IAEA
International Atomic Energy Agency

IAEA NUCLEAR SECURITY SERIES

No. 45-T

Regulatory Authorization and Related Inspections for Nuclear Security During the Lifetime of a Nuclear Facility

TECHNICAL GUIDANCE

IAEA NUCLEAR SECURITY SERIES

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

CATEGORIES IN THE IAEA NUCLEAR SECURITY SERIES

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

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

DRAFTING AND REVIEW

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

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

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

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

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

REGULATORY AUTHORIZATION AND RELATED INSPECTIONS FOR NUCLEAR SECURITY DURING THE LIFETIME OF A NUCLEAR FACILITY

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
CABO VERDE
CAMBODIA
CAMEROON
CANADA
CENTRAL AFRICAN REPUBLIC
CHAD
CHILE
CHINA
COLOMBIA
COMOROS
CONGO
COOK ISLANDS
COSTA RICA
CÔTE D'IVOIRE
CROATIA
CUBA
CYPRUS
CZECH REPUBLIC
DEMOCRATIC REPUBLIC OF THE CONGO
DENMARK
DJIBOUTI
DOMINICA
DOMINICAN REPUBLIC
ECUADOR
EGYPT
EL SALVADOR
ERITREA
ESTONIA
ESWATINI
ETHIOPIA
FIJI
FINLAND
FRANCE
GABON
GAMBIA, THE
GEORGIA
GERMANY
GHANA
GREECE
GRENADA
GUATEMALA
GUINEA
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, KINGDOM OF THE
NEW ZEALAND
NICARAGUA
NIGER
NIGERIA
NORTH MACEDONIA
NORWAY
OMAN
PAKISTAN
PALAU
PANAMA
PAPUA NEW GUINEA
PARAGUAY
PERU
PHILIPPINES
POLAND
PORTUGAL
QATAR
REPUBLIC OF MOLDOVA
ROMANIA
RUSSIAN FEDERATION
RWANDA
SAINT KITTS AND NEVIS
SAINT LUCIA
SAINT VINCENT AND THE GRENADINES
SAMOA
SAN MARINO
SAUDI ARABIA
SENEGAL
SERBIA
SEYCHELLES
SIERRA LEONE
SINGAPORE
SLOVAKIA
SLOVENIA
SOMALIA
SOUTH AFRICA
SPAIN
SRI LANKA
SUDAN
SWEDEN
SWITZERLAND
SYRIAN ARAB REPUBLIC
TAJIKISTAN
THAILAND
TOGO
TONGA
TRINIDAD AND TOBAGO
TUNISIA
TÜRKİYE
TURKMENISTAN
UGANDA
UKRAINE
UNITED ARAB EMIRATES
UNITED KINGDOM OF GREAT BRITAIN AND NORTHERN IRELAND
UNITED REPUBLIC OF TANZANIA
UNITED STATES OF AMERICA
URUGUAY
UZBEKISTAN
VANUATU
VENEZUELA, BOLIVARIAN REPUBLIC OF
VIET NAM
YEMEN
ZAMBIA
ZIMBABWE

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

IAEA NUCLEAR SECURITY SERIES No. 45-T

REGULATORY AUTHORIZATION AND RELATED INSPECTIONS FOR NUCLEAR SECURITY DURING THE LIFETIME OF A NUCLEAR FACILITY

TECHNICAL GUIDANCE

INTERNATIONAL ATOMIC ENERGY AGENCY
VIENNA, 2024

COPYRIGHT NOTICE

Publishing Section
International Atomic Energy Agency
Vienna International Centre
PO Box 100
1400 Vienna, Austria
tel.: +43 1 2600 22529 or 22530
email: sales.publications@iaea.org
www.iaea.org/publications

Printed by the IAEA in Austria
December 2024
STI/PUB/2016
https://doi.org/10.61092/iaea.kkxl-qqqp

