHALLENGES FOR NUCLEAR SECURITY AT RRRF

The Convention on the Physical Protection of Nuclear Material (CPPNM) highlights the need for a legal and regulatory basis for nuclear security. It is a State's responsibility to develop a nuclear security regime with a legal basis and a regulatory structure that includes threat assessment, trustworthiness programmes, development of regulations, establishment of thresholds of unacceptable consequences, licensing, inspection and response arrangements. Specific nuclear security requirements would be established by the regulatory or competent authority and would serve as the basis for the RRRF nuclear security system. The IAEA's Code of Conduct on the Safety and Security of Radioactive Sources provides a foundation for the security of radioactive sources that has application to, but is not specific to, RRRF. In addition, the IAEA has published recommendations for nuclear security that are intended to be input for State regulations but which do not specifically address RRRF.

Figure 1 outlines the State's nuclear security regime and highlights security related activities, governance and organizational interfaces and the relationships required to implement and maintain an integrated security management system. Figure 1 also outlines the interfaces and requirements that drive a nuclear security management system.

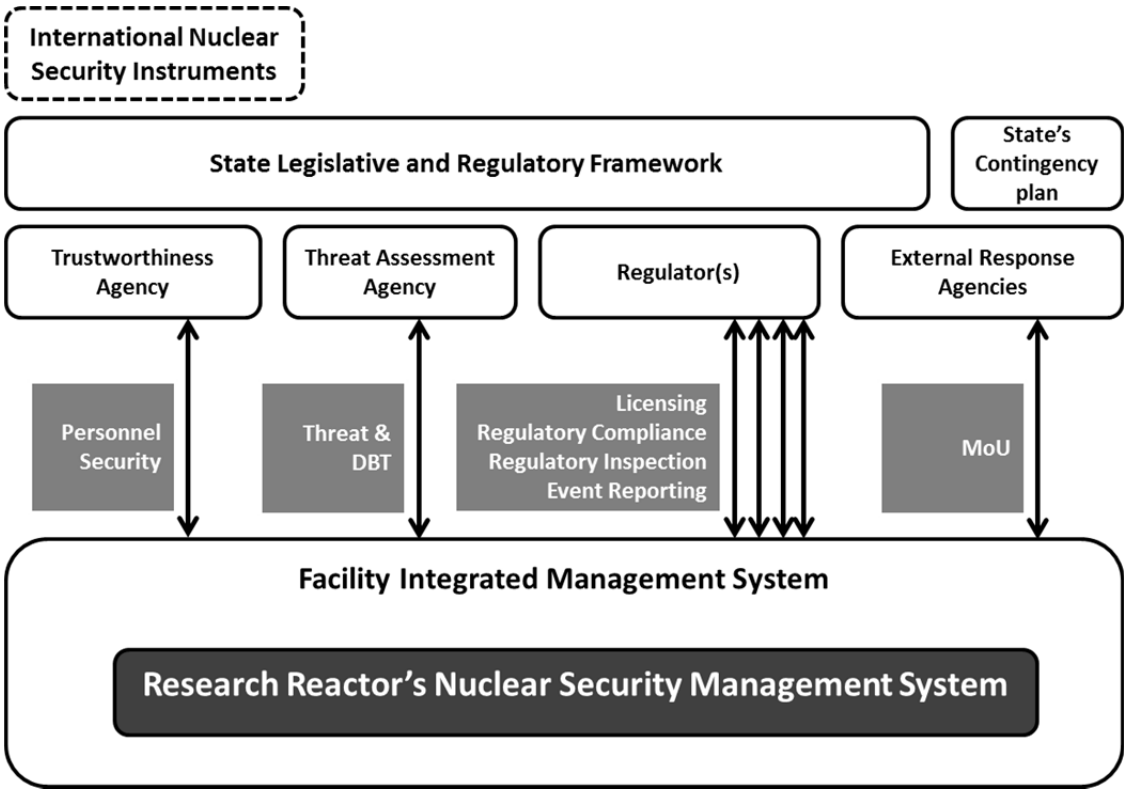

FIG. 1. Governance and organizational interfaces. (MoU: Memorandum of Understanding).

A nuclear security regime includes legislation, regulations, processes and plans that will enable a State to regulate effectively the use, storage, and processes of nuclear and radioactive material and facilities.

RRRF, owing to their diverse objectives, settings, and funding and staffing arrangements, present a particular set of challenges to the implementation and maintenance of an effective

nuclear security programme. These challenges are summarized below and are addressed in greater detail in subsequent sections.

2.1. SECURITY VULNERABILITIES INHERENT IN DESIGN

The majority of research reactors were not designed with security as a priority, which can complicate the task of providing security. Research reactor designs were typically optimized around their specific objective (e.g. education and training, research or radioisotope production). The focus on these objectives often led to the inclusion of features that are not conducive to nuclear security, such as:

- Beam tubes and rabbit systems intended to provide easy access to the core in order to introduce or remove experiments;
- Exposed cores and hand tools for removing assemblies provided to facilitate frequent reconfiguration of the core;
- Glass-walled control rooms (to facilitate instruction and training);
- Access to resident computer systems (data and network access);
- Open and exposed spent fuel pools, to reduce cost (in the absence of emphasis on security).

These features may provide security vulnerabilities that could be exploited by an adversary intent on committing unauthorized removal or sabotage.

2.2. AVAILABILITY OF TOOLS AND OPERATIONAL EQUIPMENT

In addition to potential security vulnerabilities introduced in the design, research reactors often have tools and equipment kept readily available to facilitate research and training. Such tools and equipment often includes handling poles for fuel removal, cranes, forklifts, fuel casks, power tools, digital assets and portable shielding blocks. The availability of these types of tool and equipment could be exploited by an adversary to assist in an act of unauthorized removal or sabotage.

2.3. SPECIFIC SAFETY DESIGN

Owing to their lower thermal energy and fission product inventory, research reactors typically present a much smaller hazard than power reactors and as such need much less elaborate safety features to comply with safety requirements. A research reactor may have fewer and less diverse safety systems, with less redundancy, and the systems may be less robust. These safety systems may also, therefore, be more easily defeated by an adversary, and this may increase the impact of an act of sabotage in those cases where safety functions are used to address security functions as well. The limitations of research reactor safety systems would be specifically considered in designing the facility’s nuclear security systems. Relevant considerations include:

- Limited power supply redundancy;
- Type of reactivity control;
- Robustness of decay heat removal;
- Absence of containment/confinement;
- Less robust fire protection;

— Limited diversity/redundancy of safety systems;

— Limited compartmentalization.

2.4. ATTRACTIVENESS OF MATERIAL FOR THEFT

Research reactors typically use a form of uranium that is more highly enriched than that used in nuclear power plants. The duration and frequency of operation of research reactors, especially those that are underutilized, may also be such that the fuel burnup is low and the dose rates from spent or irradiated fuel may be less likely to be immediately incapacitating to an adversary. Research reactors may, therefore, hold material that is a more attractive target for unauthorized removal than that held at nuclear power plants. Other factors that may also contribute to this attractiveness include:

— Physical form, in terms of the size and weight of fuel assemblies and hence their portability;

— Chemical form with regard to the extent and complexity of the chemical processing necessary to achieve a desired form of material;

— Amount of material;

— Ease of access to the material.

2.5. CO-LOCATION WITH OTHER FACILITIES

Research reactors are often part of a larger organization (e.g. for medical radioisotope production or for training purposes) or are part of a larger research campus that has other unrelated activities. As such, they can be co-located with several other types of facility, often under the same security management system. The co-location of research reactor facilities among other types of industrial or research facility presents specific security considerations, the impacts of which need to be considered when developing a RRRF nuclear security system.

The following is a list of facilities typically co-located with research reactors:

— Radioisotope production facilities;

— Fuel research and fabrication facilities;

— Storage of fresh fuel, spent fuel, or radioactive sources;

— Radioactive waste storage and disposal;

— Laboratories, hot cells;

— Irradiation facilities.

2.6. OPENNESS OF ACCESS AND EXCHANGE OF INFORMATION

The operational business of RRRF often calls for an environment where the reactor’s research areas are easily accessible to technically skilled contractors, staff, guest scientists, students and other visitors. A large number of temporary personnel with unescorted access create complications for a nuclear security system. In addition, the environment of information sharing and data transparency that is integral to the research community, owing to the need to remain competitive and viable, can create vulnerability for the nuclear security system, including the security of computer based systems. Lastly, high levels of computer literacy,

which is a common attribute of researchers, presents a potential security vulnerability, given the researchers' access to the information technology infrastructure.

2.7. VARIETY OF USES OF RESEARCH REACTORS

As indicated above, research reactors have a wide variety of designs to fulfil different specific purposes, such as: training, research and education; irradiation; neutron scatter experiments; neutron radiography; source/radioisotope production; medical therapy and research; and neutron activation. This diversity complicates any effort to impart a standard approach to security.

2.8. FUNDING

Research reactors may be owned and supported by a number of different types of organization. This can influence the extent and predictability of funding, including that for security. Furthermore, competing priorities within organizations, particularly when funds are scarce, may put a strain on funding the maintenance of reactor security. Funding limitations can make it difficult to implement and maintain adequate nuclear security systems.

2.9. REGULATORY AND OPERATOR ISSUES

A RRRF operating organization(s) may lack an appropriate nuclear security culture, at times believing that the reactor's purpose or mission is more important than compliance with regulatory requirements. This can be exacerbated by a lack of nuclear security expertise and/or organizational independence in the regulatory body in States where nuclear research operation/promotion and regulatory oversight responsibilities are within the same government organization. Such conditions may result in the lack of effective regulatory oversight. This, combined with the lack of a nuclear security culture among researchers, can significantly complicate effective implementation of security measures.

2.10. RRRF SITE LOCATION

Many RRRF are in geographic locations that might be undesirable from a purely nuclear security perspective. Such locations might, for example, have the following complicating characteristics:

- Close proximity to centres of population;
- Dense traffic in the surrounding area;
- Unfavourable climate or frequent extreme weather;
- Seismic activity;
- Disadvantageous topography from a security perspective;
- Possibility of unattended operation;
- Co-location with other facilities;
- Location in an area not under the control of the State.

2.11. LEVEL OF SECURITY EXPERTISE

At all but the largest RRRF, responsibilities for nuclear security are typically one of a number of duties assigned to a single staff member. Staff responsible for security often lack specialized experience and knowledge of the security system or of security measures. This

can be exacerbated by a lack of security expertise in senior management within the organization and/or at the regulatory authority, which limits the ability to perform effective checks and balances. Lack of expertise can result in the following:

— The responsibility for overseeing and implementing security is effectively ignored.

— The security responsibility is undertaken, but the resulting security is ineffective due to the limited depth of knowledge and experience in security.

— The security responsibility is transferred to a commercial contractor, whose primary motivation is profit rather than effective security.

2.12. FACILITY AGEING ISSUES

More than 70% of research reactors are more than 30 years old. As such, they were typically built with older technology, and security considerations were not taken enough into account in their initial design and construction. Although many of these have been upgraded, these upgrades may still not give adequate consideration to security. The effectiveness of those security features that were originally present or incorporated may also have degraded with age. Examples of weaknesses in security due to ageing include:

— Lack of robust barrier design;

— Degradation of security and safety components;

— Inability to support upgrades due to lack of infrastructure or structural robustness;

— External contractors having access to the facility and/or its security features during facility upgrading without having been subject to trustworthiness checks;

— Security system obsolescence;

— Facility configuration or geometry that cannot accommodate security upgrades.

2.13. RESEARCH REACTORS IN EXTENDED SHUTDOWN

Many research reactors are in extended shutdown, and maintaining the commitment necessary for the effective protection of the material is a particular security concern for such reactors. Specific concerns include:

— Fuel remaining on-site;

— Degradation of security vigilance over time due to regulatory and operator complacency;

— Lack of funding and/or personnel; and

— Reduced likelihood of fuel being self-protecting due to low burnup and/or radioactive decay.

2.14. ON-SITE MOVEMENT OF NUCLEAR AND OTHER RADIOACTIVE MATERIAL

Research reactor operations may require frequent on-site movements of material, and these movements may not, in many cases, follow defined, formal security procedures. This lack of formality with procedures can result in potential security vulnerabilities, particularly with respect to unauthorized removal, which depends on the frequency and duration of material movement and the ‘attractiveness’ of the material being moved.

3. THREATS, TARGETS AND RISK AT RRRF

RRRF facilities need to manage the level of risk related to the potential consequences of an act of unauthorized removal and/or sabotage of nuclear or other radioactive material. Risk reflects a combination of the consequences of such an act if it occurred and the likelihood that the act, and therefore the consequences, will occur.

3.1. RISK

Risk management aims to provide a graded approach by identifying the level and effectiveness of nuclear security measures that provide an appropriate balance between the risk associated with the potential unauthorized removal or sabotage of nuclear or other radioactive material and the costs (including, but not necessarily limited to, the financial cost) of providing such security. Risk management includes consideration of:

- The characteristics of the likely adversary threat;
- The potential severity of consequences (which depends on the isotope, form, and activity of nuclear and other radioactive material);
- The thermal power of the facility and the effectiveness of its safety features in the case of sabotage;
- The effectiveness of nuclear security systems for the materials and facilities where they are present;
- All costs associated with implementing and maintaining the nuclear security systems.

The severity of the potential consequences of a malicious act, therefore, influences the necessary effectiveness of nuclear security systems. This effectiveness is proportional to the severity of consequences in a graded approach, which is one of the fundamental principles of nuclear security and one of the tools of risk management.

The graded approach to security against unauthorized removal is applied in practice through the categorization of materials as defined in INFCIRC 225 (for nuclear material) and the Code of Conduct on the Safety and Security of Radioactive Sources. The graded approach for sabotage of nuclear facilities is applied, based on potential consequences, through layers of security that protect vital areas from physical and computer based attacks. The robustness of security measures is driven by State defined threats. The number of layers of security is driven by the severity of consequences with respect to criteria for “unacceptable radiological consequences” defined by the State.

The overall effectiveness of a nuclear security system is a combination of its success in:

- Detecting any malicious act early in its development and communicating this to appropriate response authorities;
- Delaying the progress of the malicious act after detection long enough to ensure that an adequate and trained response force arrives to interrupt the adversary prior to completion of the malicious act; and
- Preventing the adversary from completing the malicious act.

The level of confidence that the security system can accomplish these three steps would be proportionate to the severity of consequences of the malicious act.

Risks can be reduced by:

— **Deterring the threat**. Risk may be reduced, for example, through the deterrent effect of robust security measures and by protecting the confidentiality of sensitive information.

— **Improving the effectiveness of the nuclear security system**. Strengthening defence in depth, enhancing a nuclear security culture or otherwise improving preventative nuclear security measures may increase the nuclear security system's effectiveness.

— **Reducing the potential consequences of malicious acts**. This can be achieved by modifying specific contributory factors, for example, the amount, type and form of nuclear material and the design of the facility.

3.2. SEVERITY OF CONSEQUENCES

For nuclear material and facilities, the severity of the potential consequences of an act of unauthorized removal depend on the amount and form of the material. The potential consequences of an act of sabotage depend on the reactor's thermal power, the accumulated fission product inventory and the effectiveness of the mitigating safety systems. Potential consequences that may result from either the detonation of an improvised nuclear device or the uncontrolled release of radioactive material from a sabotaged reactor may include: deterministic and stochastic health effects of radiation exposure, financial costs of clean-up and the associated loss of use of contaminated areas, and negative political impact.

For radioactive material, the severity of potential consequences is determined by the chemical form, isotopic composition and activity of the radioactive material, and in some cases, on the immediate location into which the radioactive material would be released. As stated above, these consequences may include deterministic and stochastic health effects from exposure to radiation, financial costs of clean-up, economic impact resulting from loss of use of the areas contaminated and the political repercussions of the event.

3.3. LIKELIHOOD OF CONSEQUENCES

The likelihood of consequences occurring depends on several factors. These include:

— The attractiveness of the nuclear and other radioactive material as targets for unauthorized removal or of the related facilities as targets for sabotage;

— The intentions of potential adversaries;

— The capabilities of potential adversaries with respect to unauthorized removal or sabotage as compared to the security, safety and other systems that they would need to overcome.

Understanding and qualifying or quantifying the likelihood of any nuclear security event is different from quantifying the likelihood of a similar safety scenario because of the deliberate intent of an adversary to overcome or bypass security measures.

3.4 THREATS

To estimate the likelihood of a nuclear security event, the threat to nuclear security, which refers to the characteristics or attributes of adversaries that may undertake an intentional malicious act involving these materials or facilities, needs to be assessed. Among these characteristics are motivation, which relates to the likelihood of a malicious attempt, and

capability, which relates to the likelihood of their success given an attempt. Adversary characteristics are typically identified through the assistance of the intelligence community, but are rarely, if ever, quantifiable.

Further information on threat can be found in IAEA NSS No. 10, “Implementing Guide on the Development, Use and Maintenance of the Design Basis Threat”.

4. OBJECTIVES OF THE FACILITY’S NUCLEAR SECURITY SYSTEM

The overall objective of a State’s nuclear security regime (as per IAEA Nuclear Security Series Nos 13 and 14) is to protect persons, property, society and the environment from malicious acts involving nuclear and other radioactive material. More specific objectives are:

- Protecting against unauthorized removal and other unlawful taking of nuclear and/or other radioactive material;
- Ensuring the implementation of rapid and comprehensive measures to locate and recover nuclear and other radioactive material which is lost, missing or stolen, and to re-establish regulatory control;
- Protecting nuclear and/or other radioactive material and related facilities against sabotage;
- Mitigating or minimizing the radiological consequences of sabotage.

The objectives mentioned above would be addressed in an integrated manner, taking into account the different risks covered by nuclear security. Risks arising from computer based attacks on security, safety and/or emergency preparedness systems would be taken into account. These objectives are realized through security measures to deter, detect, delay and respond to a potential malicious act and to provide for the security management of nuclear and radioactive material and related facilities.

These security measures would be based on a risk-informed graded approach so that similar security is provided for material capable of resulting in similar potential radiological consequences arising from use in a malicious act. The concept of defence in depth would also be used.

5. SECURITY MANAGEMENT

5.1. FACILITY INTEGRATED MANAGEMENT SYSTEM

At any facility, there would be a facility integrated management system (IMS) that integrates all of an organization’s systems and processes into one complete framework, enabling the organization to work as a single unit with unified objectives. An integrated system provides a clear, holistic ‘picture’ of all aspects of the organization as well as how they affect each other and their associated risks. An IMS allows a management team to create one overall structure that can help to effectively and efficiently meet an organization’s objectives.

IMS is relevant to any organization, regardless of size or sector, seeking to integrate two or more of its management systems into one cohesive system with an integrated set of documentation, policies, procedures and processes.

5.1.1. Leadership for nuclear security

The promotion and maintenance of a nuclear security culture within the facility is one of the prime security responsibilities of senior and nuclear security management at a RRRF. By assuming a leadership role for nuclear security, management can, through the application of incentives and disincentives, ensure that high priority is given to nuclear security throughout the organization. Managers have a key role in ensuring that staff members are appropriately motivated and that their role in enhancing nuclear security is recognized and valued within the organization. Rewards, recognition and support (both tangible and intangible) can encourage vigilance, questioning attitudes and personal accountability.

5.2. NUCLEAR SECURITY MANAGEMENT SYSTEM AT A FACILITY

Security management is a term used in this publication to describe the roles and responsibilities that would be effectively performed and the programmes or functions that would be successfully implemented in order that the RRRF nuclear security programme meets the objectives laid out in international instruments, IAEA guidance and the State's regulatory requirements. The roles, responsibilities and programmes for management of security at a facility include three topical areas: operations, processes and forces. These are summarized in Fig. 2.

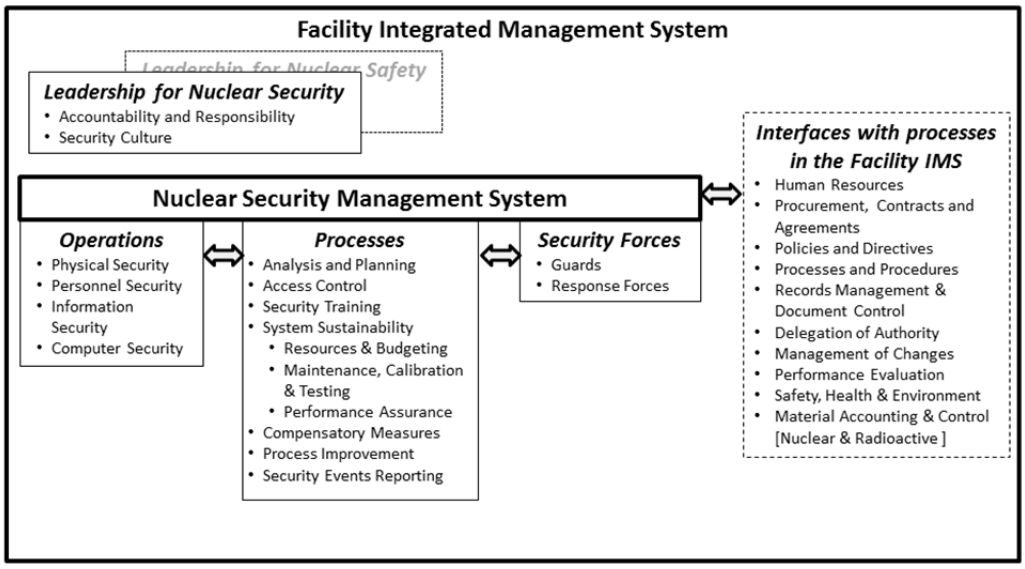

FIG. 2. Structure of facility Nuclear Security Management System.

The management structure for nuclear security at a RRRF would be clearly defined. Managers responsible for nuclear security at the facility would define the roles and responsibilities relating to nuclear security for each level of the organization and its interfaces with other aspects of facility management. This includes defining the specific assignment of responsibility for nuclear security to an individual (or individuals) and assignment to the individual(s) of the necessary authority, autonomy and resources to successfully carry out this role. The individual(s) would report to the top manager or the appropriate organization senior manager who is authorized to operate the research reactor, and the responsibilities assigned to their position would be documented in sufficient detail to avoid ambiguity.

Managers at facilities possessing nuclear or other radioactive material are responsible for ensuring that appropriate standards of behaviour and performance relevant to nuclear security are established and that expectations with regard to the application of these standards are understood. They would also ensure that there is a clear understanding within the organization

of the roles and responsibilities of each individual involved in security, including clarity concerning levels of authority and lines of communication.

Managers would also establish a formal decision making mechanism that is well understood within the organization and involve their staff in decision making, where appropriate. The quality of a decision is improved when the individuals involved are able to contribute their insights, ideas and experiences.

5.2.1. Security operations

The operational elements of nuclear security can be divided into physical security, personnel security, information security and computer security. A description of how these operational elements are implemented is presented in this section, and further details can be found in Annex.

5.2.1.1. Physical security

Physical security is employed as a system to protect the RRRF and its nuclear and other radioactive material against malicious acts that could result in unacceptable radiological consequences. A physical security system achieves this through the integrated deployment of technical and administrative measures to deter, detect, delay and respond to attempted malicious acts. The severity of potential consequences is the basis for the level (i.e. grading) of physical security to protect nuclear or other radioactive material and facilities. Physical security systems need to be designed installed and maintained to provide adequate protection against the defined threats and would be periodically evaluated to ensure that they remain effective. The Annex provides a more thorough description of physical security elements.

5.2.1.2. Personnel security

Personnel security means ensuring the honesty, reliability and trustworthiness of staff and others with access to protected targets in order to minimize the likelihood that any of these persons would be motivated to participate in a malicious act (defined as insider threats in IAEA NSS No. 8).

Personnel security is applied to persons, including contractors and visitors, who have authorized access to the RRRF and its nuclear and other radioactive material. It is therefore necessary to confirm that the honesty, reliability and trustworthiness of personnel and visitors meet national criteria that are commensurate with the nature of the facility, material or information and to the level of access granted. Background and trustworthiness checks may be used to identify any indicators that might raise concerns about a susceptibility, willingness or desire to commit a malicious act (e.g. drug or alcohol addiction, mental illness, financial problems, history of violent or criminal behaviour). Personnel security would also include defined criteria for limiting or excluding access (see IAEA Nuclear Security Series Nos 7 and 8).

Personnel would be screened prior to employment, and the granting of unescorted access would be controlled to minimize the likelihood of an insider attempting a malicious act. The programme would also include periodic checks to provide assurance that personnel and contractors continue to be trustworthy.

5.2.1.3. Information security

Information security is the control and protection of the confidentiality of sensitive information, which can be in the form of electronic or printed data, text, maps, drawings or

photographs. The disclosure of sensitive information could aid an adversary in the execution of a malicious act involving nuclear or other radioactive material or facilities housing such materials.

Operators of RRRF need to address the security of information that could be of value to an adversary's plan or in the commission of a malicious act that could result in unacceptable radiological consequences. Information security measures would protect the confidentiality, integrity, accessibility and availability of information through classification, information controls and information accountability as well as the security measures applied to the protection of information. As in physical security, information sensitivity needs to be identified, classified and graded to reflect the severity of the potential consequences if the information be compromised. Access to sensitive information would be restricted to persons having the appropriate clearance, authorization and need to know based on a strict evaluation. Information security measures include authentication, access authorization and compartmentalization, access detection, storage rules and access delay. The sensitive information programme would be periodically reviewed and updated to reflect changes in the facility characteristics. It includes, as a minimum, the following:

— Security of information in physical form (e.g. paper, electronic media);

— Security of computer systems, which is also referred to as computer security, information technology security or cyber security;

— Security of information assets (e.g. information storage and processing equipment and communications systems and networks);

— Security of information about facility employees and third parties (e.g. contractors and vendors) that could compromise the security of the above;

— Security of intangible information (e.g. knowledge).

The sensitive information protection programme would be developed in compliance with national security policy and relevant national laws and requirements. All employees would be fully aware of the need for information security.

Management has the overall responsibility for ensuring that information security is in place and effective throughout the facility or organization in order to secure sensitive information. All personnel who handle sensitive information are responsible for ensuring that its security is in line with related national legislation as well as the organization's policies and procedures.

5.2.1.4. Computer security

Computer security[1,2] is the graded protection of relevant computer based systems, networks and digital systems. These systems control the processes, the compromise, damage, control or infiltration of which could aid an adversary in the execution of a malicious act.

Interactions between computer systems in nuclear facilities may affect security in non-obvious ways. It is, therefore, important that all assets and information are identified, including making a more comprehensive inventory of those assets critical to facility security, safety, and emergency preparedness functions. The inventory would include data, computer systems, interfaces and owners. The site would develop a computer security plan that outlines

[1] Computer security, as defined here, is a subset of information security as defined, for example, in ISO/IEC 27000 with which it shares many of the goals, methodology and terminology.

[2] As per IAEA Nuclear Security Series No. 17, computer security covers the security of all (relevant) computers and all interconnected systems and networks formed by the sum of the elements.

the approach used to ensure that the appropriate level of security protection is provided for the computer systems. Computer security, as part of the overall facility security plan, would be periodically reviewed and updated to reflect changes in its characteristics. IAEA NSS No. 17 addresses technical and administrative guidance in the implementation of computer security.

Computer security needs to address the computation, communication, instrumentation and control devices that make up the functional elements of a nuclear facility. This includes not only desktop computers, mainframe systems, servers and network devices but also lower level components such as embedded systems, programmable logic controllers and all components that may be susceptible to electronic compromise.

Computer security controls include firewalls, system access levels, authorized access controls through passwords, virus scanners, restrictions on the introduction of unauthorized software or media and backups. The vulnerability of networks and other digital systems need to be assessed against the defined threat, and appropriate measures would be developed to protect the integrity, availability and confidentiality of the processes, computer systems and electronic data. The operator's contingency plan would identify specific computer security incidents that constitute a potential nuclear security event and the required response to these incidents. This contingency plan would include pre-established response arrangements for involvement of State or other qualified resources.

5.2.2. Management processes

Nuclear security management system processes include analysis and planning, access control, security training, system sustainability, compensatory measures, process improvement and security event reporting.

5.2.2.1. Analysis and planning

Threat analysis

RRRF operators would adopt security objectives consistent with national requirements. This includes the establishment of a nuclear security system that provides the necessary protection of identified targets against threats defined by the State (via DBT or through threat assessment).

If the State determines that consideration of an insider threat is necessary, then the operator needs to ensure that measures are in place to counter such a threat, such as by conducting an analysis of insider threats, including characterizing authorized individuals' access rights, authorities over processes and persons and knowledge of sensitive information. Guidance on measures against insider threats can be found in IAEA NSS No. 8.

Target analysis

The graded approach demands that the consequence severity of potential targets be considered when assessing the appropriate level of security at RRRF. This includes potential targets of theft and sabotage, when either of these have the potential to exceed unacceptable levels as determined by the State.

If the target materials, either by their form, isotopic composition, enrichment, isotopic mass, and activity exceed thresholds for unauthorized removal, as defined in IAEA NSS Nos. 13 or 14, then target analysis for these materials, including location, portability, self-protecting activity, and other attractiveness considerations would be described.

If consideration of sabotage is determined to be necessary (i.e. consequence analysis reveals that the potential consequences could exceed unacceptable thresholds), then an analysis of

targets of sabotage (materials, equipment, computer systems, or processes) that control the facility operation and safety systems would be conducted to determine the vital equipment (the equipment, which is sabotaged, would lead to unacceptable consequences) and the minimum areas, in which this equipment is located, which must be protected to prevent these unacceptable consequences (vital areas). Further detail on analysis of targets of sabotage can be located in IAEA NSS No. 16 “Vital Area Identification).

The information concerning the targets, consequence analysis, and vital area definition would be included in an appendix to the security plan. As inventories of material can vary with time, it is recommended to use the quantity that results in the highest security category for the expected life of the security plan to minimize the frequency of updating the plan.

Security system design and evaluation

The goal of the physical protection system (PPS) is to prevent theft or sabotage by an adversary/DBT (i.e. the adversary would be defeated before they complete their task). PPS effectiveness would be at a level that is acceptable for the competent authority to grant an operating licence. If PPS effectiveness is not within acceptable levels, then the system needs to be re-designed or improvements implemented.

An effective PPS relies on a combination of equipment and personnel, which is designed and integrated into an effective system. Security procedures are developed to define how personnel interact most effectively with equipment. These procedures would be documented and controlled whenever:

- Failure to perform the task correctly can result in significant degradation of security effectiveness or may result in serious personal harm or significant damage to property.
- The task is performed infrequently.
- The task is only performed by one or a few persons.
- The task is very complex.
- The results of the task would be reproducible and/or trackable.

The important steps of defining PPS requirements and designing the PPS need to be evaluated to determine its effectiveness against the threat assessment or DBT. The evaluation process uses many tools and methodologies, such as adversary sequence diagrams, single path analysis, neutralization analysis, scenario analysis, computer security risk assessment and insider analysis. Further discussion on each of these can be found in IAEA-TECDOC-1276.

Developing a security plan

A security plan, prepared and maintained by RRRF security management, would include all information necessary to describe the security objectives, approach and system being used for the protection of materials, facilities and information. The level of detail and depth of content would be commensurate with the category of the material or facility covered by the plan. The security plan usually requires approval by the competent authority. It will, in many cases, serve as a basis for regulatory inspections and, therefore, would be organized so as to address security requirements and demonstrate how the facility is protected against DBT (or other threat criteria) by the nuclear security system, based upon the State’s threat assessment.

Appendix II provides a typical outline for a RRRF security plan as well as more detailed guidance for the author of such a plan.

The security plan would be periodically reviewed to ensure that the conditions and assumptions under which it was developed are still valid. If changes are needed, they would be introduced by the responsible facility personnel and reviewed and approved, if required, by

the competent authority. In addition, the plan would be reviewed and updated whenever changes to the facility, material inventory, security system or regulations (including threat characteristics) take place. The plan would include a means of document version control to ensure that all parties are working to the current, approved security plan.

Developing a security contingency plan

A security contingency plan describes the predefined sets of actions for response to unauthorized acts indicative of attempted unauthorized removal or sabotage, including threats thereof, designed to effectively counter such acts. This plan outlines the strategic objectives of the security response for a given type of event (e.g., containment of the adversary to prevent them from leaving the facility perimeter, denial of access to targets in the facility, or prevention of sabotage of critical systems via computer-based attacks) and the tactical approach to achieve these objectives. The contingency plan can be a part of the security plan, or it can be a separate document. It outlines the roles and actions of security staff, the interaction of site security with offsite response (e.g., law enforcement and/or military forces), and the actions taken by onsite employees/contractors to prevent interference with the response forces and to avoid harm from an adversary. These roles include, but are not limited to:

- A Central Alarm Station (CAS) operator assessing a security alarm or event and communicating information to response forces,
- A guard meeting and escorting response forces,
- Guards assigned to communicate and direct facility personnel to either shelter-in-place or evacuate,
- A supervisor acting as an event coordinator,
- A technical staff member assessing the computer security situation, or
- A technical staff member assessing the radiological situation, etc. (would this not be emergency response plan rather than contingency plan?)

The contingency plan would address actions that site personnel can take to delay an adversary and assist the response force. Examples include:

- Removal of utilities (power, heating/cooling),
- Deployment of barriers,
- Locking doors and blocking of vehicle exits,
- Providing situation report to response forces,
- Escorting response onsite, if needed, and
- Evacuation or sheltering of onsite staff and contractors (if possible).

In addition, the contingency plan would describe command and control during a security event as well as the rules of engagement for onsite security forces. Appropriate and realistic drills and exercises of the contingency plan that include the RRRF staff, guards, and response forces would be conducted periodically. The RRRF contingency plan would be coordinated with the facilities emergency response plan and consistent with and complementary to the State’s contingency plan.