IAEA Library Cataloguing in Publication Data

Names: International Atomic Energy Agency.
Title: Regulatory authorization and related inspections for nuclear security during the lifetime of a nuclear facility / International Atomic Energy Agency.
Description: Vienna : International Atomic Energy Agency, 2024. | Series: IAEA nuclear security series, ISSN 1816–9317 ; no. 45-T | Includes bibliographical references.
Identifiers: IAEAL 24-01722 | ISBN 978-92-0-127922-4 (paperback : alk. paper) |ISBN 978-92-0-128022-0 (pdf) | ISBN 978-92-0-128122-7 (epub)
Subjects: LCSH: Nuclear facilities — Safety regulations. | Nuclear facilities — Safety measures. | Nuclear facilities — Inspection. | Nuclear facilities — Security measures.
Classification: UDC 621.039 | STI/PUB/2016

FOREWORD

by Rafael Mariano Grossi
Director General

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

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

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

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

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

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

EDITORIAL NOTE

Guidance issued in the IAEA Nuclear Security Series is not binding on States, but States may use the guidance to assist them in meeting their obligations under international legal instruments and in discharging their responsibility for nuclear security within the State.

Guidance expressed as 'should' statements is intended to present international good practices and to indicate an international consensus that it is necessary for States to take the measures recommended or equivalent alternative measures.

Security related terms are to be understood as defined in the publication in which they appear, or in the higher level 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.

CONTENTS

1. INTRODUCTION

BACKGROUND

1.1. The development of a nuclear facility needs careful planning, adequate preparation and substantial investment in terms of financial and human resources. This includes establishing a legislative and regulatory framework that contains provisions to assess the adequacy of nuclear security and authorize (within the regulatory framework) activities at nuclear facilities at key stages in their lifetimes. IAEA Nuclear Security Series publications provide nuclear security guidance that can be used during the authorization process.

1.2. IAEA Nuclear Security Series No. 20, Objective and Essential Elements of a State's Nuclear Security Regime [1], identifies a legislative and regulatory framework as an essential element of a State's nuclear security regime. An effective legislative and regulatory framework for nuclear security within a State includes a well defined process for the authorization of activities at nuclear facilities based on an assessment of the adequacy of nuclear security.

1.3. Fundamental Principle C in IAEA Nuclear Security Series No. 13, Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5) [2], states:

> "**The State is responsible for establishing and maintaining a legislative and regulatory framework to govern physical protection. This framework should provide for the establishment of applicable physical protection requirements and include a system of evaluation and licensing or other procedures to grant authorization. This framework should include a system of inspection of *nuclear facilities* and *transport* to verify compliance with applicable requirements and conditions of the licence or other authorizing document, and to establish a means to enforce applicable requirements and conditions, including effective sanctions.**"

1.4. IAEA Nuclear Security Series No. 27-G, Physical Protection of Nuclear Material and Nuclear Facilities (Implementation of INFCIRC/225/Revision 5) [3], provides further guidance on authorization procedures.

1.5. IAEA Nuclear Security Series No. 29-G, Developing Regulations and Associated Administrative Measures for Nuclear Security [4], provides guidance for States and their competent authorities on measures they should take to develop

and maintain a legislative and regulatory framework to govern the nuclear security regime and to put its provisions into effect.

1.6. IAEA Nuclear Security Series No. 19, Establishing the Nuclear Security Infrastructure for a Nuclear Power Programme [5], provides guidance on the actions that should be taken by a State to establish an effective national nuclear security infrastructure for a nuclear power programme and describes in detail the regulatory infrastructure needed to develop and sustain the authorization processes of a competent authority.

1.7. IAEA Nuclear Security Series No. 35-G, Security During the Lifetime of a Nuclear Facility [6], provides guidance on appropriate nuclear security measures during each stage in the lifetime of a nuclear facility. The stages in the lifetime of a nuclear facility and the associated authorization processes described in the present publication are consistent with the eight stages introduced in Ref. [6]. These stages are broadly consistent with the stages in the lifetime of a nuclear facility that are considered for the safety of such facilities.

1.8. IAEA Nuclear Security Series No. 25-G, Use of Nuclear Material Accounting and Control for Nuclear Security Purposes at Facilities [7], provides guidance for States and their competent authorities on measures they should take to develop and maintain a regulatory framework that establishes requirements for the design and performance of systems for nuclear material accounting and control at the facility level, including those relating to nuclear security.