5.2.2.2. Access control

RRRF can have a wide variety of technically skilled contractors, staff, guest scientists, students and visitors with a wide variety of backgrounds. Further, the business of the RRRF may depend upon easy and user-friendly access to be successful. These conditions for access impose unique constraints on the operator to maintain effective access control that reflects the specific utilization of the facility. For example, some research reactors have a single use, which does not change with time, such as radioisotope production reactors or reactors used only for neutron scatter experiments. For radioisotope production reactors, the set of personnel needing access to the facility is stable. In a research reactor dedicated to neutron scatter experiments, researchers need repeated access to the neutron scatter building and only occasional access to the reactor hall; they do not need access to sensitive areas of the facility such as the reactor control room or the reactor pool level (for a pool type research reactor).

Access control processes are typically integrated into physical security, information security and computer security systems. The process of access control includes:

- Creation of physical and logical access zones for compartmentalization of areas, which limits access to those with need;
- Management of approval processes for facility access requests;
- Issue of access control keys, key cards, network accounts, badges and/or other access systems;
- Protection of badging or enrolment equipment, databases, spare badges and spare keys;
- Specification of unauthorized items and/or materials that may not be taken through access controls (e.g. contraband);
- Implementation of two person rule for designated areas;
- Consideration of emergency access.

5.2.2.3. Security training

In addition to having specific competency training for particular jobs, all staff need to undergo the training necessary to be competent to carry out their security responsibilities. This training would include security awareness and actions to be taken in support of the nuclear security contingency plan.

Security management would also make sure that all personnel who are assigned duties that can affect security have a sufficient understanding of the facility and its security features, as well as sufficient competence to ensure secure operation of the facility. All staff would be provided with computer security awareness training. Individuals having computer security responsibilities would be specifically trained to support computer security, recognize potential computer security events and respond appropriately.

5.2.2.4. System sustainability

Sustaining an effective nuclear security system will require a long term commitment for the provision of resources necessary to maintain essential processes in place.

5.2.2.5. Resources and budgeting

RRRF management would make securing the resources required for the operation and sustainment of its nuclear security programme (not just the PPS) a priority. This includes having established human resources that will manage the programme; implement the technical, physical and administrative controls detailed within the facility security plan; design, install and operate the physical protection equipment; and accomplish nuclear security in all processes, procedures and programmes. In addition, financial resources are needed to employ or contract for the human resources identified above, as well as to purchase, install, operate, maintain and test physical protection equipment and provide the expendable items exhausted in the performance of the daily security tasks. The costs of training and retraining in support of nuclear security would also be addressed.

Planning for resources requires that the RRRF site management assess the financial costs of human resources and the costs of nuclear security system operation and sustainability, including the costs of the materials expended in testing, training, badging, trustworthiness checks, and document development and management. It further requires that site management invest time in recruiting staff that possess the prerequisite competencies necessary to perform nuclear security tasks and in developing staff competence.

5.2.2.6. Maintenance, testing and calibration

Maintenance, testing and calibration programmes are established at the facility to ensure that equipment and systems are working properly. Preventative maintenance is conducted on a regular basis to prevent the degradation or failure of equipment and components. Maintenance can, and typically does, include the calibration of security systems and equipment. Corrective maintenance is conducted to respond to equipment failure.

Testing includes actions to confirm that security components are operating as designed, particularly after maintenance or repair.

Maintenance plans, procedures and testing are prepared so as to outline the schedule of maintenance, the steps followed when conducting maintenance and the information to be recorded concerning the maintenance activity. Performance of maintenance would be recorded and the records kept in accordance with the facility records management and procedural controls (see Section 5.3.5.).

5.2.2.7. Performance assurance

The performance assurance process is an integral part of the nuclear security quality programme at a RRRF. It would be conducted on a periodic basis to ensure that the system continues to operate as expected. It provides assurance that the overall security programme is operating as designed and provides confidence that the protection provided to the facility and to its nuclear and other radioactive material is adequate. The performance assurance process involves self-assessment of the overall security system effectiveness and the testing of all equipment and subsystems. The test phase consists of performance tests, drills and exercises and includes developing performance test plans, conducting the planned tests and analysing the results of the tests. The assessment phase consists of identifying adversary scenarios that could challenge the security system and then, considering the test results, evaluating the security system response with the purpose of identifying any vulnerabilities. Self-assessment also includes the identification and implementation of solutions and compensatory measures to address all identified vulnerabilities.

5.2.2.8. Compensatory measures

The compensatory measures programme describes the actions necessary to correct for compromised, degraded or inoperable[3] security related equipment, systems and components and to address security vulnerabilities introduced by abnormal situations (e.g. severe weather, non-malicious civil unrest, equipment failure, public reports of critical computer vulnerabilities). Compensatory measures would provide a level of protection that is equivalent to that which the degraded or inoperable equipment, system or component provided. Compensatory measures would be promptly implemented to eliminate any vulnerability. Implemented compensatory measures would be reported and discussed with the competent authority, including the expected duration that the compensatory measures would be in place. Whenever possible, standard compensatory measures would be pre-planned (e.g. for a power outage or a component failure) and have the prior consent of the competent authority.

5.2.2.9. Process improvement

A formal programme would be implemented to continually improve the processes supporting the nuclear security system. This process improvement programme would assimilate information gathered from both operating experiences and facility specific corrective actions.

5.2.2.10. Security event reporting

The RRRF would develop a programme to identify, gather information about, report and investigate site related nuclear security events in accordance with State practices. Reportable events would include intrusions; personnel occurrences that violate the trustworthiness rules (such as arrest for a criminal act); unaccounted for material or material missing in an audit; potential acts of espionage or sabotage; computer security events adversely impacting a PPS or other critical system; loss of confidentiality, availability or integrity of sensitive information and other similar events. Events would be accurately reported in a timely manner to minimize potential consequences.

5.2.3. Security forces

5.2.3.1. Guard forces

Guard forces are instrumental to the successful operation of many elements of physical security, such as guarding access control points and alarm stations, verifying access authorization, conducting contraband searches, performing patrols, assessing and communicating alarms to response forces and, in general, enforcing adherence to procedures by on-site personnel. Guard forces might also serve as first responders to a security event, deterring, delaying, interrupting and even neutralizing the adversary. Guard forces would be recruited, managed, trained and tested. Guards would be provided with written operating procedures.

5.2.3.2. Response forces

Response forces are qualified persons, either on-site or off-site, who are armed and appropriately equipped and trained to counter nuclear security events. Response forces are

[3] A system, subsystem or component is inoperable or degraded when it no longer meets its performance objectives.

normally activated by facility guards upon the assessed detection of an attempted malicious act. Their response would be timely, with sufficient numbers of appropriately equipped and armed personnel, and deployment would be made in a tactical manner (in accordance with policy and agreements) to arrest, effectively incapacitate, neutralize or cause an adversary to flee prior to completion of the malicious act. Response forces would be familiar with the site, the targets to be protected and their hazards, and the rules of engagement. The response would be based upon a contingency plan and be exercised periodically, in coordination with facility personnel and guards. Furthermore, response forces would be prepared to address the possibility that material might be taken off-site, and in this regard, written plans and tactics for recovery of stolen material would also be exercised.

5.3. FACILITY INTEGRATED MANAGEMENT SYSTEM INTERFACES

The IMS consists of formal documentation, practices and actions that implement disciplined and structured operations that support facility success. The goal of the IMS is to minimize the likelihood and consequences of human fallibility or technical or organizational system failures. It can be implemented through facility policies, directives, processes, plans and/or procedures.

In the case of the nuclear security management system, IMS documentation, policies, procedures and processes are utilized in an interfacing approach. This is important in order to avoid duplication, which is not cost effective, and the organization becomes a unified whole, improving the performance overall.

5.3.1. Human resources

Human resource development for a RRRF staff consists of recruiting individuals with the relevant competencies (i.e. knowledge, skills, attributes, education and experience) and then providing job specific knowledge and skills through training. Determining the competency needs of staff is the initial step in human resource development. On the basis of these competency needs, a programme to recruit and employ or otherwise obtain the services of needed staff would be established. Since these needs evolve and staff change, the recruitment programme would be an ongoing effort. Appendix I describes security competencies and training needs based on job functions.

The core competency elements of knowledge and skills that are required to effectively perform a job are best provided through on-the-job mentoring and training of recruited staff. The training programme would be founded on a needs based approach in which needed knowledge and skill deficiencies are identified by comparing known required core competencies to existing staff competencies. The training programme is then developed to eliminate specific competency deficiencies for staff members and includes a training needs assessment, training course materials development and maintenance, instructor development, use of learning approaches and feedback. The training programme would be continuously reviewed and improved where needed.

Training of persons who have a security role but who are not recruited staff would be addressed in the contract or by a Memorandum of Understanding (MOU) with the external organization.

5.3.2. Procurement, contracts and agreements

It may be advantageous or necessary to obtain resources and/or cooperation for nuclear security operations from external organizations through a contract or other agreement rather

than through direct staffing. There could be many reasons for this, including economic, legal, political and administrative. In these cases, a programme for administering contracts and agreements, including oversight of performance, would be established by management. These contracts or agreements would include provisions for adherence to facility security procedures, along with penalties for non-compliance.

Further, management would clearly understand which external organizations are likely to have a role or stake in the RRRF nuclear security. Owing to the international nature and transboundary aspect of security, the RRRF would coordinate with similar organizations to establish expeditious means of communicating security related or sensitive information. Further, they would maintain close cooperation for the exchange of intelligence and data that could impact the security of these facilities, including transport aspects. This coordination may include international organizations, State and local authorities, other nuclear facilities and, in particular, external response forces and law enforcement organizations.

If external law enforcement or military organizations provide response during security events, a formal agreement or MOU that outlines the roles, responsibilities, communication, level of competence/training, coordination and joint exercise arrangements in relation to security events would be duly signed. A point of contact would be identified for any organization within the agreement or MOU. A sample response MOU is provided in Appendix III.

5.3.3. Policies and directives

Policies and directives would be issued to reflect and implement nuclear security objectives, regulatory requirements and corporate security objectives.

5.3.4. Processes and procedures

Formally established processes and written procedures provide more confidence that work will be performed correctly and consistently regardless of which staff perform the work. Processes and procedures would be based upon overarching policies and directives. Appropriate and effective procedures that provide clear, unambiguous description/instruction of the nuclear security related actions to be performed by staff would be developed, documented, approved, communicated, trained on, tested and maintained. Written procedures would be developed to describe the correct execution of any task that is critical, infrequent, complex or that must be consistently performed among staff.

Procedures can be issued in any practical or useful format, i.e. manuals, diagrams, pictorials, checklists, etc. The procedures would be developed and documented by experts in the relevant discipline to ensure that they are appropriate, and they would be checked by non-experts to ensure that they are clear and unambiguous. Procedures would be approved by management to convey support and acceptance. The content of the procedures would be communicated to responsible personnel for awareness, personnel would be trained on proper procedure execution and personnel would be tested to ensure that procedural performance expectations are understood. Procedures also need to be periodically reviewed and updated as necessary. Changes would be communicated to facility personnel. Periodic retraining of personnel would also be undertaken, even when there has been no change to the procedures, in order to ensure that personnel remain aware of procedure content and are capable of properly performing the procedures and to ensure that current procedural expectations remain understood by personnel.

5.3.5. Records management and document control

A programme that includes processes and procedures for records management needs to be established for all relevant information, including files, data and communications. Records management would include details on what information will be developed, processed and stored and the frequency, duration and method that these records are to be stored.

A process for document control would be developed and implemented to ensure that all stakeholders are working with the current, approved document versions. This applies to any policies, directives, processes, procedures, plans, instructions, etc., that impact work. Document control addresses document format, file structure, approval process, change control and disposition. For more information, refer to the document management process in the IAEA Safety Standards Series No. GS-G-3.1, Application for the Management System for Facilities and Activities.

5.3.6. Delegation of authority

Process and procedures pertaining to appropriate and proper delegation (both permanent and temporary) of the responsibilities, accountabilities, authorities and resources would be clearly outlined.

5.3.7. Management of change

Many organizational problems and failures arise from inadequate change management processes. This is true of changes in equipment, procedures, organizational structures, roles, personnel and service providers. Therefore, the organization would have effective processes in place to understand, plan, implement and reinforce change as it applies to the security function. Management would ensure that:

- Change management processes are in place for changes that could directly or indirectly affect the security function.
- Changes in such areas as operations, safety and security are coordinated with all potentially affected organizations.
- Assessments of changes are made to confirm that the desired outcomes have been obtained.
- Evaluations are conducted on completion of the change process to determine if the change inadvertently affects established security.
- Decisions to implement a modification to existing critical computer systems involve careful consideration of possible impact on reactor safety and security.

5.3.8. Performance evaluation

To evaluate the nuclear security system, management would define performance evaluation metrics and performance indicators that enable measurement and assessment of the system’s effectiveness. These metrics would be quantifiable and measurable. Metrics would be carefully selected to ensure that they accurately provide insight into the success of the programme or operation. For example, the security culture in an organization could be partially evaluated by tracking how often staff failed to follow procedures (metric), with less than some predefined number defined as being satisfactory (performance indicator). A process for evaluating performance data and addressing non-conformance, including corrective actions and implementation of improvements, would be developed and applied.

5.3.9. Safety

Safety related activities that offer potential additional added value for security include:

— *Physical barriers in an installation designed for confinement (containment) and shielding.* These are often a solid starting point for use as intrusion barriers as long as they form a continuous, enveloping layer around the target area and are located to facilitate use as a security layer (e.g. access control requirements at each entry point are similar and the boundary lends itself to access controls). In general, compartmentalization in the installations (e.g. for fire protection) is also a good starting point for use as an intrusion barrier (extra layers of access/delay). As a result of this possible synergy of the barrier, the design of new facilities or changes to existing installations would endeavour to integrate safety and security requirements. Both the robustness of the barriers and design of the 'entry/exit' (or weaker parts that can be used for malicious access) would be discussed in the safety security interface.

— *Safety studies.* Safety studies are a basis for security consequence analysis. The accident scenarios in the safety files (and the related consequence prognosis) can be used for consequence assessment of security scenarios. However, the security consequence analysis would include additional sabotage/attack scenarios that are often discounted or not even considered in the safety studies (e.g. scenarios where the probability based on unintentional failures is too low or scenarios that include multiple, unrelated initiating events). This security consequence analysis would be developed jointly by safety and security specialists.

— *Redundancy and diversity of safety systems.* Redundant systems, particularly if physically separated, can complicate an intentional adversary sabotage scenario. Diversity complicates possible computer based attacks by requiring an adversary to compromise different, diverse, technologies. The regular checks and testing of safety systems can help to detect planned or in-process sabotage in the same way that inventory control is used as a detection mechanism against theft. The frequency and process of checks and testing would be established to support security scenario interruption. The current safety practice of using electronic personal dosimeters and the radiological monitoring of personnel at access points could yield information useful for security if those radiological monitoring systems were designed to prevent or complicate the possibility of circumvention by an adversary. Such information from these measurements would need to be provided to security in a timely manner for it to be useful.

Activities in safety that can complicate security risks:

— Safety needs for quick egress from facilities. Emergency exits provide ideal access for adversaries. Emergency exits would be protected from entry and be minimized to meet safety requirements, and they would include security provisions.

— Rapid entry of emergency responders to address a safety incident.

— A safety culture of 'openness of information' can provide an easy mechanism by which an adversary can collect potentially sensitive information. Information would be reviewed from the view of how the information could benefit an adversary and then protected accordingly.

Security measures that can benefit safety include:

— Access control, authorization to areas, information/processes and materials implemented for security can benefit safety by limiting the persons with access to 'dangerous' areas to those who have a job requiring access. This also limits those with need of access from introducing or removing unsafe/unapproved equipment and materials.

— Personnel screening done for security (looking for issues such as addiction or emotional instability) includes aspects that can have a positive effect on the safety characteristics of the workforce.

Activities in security that can complicate safety risks include:

— Access restrictions on emergency egress. Restricting emergency egress can place an additional risk of injury.

— Confidentiality of information. Restricting public access to some safety reports (or information therein) may undermine public trust in installations by creating the impression that something is being hidden from public view.

— Requiring multi-person activities to minimize the possibility of an insider, acting alone, from committing a malicious act can increase the population of persons receiving occupational radiation doses.

Activities in safeguards that can benefit and complicate security risks:

— Material accounting checks and inspections. Requirements for national and international controls require that security systems be breached (albeit appropriately) and material exposed. Although there can be a security benefit to knowing material is present, the inspection and accounting checks would be developed considering security concerns.

5.3.10. Nuclear material accounting and control

Nuclear material accounting and control (NMAC) is an integrated set of measures designed to provide information on, control of, and assurance of the presence of nuclear material during storage, use and movement. The general principles of NMAC systems can also apply to the security of radioactive material other than nuclear material.

NMAC systems can assist in the deterrence and detection (albeit not timely) of unauthorized removal of nuclear material via use of accurate, up-to-date inventories of all nuclear material (and/or other radioactive material) and established controls that help detect minor irregularities. The accounting system operates in conjunction with physical and administrative control measures.

States having an INFCIRC/153 comprehensive safeguards agreement with the IAEA are required to establish a system of accountancy and control for nuclear material under the terms of such an agreement. IAEA Services Series No. 15, Nuclear Material Accounting Handbook, describes the accountancy and reporting elements necessary for nuclear material accounting at a facility level in Section 5 of this publication. Any such existing accounting and control systems may be used as a basis for developing enhanced NMAC measures in support of nuclear security.

To be effective, an NMAC system would provide information on the quantity, type, location, use, movement and transformation of all nuclear material. It would have the capability to

register an alarm (either timely or not timely) that could in turn initiate a response to indications of unauthorized removal or use of nuclear material. Further, it would also provide for deterrence of the unauthorized use of, or interference with, equipment used in the handling and movement of nuclear material by insider adversaries.

An effective NMAC system can detect insider (and possibly outsider) unauthorized activities and assists in the correct assessment of an inventory irregularity involving material. When unauthorized removal of material has taken place, the NMAC system would be able to provide specifics regarding the quantity, category and form of the nuclear material removed. NMAC and physical protection systems would be coordinated and function in a complementary manner.

In a RRRF, a graded approach would be applied to the development of the NMAC system, taking into consideration the quantity and attractiveness of the materials held. Other factors, such as security vulnerabilities inherent in the design, availability of tools and equipment, openness of the facility, presence of co-located facilities and the particular use of the facility (as discussed elsewhere) would also be taken into account.

Further guidance on NMAC in support of nuclear security is given in IAEA NSS No. 21, Use of Nuclear Material Accounting and Control for Nuclear Security Purposes at Facilities.

6. PREPARING FOR A SECURITY INSPECTION

The following information is intended to assist the RRRF to prepare for a regulatory security inspection. This guidance is general and may not include State regulations.

Preparations for a security inspection consist of ensuring that the RRRF meets all regulatory requirements and preparing the appropriate documentation to adequately demonstrate this.

6.1. ASSURANCE OF REGULATORY COMPLIANCE

The following steps are suggested to provide assurance that regulatory requirements are met by the nuclear security programme:

(1) Conduct a thorough review of requirements (this includes the regulatory body's inspection procedures, if available) and make a comparison between them and the security plan. For some facilities, an approved security plan serves as the basis for security inspections, and if so, this step can be bypassed.
(2) Review the security plan to ensure that all programmes are being implemented and maintained as specified by the plan and that the associated documentation is accurate, up-to-date and made available to the inspector during inspection (particularly physical security maintenance and alarm log records, firewall logs and audits, personnel records, security event records, security training records, and security system and component testing records). Sensitive or classified information provided to the inspector for review would be protected in accordance with the security plan.
(3) Prior to inspection, conduct a self-assessment of the nuclear security system to ensure that it meets the objectives outlined in the security plan and thereby:
    (a) Ensure that sensors, cameras, access control equipment, and lighting are functioning properly. If any are not functioning, either initiate their repair or implement compensatory measures in compliance with the security plan and the regulations.

(b) Verify that access control, CAS operation, alarm response, visitor escort, key control and other physical protection actions are followed as per documented procedures.
(c) Ensure that personnel, information, and computer and network security processes are in place and operating as intended and that documented procedures are being followed.
(d) Ensure that any discrepancies are identified the proper resolution implemented.

6.2. ASSEMBLING NUCLEAR SECURITY DOCUMENTATION

Gather all relevant documentation needed for the inspection. This may include (but is not limited to):

— Facility security plan;
— Physical and computer security maintenance and alarm log records;
— Personnel records;
— Security training records;
— Security system and component testing records;
— Security event records;
— Documents on threat and consequence analysis;
— Documents on vulnerability analysis;
— Records on trustworthiness checks, if the site maintains these.

These records would be organized and shared with the inspectors to demonstrate the RRRF compliance with the security plan.

6.3. PREPARING FOR INSPECTION

(1) Communicate with licence holder(s) concerning the inspection.
(2) Gain agreement with the inspection team, if possible, on the scope of the inspection.
(3) Develop an inspection schedule.
(4) Arrange for safety and security operations and compensatory measures to allow for inspection activities to be conducted (e.g. shadow forces when testing guards).
(5) Arrange for appointments, visits, interviews, authorizations and escorts.
(6) Prepare personnel for inspection:
(a) Inform facility management.
(b) Provide an overview briefing to facility personnel on the agenda, objectives of the inspection and their duties. Agenda will include:
(i) Inspection of security functions;
(ii) Validation of information;
(iii) Analysis of collected information;
(iv) Inspection exit briefing.
(c) Provide information to RRRF staff on conduct appropriate during an inspection.

6.4. CONDUCT OF INSPECTION

(1) Verify the identity of each member of the inspection team and follow access procedures.
(2) Provide entrance briefing, explaining applicable security and safety rules and procedures for the inspection team.
(3) Facilitate inspection of security functions.
(4) Provide security information requested for analysis.
(5) Implement and maintain, as necessary, appropriate compensatory actions for any non-compliances identified by the inspectors until permanent corrective actions can be established.
(6) At the exit briefing, discuss and verify preliminary findings of the inspection team.

6.5. POST-INSPECTION ACTIVITIES

(1) Review the final report prepared by the inspection team and list any corrective actions to be considered.
(2) Perform simple corrective actions (e.g. replacement of a light bulb).
(3) Prepare a plan to address more complex corrective actions (e.g. replacing keys with a biometric access control system) and gain the agreement of the inspection team.
(4) Complete the corrective action plan in a timely manner.
(5) Prepare formal documentation to acknowledge that post-inspection activities have been completed.

APPENDIX I: SECURITY COMPETENCIES AND TRAINING NEEDS BASED ON JOB FUNCTION

I.1. COMPETENCIES

Identification of the core competencies necessary to perform the tasks required to achieve effective nuclear security is one of the fundamental elements of an effective nuclear security programme. Once identified, these necessary competencies would be compared to the current competencies of existing staff to establish human resource needs at the facility. This section will present an overview of the process of determining required core competencies for nuclear security at a RRRF. In so doing, this section will describe a process for developing a baseline list of core competencies. The example provided below can be used as a starting point for developing a customized list of competencies at a particular facility.

Competencies can be characterized as the knowledge, skills, attributes and even attitudes required to perform a job function or task. Knowledge is an organized body of information, usually of a factual or procedural nature. Skill is the proficient verbal or mental manipulation of data, people or things that can be learned. Skills can be job specific and are learned; these are commonly taught on-the-job. Attribute is the power to perform an activity and typically addresses education and innate or hereditary traits. Attitudes refer to drive, motivation and other inherent character traits required to succeed at a task. By reviewing the required job functions or tasks that would be undertaken successfully in a nuclear security programme at a RRRF, core competencies can be determined in terms of the required knowledge, skills, attributes and attitudes needed to perform the job functions or tasks.

As skills can be learned, the distinction between knowledge and skills can be difficult to clearly distinguish; therefore, the two will be considered together for this example. From the perspective of human resource development, attributes can be seen as job prerequisites and will, therefore, not be addressed in this publication. Universally, positive work related attitudes such as motivation and ethics are desirable regardless of the task and will not be formally addressed with each task.

The approach to define core competencies begins with a job analysis that details job functions, responsibilities and associated tasks or activities that would be performed at a RRRF to ensure an effective nuclear security programme. This Appendix provides an example of this approach for the RRRF security management. Only one task (below) within the planning and analysis process is used for the example. This approach would be replicated for all tasks within the nuclear security management system to assemble a complete list of required competencies.

Job function: Nuclear security processes: Planning and analysis

- Basis for robustness of nuclear security at RRRF
  - **Task 1**: Characterize RRRF (activities not listed).
  - **Task 2**: Identify facility targets:
    - **Activity 1**: Understand the State's material categorization guidance and unacceptable consequences.
    - **Activity 2**: Identify targets, including vital areas and other targets subject to sabotage.
    - **Activity 3**: Categorize facility materials for theft.
  - **Task 3**: Define site specific threat based on the State's threat criteria.

From the tasks and activities identified, competencies can be defined that will lead to a training needs assessment.

Task 2: Identify facility targets	
Activity	**Competencies (knowledge and skills)**
Activity 1: *Understand State material categorization guidance and unacceptable consequences.*	• Interpret State categorization guidance for nuclear and other radioactive material. • Understand radiological consequences assessment process.
Activity 2: *Identify targets including vital areas and other targets subject to sabotage.*	• Understand the facility and potential physical or computer sabotage scenarios. • Interpret safety reports and assessments to identify inappropriate assumptions. • Determine vital area sets for targets subject to sabotage.
Activity 3: *Categorization of facility materials for theft.*	• Apply State categorization guidance to facility materials. • Aggregate facility materials to determine grouped categorization and security areas. Aggregation is a process of combining dissimilar target materials and determining a combined material attractiveness category.

I.2. TRAINING

I.2.1. General

RRRF nuclear security management is responsible for defining and facilitating the training needs of its own personnel and for ensuring that any contract personnel are suitably trained or experienced so that all work is carried out in a secure and safe manner. Security management would also make sure that all personnel who are assigned security related duties have a sufficient understanding of the facility and its security features, as well as sufficient competence in areas such as management and supervisory skills, to ensure secure operation of the facility. This requires that personnel competencies be sustained through a programme of regular training and review complemented by developmental programmes intended to ensure the continuous availability of competent personnel to meet the anticipated organizational needs.

Security management would develop and implement an overall training policy. Such a policy demonstrates the commitment by management to the training of personnel and is an acknowledgement of the critical role that training plays in the secure, safe and reliable operation and maintenance of any RRRF. Training at a facility can consist of formal courses, on-the-job training, fellowships, informal meetings, awareness sessions, exercises, mentoring and personal study. These can be accomplished via in-house, national or international training sessions.

A training plan would be prepared on the basis of the long term needs and goals of the facility and would be an integral part of the overall security plan. The training plan would be evaluated periodically in order to ensure that it is consistent with both current and future needs and goals. Factors which would require a change to the training plan include:

— Changes to the organization’s operation or policies;

— Significant modifications to the facility infrastructure, environment, threat, response or other outside organizations;

— Feedback of operational experience from other facilities or the State's legislation or regulatory requirements.

The training needs for jobs that are important to security would be considered a priority, and relevant procedures, references, resources, tools, equipment and standards would be used in the training process to ensure, as far as practicable, that errors, omissions and poor practices are not accepted. For these critical jobs, the training environment would be as realistic as possible to promote positive carry-over from the training environment to the actual job environment. Adequate training of personnel needs substantial resources in terms of both personnel and finance. Sufficient time and thought would be devoted to defining the necessary training requirements and the establishment of an effective training programme.

In addition, for each position deemed important to security, a series of requirements for both initial and continuing training would be established. These requirements would vary according to the individual position, level of responsibility and specific level of competence required. Requirements would be prepared by persons having specific competence in facility operation and experience in developing training activities or by acknowledged experts in the field. Established requirements would relate to the tasks and activities to be performed.

It would be the responsibility of security management to ensure that:

— Training needs are continuously analysed and an overall training programme is defined.

— Performance of all trainees is assessed at various stages of training.

— Effectiveness of training is evaluated.

— Competence of persons occupying security important jobs is periodically verified and training/retraining is provided on a regular basis so that level of competence is maintained.

— Participation in training is given a high priority with respect to allocating resources.

Consideration would be given to enhancing training programmes for personnel at ageing facilities to compensate for losses of personnel due to retirement, job changes and other reasons. Training programmes would also be adapted to accommodate the special technical, administrative and operational needs of an ageing facility. Training would ensure that personnel are aware of technological developments and new security principles and concepts.

Some jobs require specific qualifications mandated by regulation. These would be formally addressed in the training programme and may be required to be included in the security plan as well.

I.2.2. Systematic approach

A systematic approach to training (SAT) could be used for the training of facility personnel. The SAT provides a logical progression of training needs from identification of the competencies required to perform a job to the development and implementation of training towards achieving these competencies, and then to the subsequent evaluation of the training. The use of a SAT offers significant advantages over more conventional, curricula driven training in terms of consistency, efficiency

and management control, leading to greater reliability of training results and the enhanced security and efficiency of the facility. Further information on this is available in IAEA-TECDOC-1057, Experience in the Use of Systematic Approach to Training (SAT) for Nuclear Power Facility Personnel.

Training would enable the efficient and effective acquisition of all knowledge and skills for those competencies required to perform the actual job in the workplace. These range from the application of technical knowledge through human factor related competencies to monitored job performance with feedback (development). Experience has shown that, initially, training programmes aim to provide technical knowledge that is of a more academic nature rather than being job related. Following this phase, technical skills related more to the actual job are introduced into the training programme, and then human factor related competencies (e.g. attitudes related to security and safety culture) are added. Finally, training is provided for individual development through monitored on-the-job performance with feedback from performance assessment. The most complete training programme will encompass all the training needed to attain full competence in a job, including all required competencies related to work/tasks performed within a team.

I.2.3. Training for emergency and security event response

A training programme for emergency and security event response would be established to instruct and evaluate facility personnel, as well as personnel from external response organizations, in:

— Confronting security event conditions;

— Coping with security events;

— Maintaining and improving the effectiveness of the response.

Emergency and security event response preparedness exercises would be designed to ensure that all personnel (facility and other participating organizations) possess the essential knowledge, skills and attitudes required for the accomplishment of non-routine tasks under stressful emergency conditions.

While the emergency or security event response assignments of facility personnel are based on routine job assignments under normal operations, personnel would also receive specialized training relevant to the duties they will have to perform during an emergency or a security event.

Training would be provided for all personnel who have assignments under the emergency response plan. The training programme for emergency and security event response would include the periodic performance of drills and exercises, which would be held to reinforce training and to assess the effectiveness of the response capability. In addition, there would be full-scale exercises that involve external organizations such as the police, fire services, ambulance teams, rescue teams and other response services. These exercises would:

— Demonstrate how effectively the response plan (or part of it) can be implemented.

— Confirm the adequacy of the plan to deal with emergency and security event response and identify potential improvements.

— Verify that the appropriate lines of communication are established and maintained.

— Verify that all individuals participating in the exercise are familiar with, and are capable of performing, the response duties assigned to them.

— Verify that the response and all related duties can be carried out in a timely manner according to the planned schedule and under stressful situations.

Exercise scenarios at the facility, as well as simulated attack scenarios, would be carefully prepared and would include training objectives, conditions for termination and reference sources. Furthermore, the conduct of a facility exercise would not create any condition that could jeopardize facility security or safety.

A general training programme would also be provided for on-site personnel who have no emergency duties to familiarize them with the procedures for alerting the appropriate personnel to emergency conditions. Similar training or, as the minimum, well-structured information briefing, would be provided to contractor personnel and other temporary personnel.

I.2.4. Records and reports

Training documentation consists of records and reports associated with the training programmes and with the trainees' performances. These records and reports would be used to assist management in monitoring the effectiveness of a training programme as well as in annual follow-up of personnel competencies by management. Training documents would also provide a historical record of changes made to a programme as a result of evaluation and feedback.

The person responsible for the training programme would periodically report on the status and effectiveness of training activities to the appropriate levels of management. Significant events or problems in training would be identified and reported when they occur.

I.3. TRAINING PROGRAMMES

All new employees starting work at a facility would be introduced to the organization and to their working environment in a systematic and consistent manner. General personnel training programmes would give new employees a basic understanding of:

— Their responsibilities;

— Security and safety work practices;

— Information security;

— Computer security acceptable use policy;

— The importance of quality programmes and of following procedures;

— The practical means of protecting themselves from the hazards associated with their work.

The amount of training to be provided on each topic would be commensurate with the individual's position and duties. The basic principles of a security and safety culture would be taught to all employees, and refresher training on general topics would also be periodically provided.

A security and safety culture would be frequently reinforced with all personnel involved in security related and safety related activities. In particular, the need for a questioning attitude, a rigorous and prudent approach and an adequate capability for communication would be emphasized in connection with all security related and safety related activities at the facility. Training programmes would stress the need for

an understanding of security and safety issues, include consideration of the possible consequences of security and safety errors, and deal specifically with ways in which such errors may be avoided or corrected if committed.

The training programme would ensure that all staff that handle sensitive information (including all management, employees and contractors) receive continuing on-the-job security training and periodic refresher information security training. The programme would maintain records of the formal training received and completed by all employees and contractors. It is essential that employees and contractors receive information security education and training commensurate with their individual responsibilities and needs.

I.3.1. Training programmes for managers and supervisory personnel

Training programmes for managers and supervisory personnel would emphasize the concept of a security and safety culture and include training in the making of successful presentations related to security and safety messages for subordinates. This will assist managers and supervisory personnel in promoting among their personnel the awareness that security and safety would be considered primary objectives in their day-to-day activities. The pre-eminence of security and safety over production would be emphasized.

I.3.2. Training programmes for operations personnel

The formal training of operators would cover relevant areas of technology to the levels necessary for the tasks to be performed. Emphasis would be placed on systems that are of security and safety significance.

I.3.3. Training programmes for security personnel

Training programmes for security personnel would emphasize the concept of a security and safety culture. They need to promote and support among personnel the awareness that security and safety would be considered primary objectives in day-to-day activities. The pre-eminence of security and safety over operations and production would be emphasized.

In particular, training would address these unique features and required security core competencies:

(a) Understanding of the overall organization, facility security objectives, relevant State security regulations, and corporate and cyber security requirements;
(b) Knowledge of the organization’s policies, directives, processes, procedures, change management, performance evaluation, operations, systems, event reporting and security culture (including their consequential accountability and responsibilities);
(c) Understanding of the specific and unique security issues for RRRF, including safety and security features and their interfaces;
(d) Relationships between threat characteristics (including insiders) and security features;
(e) Knowledge of and access to the State’s threat and DBT criteria and capabilities;

(f) Familiarization with risk management processes and identification of nuclear and radioactive material targets and of potential unacceptable consequences due to malicious acts;
(g) Planning and analysis of a security system (including access control) to accommodate the variety of users and service providers;
(h) Determination of the appropriate trustworthiness of personnel;
(i) Awareness of NMAC arrangements and procedures;
(j) Understanding of nuclear security principles and nuclear security systems and their operations;
(k) Selection, operation and maintenance of nuclear security systems and subsequent identification of design strengths and vulnerabilities;
(l) Assessment of security system effectiveness, testing and exercising;
(m) Development, improvement and maintenance of security procedures;
(n) Knowledge of State security requirements;
(o) Development and implementation of security and contingency plans;
(p) Familiarization of response operations, including response arrangements, strategies, tactics and weapons used, joint planning and exercises;
(q) Understanding of command and control of security event response;
(r) Understanding of the impact on security of the changing status of the RRRF and its associated installations;
(s) Capability to communicate (including oral, written and technical communication);
(t) Awareness of security, safety, safeguards and environmental interfaces and interactions.

CAS operators would also be trained in systems diagnostics, control actions, administrative tasks and human factors (e.g. attitudes and human–machine and human–human/teamwork interfaces).

Shift supervisors would additionally be trained in supervisory techniques and communication skills. Their training would, in general, be more broadly based than that of other operators.

I.3.4. Training programmes for response personnel

Training programmes for response personnel would emphasize the importance of security. They need to promote and support among personnel the awareness that security would be considered a primary objective in their day-to-day activities.

The training of response personnel would include facility guarding and off-site response personnel. In particular, the training of response personnel would address the following unique features and required security core competencies:

(a) Knowledge of organization policies, directives, procedures, operations, facility layout and systems;
(b) Understanding of specific and unique security issues for RRRF;
(c) Familiarization with risk management processes and identification of the nuclear and radioactive material targets and potential unacceptable consequences due to malicious acts;
(d) Knowledge of, and access to, State threat and DBT criteria and capabilities;

(e) Understanding of the relationships between threat characteristics (including insiders) and security features;
(f) Determination of the appropriate trustworthiness of personnel;
(g) Identification of security system strengths and vulnerabilities;
(h) Assessment of security system effectiveness, testing and exercising;
(i) Knowledge of response arrangements, including response operations, strategies, tactics and weapons used, joint planning and exercises;
(j) Understanding of the command and control of security event response;
(k) Capability to communicate (including oral, written and technical communication);
(l) Awareness of security, safety, safeguards and environmental interfaces and interactions.

I.3.5. Training programmes for maintenance personnel

Training programmes for maintenance personnel would emphasize the potential consequences for security or procedural errors. A review of experience with faults and hazards caused by errors in maintenance procedures and practices at the facility (or at other facilities/industries) would be taken into account in the training programmes, as appropriate.

I.3.6. Training programmes for other technical personnel and craftspersons

Personnel involved in computer systems, chemistry, radiation protection, nuclear engineering or other technical functions would receive security training appropriate to their jobs and responsibilities.

I.3.7. Training programmes for the trainers

Training instructors, both on-site and off-site, would have the appropriate knowledge, skills and attitudes in their assigned areas of responsibility. They would thoroughly understand all aspects of the contents of the training programmes and the relationship between these and the overall operation of the facility. This means that they would be technically competent and have credibility with the trainees and other facility personnel. In addition, the instructors would be familiar with the basics of adult learning and SAT, and they would have adequate instructional and assessment skills.

I.3.8. Review and modification of training programmes

The training plan would be periodically reviewed and modified as necessary. Review would cover the adequacy and effectiveness of training with respect to the actual performance of employees in their jobs. The review would also examine training needs, training programmes, training facilities and the training materials necessary to deal with changes to regulations, modifications to the facility and lessons learned from experience in the industry.

APPENDIX II: RRRF SECURITY PLAN

II.1. TYPICAL STRUCTURE OF A RRRF SECURITY PLAN

- Introduction
- Nuclear security requirements and objectives
  - Compliance regulation
  - Prevention of unacceptable consequences
- Scope and purpose of the security plan
- General facility description, facility purpose and characterization
- Facility integrated management system
  - Leadership for nuclear security
- Nuclear security management system
  - Operations
    - Physical security
    - Information security
    - Computer security
  - Processes
    - Addressing the threat
    - Access control
    - Security training
    - System sustainability
    - Compensatory measures
    - Process improvement
    - Security events reporting
  - Security forces
- Facility interfaces
  - Human resources
  - Procurement, contracts and agreements
  - Policies and directives
  - Processes and procedures
  - Records management and document control
  - Delegation of authority
  - Management of changes
  - Performance evaluation system
  - Safety, health and environment
  - Nuclear material accounting and control
- Contingency plan
- Review of the plan
- References

II.2. INTRODUCTION

This security plan is prepared and maintained by [*facility name*] RRRF security management and includes the information necessary to describe security objectives, approach and systems being used for the protection of nuclear and other radioactive material, these facilities, associated co-located facilities and information. The level of detail and depth of content within this plan is graded, commensurate with the level of threat and the potential severity of consequences of the material due to theft or sabotage.

This security plan is prepared in accordance with relevant regulatory requirements and licences. This plan is approved by [*competent authority name*] and can serve as a basis for regulatory inspections. It is, therefore, organized to address each security requirement and demonstrates how this facility is protected by the nuclear security system against the DBT or other threat criteria, which is based on the State's threat assessment.

II.3. NUCLEAR SECURITY REQUIREMENTS AND OBJECTIVES

The overall objective of a State's nuclear security regime (as per IAEA Nuclear Security Series Nos 13 and 14) is to protect persons, property, society and the environment from malicious acts involving nuclear and other radioactive material. The objectives of the State's physical protection[4] regime, which is an essential component of the State's nuclear security regime, are:

— Protecting against unauthorized removal and other unlawful taking of nuclear and/or other radioactive material;

— Ensuring the implementation of rapid and comprehensive measures to locate and recover, nuclear and other radioactive material which is lost, missing or stolen, and to re-establish regulatory control;

— Protecting nuclear and/or other radioactive material and associated facilities against sabotage.[5]

— Mitigating or minimizing the radiological consequences of sabotage.

The State's physical protection regime would seek to achieve these objectives through:

— Prevention of a malicious act by means of deterrence and by protection of sensitive information;

— Management of an attempted malicious act or a malicious act by an integrated system of detection, delay and response;

— Mitigation of the consequences of a malicious act.

The objectives mentioned above will be addressed in an integrated and coordinated manner, taking into account the different risks covered by nuclear security.

---

[4] From IAEA Nuclear Security Series No. 13, "Historically, the term 'physical protection' has been used to describe what is now known as the nuclear security of nuclear material and nuclear facilities."
[5] If required (see IAEA Nuclear Security Series No. 13, Section 5).

II.3.1. Compliance and regulation

This section outlines the State's security regulations and other organizational security objectives for which the nuclear security system is implemented.

Author guidance:
References to applicable State and international nuclear security instruments and to IAEA guidance publications that assist interpretation of security requirements would be cited here, as well as inserting the specific requirements contained within these that the site security system is addressing.

II.3.2. Prevention of unacceptable consequences

This section provides a description of all targets to be protected according to international and State nuclear security criteria, based on the State's unacceptable consequence criteria. The target description(s) and inventory include both targets of theft (along with the corresponding nuclear or other radioactive material by categorization level) and targets of sabotage (materials, equipment or processes) that control the reactor operation and safety systems. In addition, this security plan addresses every other unacceptable consequence and target of importance to the facility/organization.

Author guidance:
The basis for the State's unacceptable consequences would be referenced in this section. Further, the description of the targets would include their location and the nature of theft targets (i.e. quantity/activity, form, isotopic composition, enrichment) as well as the areas in which sabotage targets are located.

Additional information concerning the targets, consequence analysis and vital area definitions would be included in an Annex to the security plan. As inventories of material can vary with time, it is recommended to use the quantity that results in the highest security category for the expected life of the security plan to minimize the frequency of updating the plan.

The security plan would also identify the types of information that have been deemed sensitive for security purposes. Information can be hardcopy, visual, electronic and computer based or known by staff. The rationale behind the identification of the information as sensitive, the level of the information (e.g. highly confidential, confidential) and its location would also be described.

Computer based processes that control operations or are intended to provide safety and mitigation systems to prevent unacceptable consequences need to be protected against sabotage or compromise.

Suggested outline:

- *Make reference to:*
  - *International and State nuclear security criteria:*
    - *Theft categorization tables for nuclear and radiological materials;*
    - *State's unacceptable radiological consequence criteria.*
  - *Basis for including other significant consequences due to non-nuclear events (e.g. fire, flood, severe weather conditions).*

- *Description of all targets to be protected based on unacceptable consequence criteria:*
  - *Targets of theft (graded):*
    - *Location;*
    - *Quantity, form, isotopic composition, enrichment, activity;*
    - *Categorization level.*
  - *Targets of sabotage (graded):*
    - *Areas (vital areas);*
    - *Materials;*
    - *Equipment or processes that control reactor operations and reactor protection system.*
  - *Sensitive security information and rationale.*
  - *Other key processes (computer or non-computer controlled).*
- *Consequence analysis:*
  - *Analysis of the potential severity of radiological consequences;*
  - *Comparison with the State defined unacceptable consequences to provide a basis for security requirements and determination of the appropriate level of security.*
- *Evaluation.*
- *Review.*

II.4. SCOPE AND PURPOSE OF THE SECURITY PLAN

The [*facility name*] security plan details facility security arrangements to comply with State regulations and organizational objectives. This plan interfaces with other facility plans, such as the emergency plan, contingency plan, computer security plan, etc.

Author guidance:
This document is intended to be a single source of information to assist RRRF management responsible for the implementation of nuclear security in the development and maintenance of an effective and comprehensive site-wide nuclear security programme. It would also assist management in demonstrating the effectiveness of the programme to inspectors from the competent authority that is responsible for nuclear security oversight.

II.5. GENERAL FACILITY DESCRIPTION, FACILITY PURPOSE AND CHARACTERIZATION

This section provides a description of the facility, with special consideration given to the unique characteristics of [*facility name*] that may impact security (e.g. uses, design, users, co-located facilities and/or local environment) and the security system.

Author guidance:
The author would provide an overview of facility specific information that is relevant to the nuclear security arrangements.

Suggested outline:
- *Background*
  - *Reference:*
    - *Organization mission statement;*
    - *Legislation, competent authorities and operating licence;*
    - *Other relevant plans and agreements.*

- *General description of research reactor facility:*
  - *Location of facility and environs.*
  - *Characteristics of the research reactor, such as:*
    - *Thermal power;*
    - *Open pool or vessel type;*
    - *Fuel, moderator and coolant.*
  - *Purpose of the research reactor:*
    - *Material testing reactor;*
    - *Training;*
    - *Research;*
    - *Radioisotope production;*
    - *Other.*
  - *Non-staff users of the facility (researchers, students, others).*
  - *Facility operating hours.*
  - *Facility stakeholders.*
  - *Access control of persons (staff and non-staff) and vehicles.*
  - *Number of staff (staff turnover).*
  - *Number of users, contractors and visitors (estimated numbers).*
  - *Layout of buildings, floors, entry/access points.*
  - *General description of co-located facilities, such as:*
    - *Radioisotope production facility;*
    - *Fuel fabrication facility;*
    - *Storage of fresh fuel, spent fuel or radioactive sources;*
    - *Radioactive waste storage and disposal;*
    - *Laboratories and hot cells;*
    - *Irradiation facilities;*
    - *Other facilities.*
  - *Nature of business.*
  - *Operations.*
  - *Infrastructure.*
  - *On-site storage and movement of nuclear and other radioactive material (frequency, material characteristics).*
  - *Reference to existing descriptive documents:*
    - *Facility safety and environmental plans and licences;*
    - *Security regulations and licences;*
    - *Facility security related policies and procedures.*
  - *Surrounding environment:*
    - *Nearby facilities;*
    - *Sketch of the location of the facility relative to areas accessible to the public;*
    - *Location of nearest public thoroughfares;*
    - *Distance from nearest appropriate police/response force.*
  - *Unique characteristics of the research reactor that may impact on its nuclear security at the facility as detailed in Section 2 above.*

II.6. FACILITY INTEGRATED MANAGEMENT SYSTEM

This section outlines the formal documentation, policies, procedures, practices and actions that are in place to implement disciplined and structured operations that support facility success.

Author guidance:
Insert the approved organizational structure (e.g. diagram), including detailed structure of the facility security organization. The organizational structure would include:

- *Roles and responsibilities of RRRF personnel with associated accountability, authority, autonomy and resources as defined by management and communicated to the organization;*
- *Relationships with external security organizations identified within the structure (e.g. identification of the position that manages the relationship with external response force);*
- *Contracted organization or separate law enforcement organization that provides on-site or off-site response forces through an agreement.*

II.6.1. Leadership for nuclear security

This section outlines management's leadership role for nuclear security. Managers are responsible for ensuring that appropriate standards of behaviour and performance associated with a nuclear security culture are set and that expectations as to the application of these standards are well understood. Management will, through application of incentives and disincentives, influence the priority given to nuclear security throughout the organization. Management would also ensure that there is a clear understanding within the organization of the security roles and responsibilities in relation to the accountability of each individual, including clarity concerning all levels of authority and lines of communication.

Author guidance:
Leadership is one of the most important roles of upper management. Through leadership, managers influence the attitudes and culture of the organization and personnel. How this is addressed at the facility would be described in the plan.

Suggested outline:

- *Describe activities, programmes and efforts undertaken to lead the effort to promote a security culture.*
- *Reference existing policies, charters or mission statements expressing executive management support for the nuclear security programme, including a demonstration of support for a strong and effective nuclear security culture that incorporates incentives and disincentives.*

II.7. NUCLEAR SECURITY MANAGEMENT SYSTEM

II.7.1. Operations

The security plan describes in detail the primary security operational elements of physical, personnel, information and computer security.

II.7.1.1. Physical security

The physical security system achieves its objectives through the integrated deployment of technical and administrative measures to deter, detect, delay and respond to malicious acts. This section details the physical security system, its measures, and how it addresses the security objectives and requirements for protection

against the DBT or other defined threat criteria (following a graded approach) in relation to the targets as defined in this security plan.

Author guidance:
The description of the physical security system is organized by areas[6] and describes, at each concentric security area (e.g. the protected area), how:

- *The boundary of the area is delineated (e.g. by a fence);*
- *Detection of a malicious act is achieved (e.g. type of sensor);*
- *Detection is assessed (e.g. by camera);*
- *A malicious act is delayed by the area (e.g. by fence);*
- *Access control and contraband detection are achieved by the area (e.g. fingerprint biometric to release an electric strike on a metal security door).*

In addition, the description of the physical security would provide:

- *A description of the CAS and secondary alarm station, if it exists, including its location and the pathways of its network infrastructure;*
- *The hardness of the CAS/secondary alarm system walls and doors;*
- *The equipment within to annunciate detection, permit assessment and communicate to on-site guards and off-site response forces.*

The CAS/secondary alarm system description would include the CAS staffing levels during both working and non-working hours, and the access control procedures to the CAS and its supporting infrastructure assets.

Suggested outline:

- *Show security areas by overlaying their boundaries on a facility layout diagram.*
- *Individually describe the physical security on the boundary for each identified area, including:*
  - *Technical and administrative measures, including:*
    - *Deterrence efforts, including signage and visible impression of security robustness, etc.*
    - *Detection of intrusion into the area and supporting assessment of alarms, including:*
      - *Detection technology or method (e.g. passive infrared sensor, guard patrol);*
      - *Assessment approach (e.g. cameras with lighting, guard towers).*
    - *Access controls for entry/egress into the areas, including:*
      - *Access points;*
      - *Emergency exits points;*
      - *Material entry/exit points;*
      - *Vehicle entry/exit points;*

[6] Security systems are established in layers/areas/zones primarily by establishing measures on the boundary of the layer/area/zone. Security would be balanced around the layer/area/zone. An example of a layer/area/zone is the protected area as described in IAEA Nuclear Security Series No. 13. A facility will typically have several nested security layers/areas/zones.

        - *Physical barriers across access point (doors, turnstiles, locks) for each entry/exit point;*
        - *Access keys (e.g. mechanical key, badge, fingerprint) for each entry/exit point;*
        - *Detection across access point for each entry/exit point;*
        - *Handling of visitors to area;*
        - *Detection of introduction or removal of contraband items, including nuclear and other radioactive material on gaining access into the area for each access/exit point (e.g. metal detector, guard package search).*
      - *Delay barriers and their resistance to penetration (e.g. two courses of hollow brick wall, chain link fence):*
        - *Describe any imbalances in barrier resistance to penetration along the area boundary and describe mitigating compensation.*
      - *Guards and response time to alarms on areas.*
    - *Detail protection measures for each area that are implemented to protect against insiders, including:*
      - *Two person rule;*
      - *Limits to individual access based on 'need to access' (refer to IAEA Nuclear Security Series No. 8);*
      - *Surveillance systems over targets and processes;*
      - *Tamper indicating devices;*
      - *Procedural controls over activities involving targets of theft or sabotage.*
    - *On-site transport/movement of nuclear or other radioactive material:*
      - *Transport vehicle;*
      - *Procedures;*
      - *Locks/barriers;*
      - *Administrative procedures;*
      - *Frequency;*
      - *Escort/guard;*
      - *Security compensatory measures;*
      - *Planning and confidentiality.*

II.7.1.2. Personnel security

This section describes how [*facility name*] follows the State's and the regulatory body's criteria for establishing trustworthiness and reliability of persons who require authorized access to facilities or sensitive information, including users, visitors and contractors.

Author guidance:
Personnel security is applied to persons who require authorized access and would:

- *Confirm that honesty, reliability and trustworthiness of personnel meet national standards, commensurate with access levels granted to facilities.*
- *Involve background and trustworthiness checks to reveal any indicators that might raise concerns about tendencies, susceptibility or willingness and desire to commit a malicious act (such as drug or alcohol addiction, mental illness, financial problems, violent or criminal behaviour, etc.).*

Suggested outline:

- *Initial process:*
  - *Describe the process of how personnel are screened by the relevant authorities (see Section 5.3) and by the facility prior to employment and the granting of unescorted access to minimize the likelihood of an insider threat.*
- *Subsequent monitoring process:*
  - *Describe the process of periodic follow-up investigations and the frequency and description of formal periodic checks to ensure ongoing monitoring of personnel trustworthiness.*
  - *Describe the process used to collect information concerning trustworthiness and facility criteria that might trigger a follow-up investigation, such as:*
    - *Receiving updates to criminal records;*
    - *Updates to financial changes;*
    - *Updates to personal status;*
    - *Monitoring personnel changes in behaviour:*
      - *Procedures and guidance to identify and report behaviour changes.*
  - *Describe measures to ensure that the process is not vulnerable to a single insider.*

II.7.1.3. Information security

This section details the sensitive information protection programme to address the protection of information that could compromise nuclear security or otherwise assist in the carrying out of a malicious act against a nuclear facility, organization or transport. For example, this security plan is sensitive and needs to be protected in an appropriate manner.

Author guidance:
The sensitive information protection programme ensures confidentiality, integrity, accessibility and availability of information through classification, information controls and information accountability, as well as security measures for the protection of information. As with physical security, information sensitivity needs to be identified, classified and graded to reflect the severity of potential consequences if the information is compromised. Access to sensitive information is restricted to persons having the appropriate clearance, authorization and need to know based on a strict evaluation.

This section would describe how access to sensitive information is granted to persons having the appropriate clearance and the need to know. It would also describe information security measures such as authentication, access authorization and compartmentalization, access detection, storage rules and access delay.

Types of information that have been deemed sensitive for security purposes can be hardcopy, visual, electronic and computer based or known by staff. The rationale behind the identification of information as sensitive, the level (e.g. highly confidential or confidential) of the information and the location of the information would also be described.

Guidance on the classification to be applied to an information asset would be provided by the relevant competent authorities in the form of a classification guide or guidance. Such a document groups information on particular topics and indicates the sensitivity of the information. Those who originate sensitive information would use such a guide when deciding on the appropriate classification level.

Suggested outline:

- *Describe the process of defining sensitive information used or stored at the facility and list the criteria for sensitive information.*
- *Describe the frequency and criteria for review of the sensitive information programme.*
- *Describe the process for determining access rights to information.*
- *Describe the information security measures, including:*
  - *Classification of information;*
  - *Authentication;*
  - *Need to know designation;*
  - *Access authorization and compartmentalization;*
  - *Access detection;*
  - *Storage rules;*
  - *Access delay.*

II.7.1.4. Computer security

The computer security plan for [*facility name*] can be found [*insert reference if such a plan exists for the facility*].

Author guidance:

Assess the vulnerability of networks and other digital systems against the defined threat and develop appropriate measures to protect the integrity, reliability and confidentiality of the processes, computer systems and electronic data (refer to IAEA Nuclear Security Series No. 17). The security manager needs to provide oversight to ensure that computer security is implemented to ensure that defence in depth exists to counter computer attacks.

Suggested outline:

(a) Computer asset management:

(i) List of critical computer systems;

(ii) List of critical computer systems applications;

(iii) Network diagram, including all connections to external computer systems.

(b) System security design and configuration management:

(i) Fundamental architecture and design principles;

(ii) Requirements related to the different security levels;

(iii) Identified computer security requirements for suppliers and vendors;

(iv) Security for the computer asset life cycle.

II.7.2. Processes

II.7.2.1. Analysis and planning

This section provides a brief description of the planning and analysis of requirements for the nuclear security system based upon State threat criteria (e.g. DBT or threat assessment based criteria) against which the nuclear security system will provide protection. The process for using threat information to design and evaluate nuclear

security, the process for incorporating local threat conditions and the process for communicating and addressing changes in actual threat conditions are described.

Author guidance:
If a threat criterion is not provided, then refer to the security requirements provided by the competent authorities.

Suggested outline:

- *Refer to the DBT or threat assessment based criteria.*
- *Describe the process to define and incorporate local threats into the threat criteria.*
- *Describe how threat criteria are used to design and evaluate the nuclear security system.*
- *Describe how temporary changes in threat conditions are communicated and addressed.*

II.7.2.2. Access control

This section describes the process to control access and compartmentalize areas so as to limit the number of persons granted unescorted access into security controlled areas and to control persons with escorted access.

Author guidance:
The plan would describe the method of determining access rights (including approvals from security, operations, radiation protection and industrial safety officers) and the manner in which access is granted and removed. Address the validation of authorizations and the determination of need to access by management. Describe protection measures applied to badging equipment, enrolment stations and access databases to ensure that the system is not exploited.

Suggested outline:

- *Describe the graded approach policy for access to the facility, controlled areas and sensitive information and include:*
  - *The approach for implementing additional access controls (e.g. surveillance, guard assisted access, two person control) including the policy/criteria for when it is needed.*
- *Describe the process for requesting and granting approvals for physical and logical access and need to access.*
- *Describe the protection measures applied to badging equipment, enrolment stations, access databases and other critical computer systems to ensure that these systems are not compromised.*
- *Describe the process to evaluate access control effectiveness.*
- *Describe the process for permitting visitors onto the site and the rules for escort.*
- *Describe the process for granting emergency access to responders to emergency situations, such as fire, medical or natural disasters, and:*
  - *Describe differences in approach depending on point of access.*
- *Describe the process for granting temporary access to inspectors, investigators or others with authority and:*
  - *Describe differences in approach depending on point of access.*

- *Describe the access record management processes, including:*
  - *Authorizations and access issuance;*
  - *Controls to prevent compromise of access issuance.*
- *Describe the management of locks and keys used to ensure that access control is not compromised, including:*
  - *Maintaining an authorized persons list;*
  - *Secure key storage (and badges, combinations/PIN codes);*
  - *Measures to prohibit removal of keys from the facility or duplication by unauthorized personnel;*
  - *Measures to verify return of all keys from employees terminating or whose job responsibilities no longer require access;*
  - *Requirement to report loss of key and measures to compensate;*
  - *Process to change combinations or codes immediately if an employee no longer requires access or a compromise has occurred;*
  - *Frequency of periodic physical inventory of keys and locks.*
- *Describe items prohibited (e.g. cameras, weapons, drugs, personal removable media).*
- *Detail arrangements for staff operations during normal working hours to include:*
  - *Locking and unlocking the doors/areas of the facility at the beginning and at the end of the working day;*
  - *Activating and deactivating the intrusion detection system.*

II.7.2.3. Security training

This section describes security training of personnel to ensure that procedures and work are carried out in a secure manner.

Author guidance:
The plan would describe the process to provide security awareness training along with other methods to convey individual nuclear security roles and responsibilities of all personnel, as well as the frequency of the awareness training.

Security management is also required to make sure that all personnel who are assigned duties that can affect security have a sufficient understanding of the facility and its security features, as well as sufficient competence to ensure secure operation of the facility.

The plan would include a listing of necessary competencies and corresponding training courses and descriptions of training needs by job position, qualifications of the trainers, frequency of training and training records.

Suggested outline:
- *Describe the security awareness training for all personnel, including its frequency and the responsibilities assigned to personnel through the awareness training.*
- *Describe the security training programme for personnel that have roles and responsibilities that could impact security (including security personnel) at the facility, including:*
  - *Type and level of training needed for each individual (or position);*
  - *Training topics to be addressed;*
  - *Frequency of training;*

- *Assigned responsibilities for developing training materials and conducting training;*
- *Maintenance of course materials, training records to be kept and student evaluations;*
- *Revision of the training programme.*

- *Describe other awareness communication and security culture promotion.*
- *Describe the process used to determine the effectiveness of the training programme.*

II.7.2.4. System sustainability

This section addresses the efforts and programmes of [*facility name*] to ensure that the effectiveness of the security system will continue for the life of the facility. This section includes budgets resources, equipment maintenance, calibration, testing, and performance assurance.

Resources and budgeting

This section describes the process used to secure adequate resources and budgets to implement, manage, operate and sustain the nuclear security programme of the facility.

Suggested outline:
Address the process for ensuring the availability of resources and budget for equipment, staff, training, testing and system improvement.

Maintenance, calibration and testing

This section describes the maintenance, calibration and test programmes at the facility related to ensuring the effectiveness of security system equipment.

Author guidance:
The security plan would define a preventative and corrective equipment maintenance programme and describe the ability to respond to equipment failures. Include a process description for maintenance records.

The security plan would list the equipment type requiring calibration. It would address the criteria for equipment calibration and the frequency of calibration.

The plan would describe equipment testing to ensure that equipment is functional and effective and would include the processes of implementing test procedures, the frequency and documentation of testing and follow-up corrective actions.

Finally, describe the processes used to authorize and oversee maintenance, calibration and testing. Also, include assurances that these actions are performed as required.

Suggested outline:

- *Describe the approach used to ensure that equipment and systems are functioning as designed, including:*
  - *Preventative maintenance (regular basis);*
  - *Corrective maintenance to respond to equipment malfunction or failure;*
  - *References to maintenance procedures and schedules.*

- *Describe equipment calibration and include references to calibration procedures and schedules.*
- *Describe test actions to confirm that security equipment is effective and reference test procedures and the frequency of testing.*

Performance assurance

This section describes the security system performance assurance programme, including the integration of equipment, personnel, and procedures at the facility level or subsystem/area level.

Author guidance:

The description here would address the approach to self-assessment, including the types and frequencies of performance testing of people, procedures and equipment (individually or in combination). Describe the approach to adversary scenario development and analysis, which is conducted to identify security effectiveness and vulnerabilities and to determine solutions and compensatory measures for all identified vulnerabilities.

The plan would also detail the records that are kept for self-assessments and performance tests and exercises. See IAEA-TECDOC-1276 for further information on performance testing and analysis.

Suggested outline:

- *Describe the process for performance assurance. Include how the performance assurance programme provides confidence that the security system is operating as designed and is effective (tests can address detection, assessment, communication, delay and/or response).*
- *Reference or describe the process for implementing the performance assurance programme, including exercises of equipment, personnel and procedures at the facility level and/or subsystems/area level. This description includes the process to:*
    - *Identify the need and scope of performance tests;*
    - *Develop performance tests plans and procedures, including evaluation criteria (e.g. response time, detection success).*
- *Describe self-assessment of the effectiveness of the security system or computer security controls involving:*
    - *Identifying adversary scenarios that could challenge the security system;*
    - *Including test results;*
    - *Evaluating system response to identify vulnerabilities;*
    - *Determining solutions and compensatory measures to identified vulnerabilities.*

II.7.2.5. Compensatory measures

This section describes the compensatory measures programme, which is necessary to compensate for temporarily compromised, degraded or inoperable security related equipment, systems or components and to address security vulnerabilities introduced by abnormal situations (e.g. temporary security vulnerabilities introduced by events such as severe weather, non-malicious civil unrest, equipment failure, publically known critical computer vulnerabilities).

Author guidance:
Compensatory measures would provide a commensurate level of protection to offset deficiencies introduced by compromised, degraded or inoperable equipment, system or component and to address security vulnerabilities introduced by abnormal situations.

Suggested outline:

- *Describe the process used to determine appropriate security measures that can effectively compensate for temporary degradation or inoperability of security related equipment, systems or components and for abnormal situations.*
- *Describe the process used to gain approval by the competent authority.*

II.7.2.6. Process improvement

This section describes the formal programme to continually improve the processes supporting the nuclear security system.

Author guidance:
The process improvement programme would assimilate information gathered from operating experiences and corrective actions.

Suggested outline:
Describe or reference the programme to continually improve the processes supporting the nuclear security system.

II.7.2.7. Security events reporting

This section describes the programme for identifying and gathering information, reporting and investigating site related security events (including required external reporting).

Author guidance:
The plan would describe what, when, how and by/to whom events would be reported, the reporting time frame and the manner in which event reports are documented.

Suggested outline:

- *Describe what needs to be reported and how, in accordance with the requirements of the competent authority, including:*
  - *Types of event or incident required to be reported to the competent authority and what the required time frames are;*
  - *Training for staff on procedures and their responsibility to report events;*
  - *Process for conducting an investigation in cooperation with the competent authority;*
  - *Root cause determinations of events and the process for taking corrective actions to prevent recurrence;*
  - *Process for maintaining documentation of reportable events and corrective actions.*

II.7.3. Security forces

This section describes the guards that operate the security system on a daily basis and protect the facility and its personnel as well as the response forces that provide a response to a security event at [*facility name*].

II.7.3.1. Guards

This section describes the guard forces that operate elements of physical security (e.g. access control points and alarm stations), verify access authorization, conduct contraband searches, perform patrols, assess and communicate alarms to response forces and in general enforce adherence to procedures by on site personnel.

Author guidance:
The security plan would include guard staffing and would reference the operating security procedures for guards within the site, including procedures related to patrol, alarm enabling and disabling, key control and alarm response. The qualifications and training of guards would be referenced and included in the training process.

Guard forces might also serve as the first responders to a security event and deter, delay, interrupt and even neutralize the adversary. To do so, guards would assess and contribute to the response in a timely manner (i.e. in time to prevent adversary success). Guard forces would be recruited, managed, trained and tested. Guards would be provided with written operating procedures.

Guard forces operate these elements of the security system:

- *Access control points and alarm stations;*
- *Assess and communicate alarms to response forces;*
- *Verify access authorization;*
- *Conduct contraband searches;*
- *Perform patrols;*
- *Enforce adherence to procedures.*

Suggested outline:

- *Describe guard staffing levels and necessary competencies, including:*
  - *General and task specific competencies (such as CAS operations);*
  - *Skills and prerequisite training required;*
  - *Authorizations and legal authorities.*
- *Describe how guards operate security system elements within the site, including:*
  - *Security equipment assigned to guards (e.g. flashlight, handcuffs, radios);*
  - *Security system equipment;*
  - *Access controls, including searches;*
  - *Patrols and posts;*
  - *Key control;*
  - *Communications;*
  - *CAS operations;*
  - *Alarm response;*
  - *Enforcing adherence to security rules;*
  - *Interaction with internal and external responders;*
  - *Testing and exercises;*
  - *Response to security events.*

II.7.3.2. Response forces

This section describes the response forces that respond to security events at [*facility name*].

Author guidance:
Response forces are qualified persons, either on-site or off-site, who are armed and appropriately equipped and trained to counter any nuclear security event. Response forces are normally activated by the facility guards on the assessed detection of an attempted malicious act. Response forces would be familiar with the site, the targets to be protected and their hazards, and the rules of engagement. The response would be based upon the contingency plan and would be exercised periodically, in coordination with facility personnel and guards. Furthermore, response forces would be prepared to address the possibility that material might be moved off-site, and in this regard, written plans and tactics for the recovery of stolen material would also be exercised.

Response forces would respond in a timely manner and with sufficient numbers of appropriately equipped and armed personnel. They would be deployed in a tactical manner to arrest, effectively incapacitate, neutralize and/or cause an adversary to flee prior to the completion of the malicious act, in accordance with policy and agreements. This includes using response tactics that are in accordance with State policy on rules of force.

The security plan would address situations during a security event where nuclear or other radioactive material is removed from the facility perimeter, both when the whereabouts are known and when they are unknown.

The security plan would outline the arrangements for external response forces.

Suggested outline:

- *Describe the response forces and include details on:*
  - *Who the response forces are and what authorities and rules of engagement exist for each.*
  - *The process used to ensure that the response forces are capable of effectively responding against the defined threat in a timely manner.*
  - *The familiarity of the response forces with the facility. Provide specifics for:*
    - *Interactions with facility guards or other staff;*
    - *Exercises and tours at the facility;*
    - *Communication protocol and equipment between on-site and off-site forces;*
    - *Familiarity with site hazards, such as nuclear or other radioactive material.*
  - *Transition of command and control.*
  - *The agreement between facility and response forces.*

II.8. FACILITY INTEGRATED MANAGEMENT SYSTEM INTERFACES

The facility IMS consists of formal documentation, policies, procedures, practices and actions that implement disciplined and structured operations that support facility success.

Author guidance:
This section outlines the parts of the security programme that are often provided by the broader, or corporate, organization. The security programme may already be well developed and delivered by an existing IMS. However, there are situations where all or parts of the security programme may not exist and require specific development within the security programme.

Provide a description of how the following are achieved or reference the actual document (title, number, version) that identifies the following facility IMS interface.

II.8.1. Human resources

Suggested outline:
- *Trustworthiness requirements incorporated in pre-recruitment and post-recruitment processes;*
- *Compliance with security obligations and responsibilities documented as a condition of employment;*
- *Security awareness and education as part of employment;*
- *Disciplinary process established for breach of security obligations and responsibilities;*
- *Established competencies for the appointment of security personnel;*
- *Recording of information on employee dissatisfaction.*

II.8.2. Procurement, contracts and agreements

Suggested outline:
- *Trustworthiness of supplier/contractor to be addressed prior to the tender process.*
- *Information confidentiality to be addressed during the tender process.*
- *Documented security concerns within the terms and conditions of contract, including:*
  - *Protection of confidential information;*
  - *Compliance with security obligations and responsibilities;*
  - *Non-compliance penalties.*
- *Reference to policy on security provisions in contracts and agreements.*

II.8.3. Policies and directives

Suggested outline:
Reference the relevant policies and directives that could influence the facility's nuclear security programme (e.g. parking directive that restricts vehicles from parking too close to facilities or a public relations policy on restricting the taking of photographs).

II.8.4. Processes and procedures

Suggested outline:
Reference the facility approved procedures and processes that allow for the development, implementation, testing, approval, communication/training, and maintenance of written procedures.

II.8.5. Records management and document control

Suggested outline:
Reference the facility approved programme and procedures for records management and document control that are relevant to nuclear security.

II.8.6. Delegation of authority

Suggested outline:
Reference the facility approved formal process pertaining to both permanent and temporary delegation of authority.

II.8.7. Management of changes

Suggested outline:
Reference the facility approved processes for changes that could directly or indirectly affect the security function (e.g. a process to ensure that any change to either safety, security or operations does not adversely affect the other).

II.8.8. Performance evaluation system

Suggested outline:
Incorporate security specific performance indicators in the approved management performance evaluation system (e.g. number of reportable security events that occur in a year), including:

- *Measurement;*
- *Assessment;*
- *Improvement.*

II.8.9. Safety, health and environment

This section describes the interfaces between safety, health, environment and nuclear security.

- *Address the process for ensuring conflict resolution when security goals are at odds with safety goals.*
- *Address the process for ensuring conflict resolution when the need to protect sensitive information is in conflict with the safety culture of 'openness of information'.*
- *Reference how the safety security interface is integrated in processes such as:*
    - *Defining areas in access rules for both safety and security purposes;*
    - *Using compartmentalization for both confinement and intrusion delay;*

- *Using safety studies for the discussions on adversary scenarios and consequence analysis;*
- *Analysing how the redundancy or diversity of safety systems can complicate an adversary's sabotage scenario;*
- *How to minimize the security risks from material accounting checks and inspection;*
- *How to minimize the security risks from the need for quick egress for personnel or the need for rapid entry of emergency responders in emergency situations.*

II.8.10. Nuclear material accounting and control

This section describes how the NMAC systems can provide detection of theft or diversion of nuclear and other radioactive material that is in storage, in use or in transit during on-site movement, particularly by an insider.

Author guidance:
Describe how the facility utilizes material measurements and radiation detection equipment to provide assurance that material stewardship is not compromised. Specifically, describe how systems are used to provide assurance that materials are not stolen or diverted without detection.

Suggested outline:

- *Define interfaces and security objectives with NMAC arrangements. If there is no NMAC arrangement, then one would be instituted specifically for security and:*
  - *Describe how movements of nuclear or other radioactive material are managed so as not to result in a condition where security thresholds are exceeded (e.g. more material than the maximum allowable threshold defined in IAEA Nuclear Security Series No. 13 being brought into a security area).*
- *Describe the methodology used for conducting NMAC measures.*
- *Describe the frequency of accounting updates/measurements.*
- *Describe the minimum thresholds for measurements of protracted theft.*
- *Provide details regarding the means of checks, including:*
  - *Visual checks to verify that nuclear and/or other radioactive material has not been tampered with;*
  - *Verification that there was no intrusion (e.g. use of seals or tamper indicating devices).*
- *Describe access to documentation of records.*
- *Describe procedures for communicating discrepancies to security.*
- *Describe procedures for security response to discrepancies in accounting/inventory.*

II.9. CONTINGENCY PLAN

The contingency plan describes the predetermined sets of actions to be taken in the event of a confirmed detection of an attempted and/or in progress malicious act so as to effectively counter such acts. The [*facility name*] contingency plan is contained in [*insert location/reference*]. The plan is developed by [*insert participants*] and is

updated on a [*insert frequency*] basis or upon changes to the facility or response force configuration.

Author guidance:
The contingency plan can be a part of the security plan or it can be a separate contingency plan document. This plan would provide information as to who develops, updates and possesses the plan. Further, the plan would explain how effectiveness is validated through exercises and analysis. The facility contingency plan would integrate with, and complement, the State's contingency plan.

II.10. REVIEW OF THE PLAN

This section details the review of the plan to ensure that the conditions and assumptions under which it was developed are still valid. The [*facility name*] security plan will be reviewed [*insert frequency*] or whenever changes to the facility or threat impact permanently on security and the plan will be updated as necessary.

Author guidance:
If changes to the security plan are needed, they would be introduced by the responsible facility personnel and approved by the competent authority. In addition, the plan would be reviewed and updated whenever changes to the facility, material inventory, security system, regulations or threat characteristics takes place. The plan would include a means of version control to ensure that all parties are working to the current and approved security plan.

II.11. REFERENCES

Author guidance:
Cite documents, legislation, guidance, licences, plans, MOUs, etc., here.

APPENDIX III: DRAFT RESPONSE MEMORANDUM OF UNDERSTANDING

Term	Definition
Central Alarm Station (CAS)	The CAS will contain communications resources for the FSG to interface with the OSRF and outside personnel. This centre can be the event site command location during an event. The alarm monitoring location for on-site security alarms. The CAS contains direct and redundant communication links to the OSRF.
Design Basis Threat (DBT)	The DBT outlines the set of adversary characteristics for which the operators and State organizations together have protection responsibility and accountability. The division of these responsibilities may vary according to States. The DBT is used to define the requirements given to the operators and to clarify the protection functions that are the responsibilities of the State authorities.
Emergency Operations Centre (EOC)	The EOC supports the CAS during a security event. The EOC does not control or command the deployment and operation of the OSRF but will provide all necessary information and cooperation to the Event Commander or Chief of OSRF.
Event Commander	A member of any responding agency with event command accreditation. The Event Commander has command and control of all resources and services present during the security event.
Facility	Facility refers to the research reactor facilities and co-located facilities and activities.
Facility Security Guard (FSG)	Facility security personnel who are located at and respond at the facility site. They patrol, perform access control and searches, and monitor and respond to site response to alarms.
Facility Security Operations Manager (FSOM)	The facility staff member responsible for all security operations at the facility.
Off-site Response Force (OSRF)	Off-site local, national or military force(s) or any other force trained in the use of firearms that is authorized under any act or regulation to carry firearms and is qualified to use them to provide adequate response to an event relative to the DBT.
Security Event	Any threat that creates a risk to staff, the public or the environment as a result of: (a) Theft of nuclear material that could result in public radiation exposure; (b) Sabotage which results in a potential release of radioactivity; (c) Other criminal acts that could result in harm to staff, contractors or the public; (d) Any other event that has implications for nuclear security.
Security Exercise	A scenario based training activity designed to test the facility's security plans and procedures as well as off-site support plans, response and coordination. Exercises may directly or indirectly involve all site personnel and outside agencies.
Senior Emergency Officer (SEO)	A facility management representative who is responsible for the operation of the EOC during a site emergency.

III.1. INTRODUCTION

This MOU outlines the agreement between the RRRF and the OSRF for terms and conditions of both parties in relation to the following:

- The OSRF will provide an adequate, appropriate and effective response to calls for assistance as a result of a security event relevant to the RRRF DBT.
- The OSRF will participate in familiarity, preparedness activities and security exercises related to the provisions of the response force services.
- The facility will provide facilities, technical support, expertise and resources to support response force operations and training in relation to the RRRF.

This MOU will be in effect for [*X*] years but is subject to review and renegotiation at the request of either party (annually or otherwise) if changes occur to the governing conditions such as operating regulations, statutory authorities or threat levels (DBT).

III.2. POINTS OF CONTACT

The FSOM will be the primary facility site contact for security and response force issues with the OSRF. The on duty FSG shift supervisor will act as an alternative contact for security and response force issues.

The FSOM and/or the Chief of the OSRF are the contacts for the purposes of this MOU.

III.3. INITIAL NOTIFICATION AND RESPONSE

III.3.1. Initial notification

When a security event occurs at the RRRF, the CAS will determine whether to contact the OSRF by the agreed upon communication arrangements.

III.3.2. Initial response on-site

The FSG are the first responders to any event within the RRRF. The decision to deploy responders off-site will be made in consultation with the Chief of the OSRF and the FSOM or designates.

III.3.3. Response time

Following communication from the CAS, the OSRF will deploy, in a timely manner, appropriate and adequate response personnel to the facility to assist the FSG with the security event.

III.3.4. Response team resources

The OSRF may deploy and/or arrange with other response forces. At the request of the OSRF, the Incident Commander will deploy, as agreed, additional services to assist at the facility. Agreement on the expected strength and estimated time of arrival of each response force's primary response and supporting response elements needs to be specified as an Annex to the MOU and would include the following:

(i) Tactical response units;

(ii) Crisis negotiator;

(iii) Canine team;

(iv) Explosive disposal;

(v) Emergency response teams;

(vi) Chemical/biological/radiological/nuclear (CBRN);

(vii) Forensic identifications services;

(viii) Technical traffic collision investigation;

(ix) Dangerous goods coordinator;

(x) Underwater search and recovery;

(xi) Any other service provided by the OSRF and/or supporting units deemed necessary by the Incident Commander.

III.4. RESPONSIBILITIES OF THE OSRF

III.4.1. First member at the scene

The first member to arrive at the scene shall:

(i) Report to the CAS;

(ii) Receive a briefing from the FSOM or designate;

(iii) Assess and verify the nature of the event;

(iv) Notify the Chief of the OSRF or his designate of the event; and

(v) Assume command of the response until relieved by a member of higher rank.

III.4.2. Event Commander

The Event Commander shall proceed to the CAS and assume overall command of operations from the supervisor in charge.

III.4.3. Post-event debrief

The Event Commander shall organize a debriefing in an agreed upon timely manner following conclusion of the event. The debriefing shall include members of the facility, OSRF and emergency staff involved in the event.

III.5. SECURITY EXERCISES

III.5.1. Exercises

Exercises will be conducted between facility security and the OSRF to test the capabilities of relevant personnel and procedures.

The facility will conduct regular security exercises and drills as part of their exercise programme. The OSRF would continue, as agreed upon, to practice command and control of the response.

III.5.2. Facility visits by OSRF

The facility would arrange for OSRF personnel to conduct visits of the facility to establish and maintain a level of familiarity with respect to response logistics, plant layout, operations and equipment.

III.5.3. Planning and participation

The facility will be responsible for planning security exercises, developing the exercise scenarios and coordinating the exercise. The OSRF will appoint a liaison officer to assist in the development and coordination of OSRF involvement in the exercises.

III.6. COMMUNICATIONS

III.6.1. Communication resources

The following communication resources would be in place during security events at the facility:

(i) Dedicated telephone lines and base radio;

(ii) Direct phone line to the CAS and EOC;

(iii) Command centre/security radio link;

(iv) Compatible portable security radios.

III.6.2. Maintenance of communications equipment

The following off-site communication resources will be maintained by Facility:

(i) Dedicated telephone link between the CAS and OSRF;

(ii) Radio communication between the facility CAS and OSRF.

III.6.3. Communications testing

The FSG will conduct telephone and radio tests of communications with the OSRF as agreed upon. If a test is not initiated by the FSG, the OSRF would contact the FSG and request that the test be conducted.

III.7. COMMAND AND CONTROL

III.7.1. Security command centre

During a security event, the Chief of the OSRF and the FSOM, or designates, will operate from the CAS.

III.7.2. Emergency operations centre

The facility has the responsibility for the safe operation of the nuclear facility at all times. This overall responsibility continues during a security event.

The FSG and OSRF have the potential to impact safe operations or to shut down the facility. The Chief of the OSRF will liaise with the SEO to obtain technical and

operational information as to the effect of any action taken, along with its potential on-site and off-site effects.

III.8. RESOURCES

The facility will provide the following resources to support the OSRF:

(i) **SEO**: The SEO will provide information to the CAS so as to provide the OSRF with assistance regarding any radiological and technical issues.

(ii) **Personal protective equipment**: The facility will provide the OSRF with any personal protective equipment required for a radiological environment (e.g. dosimeters, contamination control clothing, respiratory protection, safety glasses).

(iii) **Maps**: Site maps and facility floor plans will be provided at the CAS.

(iv) **Escorts**: Qualified radiological personnel will be provided to escort OSRF personnel to the event area.

(v) **Radios**: The facility will provide the OSRF with compatible programmed radios to monitor facility security frequencies.

(vi) **Logistical support**: The facility will assist the OSRF with logistical support for such requirements as may apply to briefing areas, power supplies and staging areas.

III.9. LIMITATIONS OF LIABILITY, INDEMNIFICATION AND INSURANCE

III.9.1. OSRF

The OSRF shall not be liable in any manner whatsoever to the facility, which includes all of its respective staff, servants and agents or their successors and assign for any claim, including a claim by any third party against the facility, its staff or agents, unless it was caused by negligence of an employee or agent of the OSRF.

III.9.2. Facility

The facility does hereby indemnify the OSRF, its staff and agents, including their successors and assign against all costs, losses, expenses or liabilities incurred as a result of a claim or proceeding related to or arising from OSRF performance of this agreement unless it was caused by negligence or wilful misconduct of an employee or agent of the OSRF. Notwithstanding the foregoing, in no event shall the facility be liable for indirect or consequential damages.

The facility and the OSRF would ensure that they have appropriate general liability insurance.

III.10. TERMINATION

Either party may terminate this agreement at any time, without fault and without liability, upon [*X*] weeks written notice of termination.

Termination of this agreement does not affect any other relationship or obligations between the parties.

III.11. AGREEMENT

This agreement constitutes the entire agreement between the parties. There are no other agreements, undertakings, representatives or warranties, collateral, oral or otherwise, related to the subject matter herein.

IN THE WITNESS WHEREOF the parties have executed this agreement.

DATED AT _____, this _____*day of* _____, *year*

Signature: _____

Name: _____
Chief of OSRF
OSRF Pursuant to Delegated Authority

DATED AT _____, *this*_____ *day of*_____, *year*

Signature: _____

Name: _____
Security Operations Manager
[*facility name*]

BIBLIOGRAPHY

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

INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5), IAEA Nuclear Security Series No. 13, IAEA, Vienna, 2011.

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

INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Recommendations on Nuclear and Other Radioactive Material Out of Regulatory Control, IAEA Nuclear Security Series No. 15, IAEA, Vienna, 2011.

INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Culture, IAEA Nuclear Security Series No. 7, IAEA, Vienna, 2008.

INTERNATIONAL ATOMIC ENERGY AGENCY, Preventive and Protective Measures Against Insider Threats, Implementing Guide, IAEA Nuclear Security Series No. 8, IAEA, Vienna, 2008.

INTERNATIONAL ATOMIC ENERGY AGENCY, Implementing Guide, Security in the Transport of Radioactive Material, IAEA Nuclear Security Series No. 9, IAEA, Vienna, 2008.

INTERNATIONAL ATOMIC ENERGY AGENCY, Development, Use and Maintenance of Design Basis Threat, IAEA Nuclear Security Series No. 10, IAEA, Vienna, 2009.

INTERNATIONAL ATOMIC ENERGY AGENCY, Security of Radioactive Sources, Implementing Guide, IAEA Nuclear Security Series No. 11, IAEA, Vienna, 2009.

INTERNATIONAL ATOMIC ENERGY AGENCY, Convention on the Physical Protection of Nuclear Material, INFCIRC/274/Rev.1, IAEA, Vienna (February 1987); Amendment to the Convention on the Physical Protection of Nuclear Material, GOV/INF/2005/10–GC(49)INF/6, IAEA, Vienna, 2005.

RRFM EUROPEAN RESEARCH REACTOR CONFERENCE, 2013, Presentation on "Unique Research Reactor Features Potentially Impacting Nuclear Security".

INTERNATIONAL ATOMIC ENERGY AGENCY, IAEA Safeguards Glossary, International Nuclear Verification Series No. 3, IAEA, Vienna, 2001.

INTERNATIONAL ATOMIC ENERGY AGENCY, International Legal Framework for Nuclear Security, IAEA International Law Series No. 4, IAEA, Vienna, 2011.

INTERNATIONAL ATOMIC ENERGY AGENCY, Planning and Preparing for Emergency Response to Transport Accidents Involving Radioactive Material, IAEA Safety Standards Series No. TS-G-1.2, IAEA, Vienna, 2002.

INTERNATIONAL ATOMIC ENERGY AGENCY, Regulations for the Safe Transport of Radioactive Material, IAEA Safety Standards Series No. TS-R-1, IAEA, Vienna, 2009.

INTERNATIONAL ATOMIC ENERGY AGENCY, Identification of Radioactive Sources and Devices, Technical Guidance, IAEA Nuclear Security Series No. 5, IAEA, Vienna, 2007.

INTERNATIONAL ATOMIC ENERGY AGENCY, Identification of Vital Areas at Nuclear Facilities, Technical Guidance, IAEA Nuclear Security Series No. 16, IAEA, Vienna, 2012.

INTERNATIONAL ATOMIC ENERGY AGENCY, Computer Security at Nuclear Facilities, Technical Guidance, IAEA Nuclear Security Series No. 17, IAEA, Vienna, 2011.

INTERNATIONAL ATOMIC ENERGY AGENCY, Measures to Improve the Security of Nuclear Materials and other Radioactive Materials, GC(45)/INF/14, IAEA, Vienna 2001

INTERNATIONAL ATOMIC ENERGY AGENCY, Code of Conduct on the Safety and Security of Radioactive Sources, IAEA, Vienna, 2004.

INTERNATIONAL ATOMIC ENERGY AGENCY, Guidance on the Import and Export of Radioactive Sources (IAEA/CODEOC/IMP-EXP/2005). IAEA, Vienna, 2005.

INTERNATIONAL ATOMIC ENERGY AGENCY, Use of Nuclear Material Accounting and Control for Nuclear Security Purposes at Facilities, Implementing Guide, IAEA Nuclear Security Series No. 25-G, Vienna, 2015.

ANNEX A: BASICS OF NUCLEAR SECURITY

This Annex will provide a review of the basic principles of nuclear security that establish the basis of a nuclear security programme. These principles include: elements of nuclear security, security design principles and methods to balance safety, security and operations.

A–1. ELEMENTS OF NUCLEAR SECURITY

Physical security (physical protection) comprises a large suite of both technical equipment (e.g. sensors, cameras, badges, metal detectors, doors, locks, fences and guards) and administrative systems (e.g. procedures for controlling access, response tactics, trustworthiness checks). Equipment, people and procedures are utilized to:

(i) Detect a malicious act;

(ii) Delay the progress of the malicious act;

(iii) Respond to the malicious act.

These three goals (detect, delay, respond) are considered the basic elements of nuclear security. For any physical security system to be effective, it would successfully achieve all three elements in a timely manner for all adversary scenarios. It would be noted that for an adversary to be successful, they need only defeat one of these elements for only one of the many possible adversary attack scenarios at a facility.

Detection: Detection is the act of alerting to an ongoing malicious act. It is sequentially the first element of a security system, as it serves as the trigger for a series of actions that result in physical protection success. Detection can be achieved through:

- Sentries and other persons that visually see, hear or otherwise become aware of an ongoing malicious act;
- Intrusion sensors that trigger an alarm in response to the changes in physical phenomenon that can be associated with the intrusion of a person;
- Tamper devices that announce potential unauthorized access to an area or device;
- Process controls that can detect deviations in a process from what is expected and which may indicate a malicious action.

As many of the methods of achieving detection are not conclusive, they can also be caused by innocent means (e.g. lightning, animals/insects, wind), all alarms need to be properly assessed by a competent, properly trained person to verify evidence of an ongoing malicious act. This assessment is typically performed either by a person dispatched to investigate or by remote use of video cameras. Once an assessment has taken place, the alarm is communicated to response forces. This initiates the next two elements of security: delay and response.

Delay: Delay is the act of slowing or impeding the progress of the malicious act to permit the intervention of response forces. Since slowing or impeding an undetected malicious act does not aid in permitting the response forces to intervene, delay is not considered until after assessed detection occurs. Therefore, delay components would always be located sequentially after detection components for any adversary path. The

delay objective can be achieved by barriers, either passive (e.g. doors, walls, fences, and locks) or active (e.g. smoke and foam), or by tasks (e.g. removing bolts or extracting fluid), or by distance and separation. The barriers, tasks and distance impede progress, complicate penetration and/or extend task times for specific adversary tasks associated with theft or sabotage. Delay is successful if it impedes the adversary long enough for the response force to intercede (interrupt) prior to the completion of the malicious act.

Response: Response refers to the capability to interrupt and physically stop a malicious act prior to the initiation of unacceptable consequences. This is typically performed by a response force. While the adversary is being delayed (as above), these response forces are receiving the alarm communication resulting from the assessed detection, assembling and deploying to the location of the malicious act and tactically preparing to interrupt and engage the adversary. The time required to receive communication and to prepare, deploy and engage would be less than the time needed for the adversary to complete the malicious act after detection. In addition, the deployed response forces would be sufficiently numbered, equipped and trained and would employ sound response tactics so as to succeed in arresting, causing to flee or incapacitating the adversary or otherwise stopping the malicious act prior to its completion.

A–2. SECURITY DESIGN PRINCIPLES

A security system is the integrated interaction of the suite of appropriate detection, delay and response components. There are principles to aid in effectively organizing the design of the components to maximize security effectiveness. A full description of security design can be found in IAEA-TECDOC-1276, but some of the principles are summarized here.

Security layers: A physical security system is normally constructed in concentric layers of security (e.g. protected area boundaries) around the nuclear and other radioactive material targets to be protected. Each layer consists of a boundary demarcation that is typically a barrier, such as a fence or the wall of a building or room. Detection of unauthorized access is provided across the layer, as unauthorized access could be correlated with a malicious act. Entry control points are located along this layer to permit access of authorized persons, and these entry points include detection and delay components to ensure that they are not avenues of unauthorized entry. The number of concentric layers employed depends on the severity of potential radiological consequences.

Defence in depth: Defence in depth provides reliability that the failure of a single security component does not equate to the failure of the security element and, thereby, the security system. Therefore, multiple components of the same element (such as multiple intrusion sensors) will be installed sequentially along the adversary's path. To achieve this in practice for all potential adversary paths, the design must include multiple concentric layers of security. Defence is strengthened if technically diverse components are employed along successive layers of security for both detection and delay. For example, an adversary may need to bring (and be proficient in employing) bolt cutters, sledge hammers and cutting torches to breach successively a fence and a wall.

Balanced security: As adversaries have the freedom to select both the path and the scenario to attempt the malicious act, and as they will prefer to select the weakest

path, it is important that the security system strive for balance to optimize security resources while maximizing security effectiveness. To achieve balance, the layer would provide equivalent detection and delay effectiveness regardless of what path or scenario the adversary employs to penetrate the layer and regardless of where on the layer an adversary breaches. This includes all access points along the security layer.

A–3. BALANCING SECURITY RISK WITH SAFETY RISK AND OPERATIONS

Nuclear safety and nuclear security are equally important at a RRRF. Safety and security share many common elements and both serve to protect the research reactor and its nuclear and radioactive material. The fundamental purpose of safety and security is the same — the protection of people, society and the environment. The acceptable risk is presumptively the same whether the initiating cause is a safety or a security event. Moreover, the philosophy that is applied to achieve this fundamental objective is similar. Both safety and security typically follow the strategy of defence in depth, i.e. the employment of layers of protection. The fundamental nature of the layers is similar and priority is given to prevention. Abnormal situations need to be detected early and acted upon promptly to avoid consequent damage. Mitigation is the third part of an effective security strategy. A balanced strategy would ensure that all security measures take into account those measures established for safety, and these are developed so as not to contradict each other during either normal or emergency operation.

At times, security goals are at odds with safety or operational goals. In these situations, it is important to employ an approach that optimizes the overall protection to employees, the public, the State and the international community by minimizing the combined safety/security risk. However, while doing so, it is important to consider operations and attempt to find an approach that minimizes operational impact.

ABBREVIATIONS

CAS	central alarm station
CBRN	chemical/biological/radiological/nuclear
CPPNM	Convention on the Physical Protection of Nuclear Material
DBT	design basis threat
EOC	emergency operations centre
ECC	emergency control centre
FSG	Facility Security Guard
FSOM	Facility Security Operations Manager
IMS	integrated management system
IPPAS	International Physical Protection Advisory Service
MOU	memorandum of understanding
NM	nuclear material
NMAC	nuclear material accounting and control
OSRF	off-site response force
PPS	physical protection system
RRRF	research reactor and related facility
SAT	systematic approach to training
SEO	Senior Emergency Officer

IAEA
International Atomic Energy Agency

No. 23

ORDERING LOCALLY

In the following countries, 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.

AUSTRALIA
DA Information Services
648 Whitehorse Road, Mitcham, VIC 3132, AUSTRALIA
Telephone: +61 3 9210 7777 • Fax: +61 3 9210 7788
Email: books@dadirect.com.au • Web site: http://www.dadirect.com.au

BELGIUM
Jean de Lannoy
Avenue du Roi 202, 1190 Brussels, BELGIUM
Telephone: +32 2 5384 308 • Fax: +32 2 5380 841
Email: jean.de.lannoy@euronet.be • Web site: http://www.jean-de-lannoy.be

CANADA
Renouf Publishing Co. Ltd.
5369 Canotek Road, Ottawa, ON K1J 9J3, CANADA
Telephone: +1 613 745 2665 • Fax: +1 643 745 7660
Email: order@renoufbooks.com • Web site: http://www.renoufbooks.com

Bernan Associates
4501 Forbes Blvd., Suite 200, Lanham, MD 20706-4391, USA
Telephone: +1 800 865 3457 • Fax: +1 800 865 3450
Email: orders@bernan.com • Web site: http://www.bernan.com

CZECH REPUBLIC
Suweco CZ, spol. S.r.o.
Klecakova 347, 180 21 Prague 9, CZECH REPUBLIC
Telephone: +420 242 459 202 • Fax: +420 242 459 203
Email: nakup@suweco.cz • Web site: http://www.suweco.cz

FINLAND
Akateeminen Kirjakauppa
PO Box 128 (Keskuskatu 1), 00101 Helsinki, FINLAND
Telephone: +358 9 121 41 • Fax: +358 9 121 4450
Email: akatilaus@akateeminen.com • Web site: http://www.akateeminen.com

FRANCE
Form-Edit
5 rue Janssen, PO Box 25, 75921 Paris CEDEX, FRANCE
Telephone: +33 1 42 01 49 49 • Fax: +33 1 42 01 90 90
Email: fabien.boucard@formedit.fr • Web site: http://www.formedit.fr

Lavoisier SAS
14 rue de Provigny, 94236 Cachan CEDEX, FRANCE
Telephone: +33 1 47 40 67 00 • Fax: +33 1 47 40 67 02
Email: livres@lavoisier.fr • Web site: http://www.lavoisier.fr

L'Appel du livre
99 rue de Charonne, 75011 Paris, FRANCE
Telephone: +33 1 43 07 50 80 • Fax: +33 1 43 07 50 80
Email: livres@appeldulivre.fr • Web site: http://www.appeldulivre.fr

GERMANY
Goethe Buchhandlung Teubig GmbH
Schweitzer Fachinformationen
Willstätterstrasse 15, 40549 Düsseldorf, GERMANY
Telephone: +49 (0) 211 49 8740 • Fax: +49 (0) 211 49 87428
Email: s.dehaan@schweitzer-online.de • Web site: http://www.goethebuch.de

HUNGARY
Librotade Ltd., Book Import
PF 126, 1656 Budapest, HUNGARY
Telephone: +36 1 257 7777 • Fax: +36 1 257 7472
Email: books@librotade.hu • Web site: http://www.librotade.hu

INDIA
Allied Publishers
1st Floor, Dubash House, 15, J.N. Heredi Marg, Ballard Estate, Mumbai 400001, INDIA
Telephone: +91 22 2261 7926/27 • Fax: +91 22 2261 7928
Email: alliedpl@vsnl.com • Web site: http://www.alliedpublishers.com

Bookwell
3/79 Nirankari, Delhi 110009, INDIA
Telephone: +91 11 2760 1283/4536
Email: bkwell@nde.vsnl.net.in • Web site: http://www.bookwellindia.com

ITALY
Libreria Scientifica "AEIOU"
Via Vincenzo Maria Coronelli 6, 20146 Milan, ITALY
Telephone: +39 02 48 95 45 52 • Fax: +39 02 48 95 45 48
Email: info@libreriaaeiou.eu • Web site: http://www.libreriaaeiou.eu

JAPAN
Maruzen Co., Ltd.
1-9-18 Kaigan, Minato-ku, Tokyo 105-0022, JAPAN
Telephone: +81 3 6367 6047 • Fax: +81 3 6367 6160
Email: journal@maruzen.co.jp • Web site: http://maruzen.co.jp

NETHERLANDS
Martinus Nijhoff International
Koraalrood 50, Postbus 1853, 2700 CZ Zoetermeer, NETHERLANDS
Telephone: +31 793 684 400 • Fax: +31 793 615 698
Email: info@nijhoff.nl • Web site: http://www.nijhoff.nl

Swets Information Services Ltd.
PO Box 26, 2300 AA Leiden
Dellaertweg 9b, 2316 WZ Leiden, NETHERLANDS
Telephone: +31 88 4679 387 • Fax: +31 88 4679 388
Email: tbeysens@nl.swets.com • Web site: http://www.swets.com

SLOVENIA
Cankarjeva Zalozba dd
Kopitarjeva 2, 1515 Ljubljana, SLOVENIA
Telephone: +386 1 432 31 44 • Fax: +386 1 230 14 35
Email: import.books@cankarjeva-z.si • Web site: http://www.mladinska.com/cankarjeva_zalozba

SPAIN
Diaz de Santos, S.A.
Librerias Bookshop • Departamento de pedidos
Calle Albasanz 2, esquina Hermanos Garcia Noblejas 21, 28037 Madrid, SPAIN
Telephone: +34 917 43 48 90 • Fax: +34 917 43 4023
Email: compras@diazdesantos.es • Web site: http://www.diazdesantos.es

UNITED KINGDOM
The Stationery Office Ltd. (TSO)
PO Box 29, Norwich, Norfolk, NR3 1PD, UNITED KINGDOM
Telephone: +44 870 600 5552
Email (orders): books.orders@tso.co.uk • (enquiries): book.enquiries@tso.co.uk • Web site: http://www.tso.co.uk

UNITED STATES OF AMERICA
Bernan Associates
4501 Forbes Blvd., Suite 200, Lanham, MD 20706-4391, USA
Telephone: +1 800 865 3457 • Fax: +1 800 865 3450
Email: orders@bernan.com • Web site: http://www.bernan.com

Renouf Publishing Co. Ltd.
812 Proctor Avenue, Ogdensburg, NY 13669, USA
Telephone: +1 888 551 7470 • Fax: +1 888 551 7471
Email: orders@renoufbooks.com • Web site: http://www.renoufbooks.com

United Nations
300 East 42nd Street, IN-919J, New York, NY 1001, USA
Telephone: +1 212 963 8302 • Fax: 1 212 963 3489
Email: publications@un.org • Web site: http://www.unp.un.org

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

IAEA Publishing Section, Marketing and Sales Unit, International Atomic Energy Agency
Vienna International Centre, PO Box 100, 1400 Vienna, Austria
Telephone: +43 1 2600 22529 or 22488 • Fax: +43 1 2600 29302
Email: sales.publications@iaea.org • Web site: http://www.iaea.org/books

International Atomic Energy Agency
Vienna
ISBN 978–92–0–111315–3