1.9. IAEA Nuclear Security Series No. 26-G, Security of Nuclear Material in Transport [8], provides guidance to States and their competent authorities on how to implement and maintain a physical protection regime for the transport of nuclear material. Reference [8] may also be useful for guidance on the authorization of security measures for nuclear material during transport.

1.10. IAEA Nuclear Security Series No. 42-G, Computer Security for Nuclear Security [9], provides guidance on developing and implementing computer security as an integral component of nuclear security. More detailed guidance on computer security specific to the security of nuclear facilities, including computer security for the protection of instrumentation and control systems at nuclear facilities against malicious acts that could prevent such systems from performing their safety and security related functions, can be found in IAEA Nuclear Security Series No. 17-T (Rev. 1), Computer Security Techniques for Nuclear Facilities [10] and No. 33-T, Computer Security of Instrumentation and Control Systems at Nuclear Facilities [11].

1.11. IAEA Safety Standards Series No. SSG-12, Licensing Process for Nuclear Installations [12], provides recommendations on licensing[1] relating to safety during the lifetime of a nuclear facility, including nuclear safety, radiation safety, safety of radioactive waste management and emergency preparedness and response.

OBJECTIVE

1.12. The objective of this publication is to provide guidance to regulatory bodies[2] on the authorization process for nuclear security during each stage in the lifetime of a nuclear facility. This authorization process includes the review and assessment by the regulatory body of an application for authorization submitted by an applicant or operator, inspections by the regulatory body to verify compliance with regulatory requirements and, where appropriate, enforcement actions.

1.13. This publication can be used by applicants, operators and other entities seeking authorization to implement applicable nuclear security measures during each stage in the lifetime of a nuclear facility.

SCOPE

1.14. This publication provides guidance to regulatory bodies that are responsible for the nuclear security of nuclear facilities on the process for the authorization of such facilities and of related activities. The guidance addresses nuclear security aspects that may require regulatory authorization during the different stages in the lifetime of a nuclear facility, and identifies the elements to be included in the applications for authorization that are submitted by the applicant or operator during each of these stages. This publication provides guidance to the regulatory body on the review and assessment of these applications as a basis for authorization decisions.

1.15. This publication addresses the eight stages in the lifetime of a nuclear facility as described in Ref. [6]. These eight stages are planning, siting, design, construction, commissioning, operation, cessation of operation and decommissioning.

---

[1] In this publication, ‘authorization’ is used to refer to the process termed ‘licensing’ in SSG-12 [12].

[2] In this publication, ‘regulatory body’ is used to refer to the competent authority with regulatory responsibility.

1.16. This publication does not specifically address nuclear security for other types of facility or activity involving radioactive material. It does not provide detailed guidance relating to authorization for the nuclear security of nuclear or other radioactive material during transport.

1.17. Despite the similarities of the authorization process for nuclear security to the licensing process for nuclear safety, this publication does not provide guidance on safety considerations in the regulatory authorization of nuclear facilities.

STRUCTURE

1.18. Section 2 provides general guidance on the authorization process for a nuclear facility, including basic authorization principles and the roles and responsibilities of the regulatory body and the applicant or operator. Section 3 provides guidance on the content of applications submitted by the applicant or operator during the different stages in the lifetime of a nuclear facility, including basic principles and evaluation considerations for the authorization process at each stage. It also provides guidance on the review and assessment by the regulatory body of these applications. Section 4 provides guidance on the review and authorization of changes to nuclear facilities that might affect nuclear security. Section 5 describes regulatory inspections that may be performed during the lifetime of a nuclear facility to verify compliance or as deemed appropriate by the regulatory body. It also describes enforcement actions for addressing non-compliance with regulatory requirements.

2. THE AUTHORIZATION PROCESS FOR NUCLEAR SECURITY

2.1. This section provides general guidance on the authorization process for the nuclear security of nuclear facilities. This section includes basic authorization principles and the roles and responsibilities of the regulatory body and the applicant or operator.

2.2. Many States have unified authorization processes to address safety aspects and security aspects of nuclear facilities, and these need to be appropriately coordinated. More information on these processes and steps can be found in Ref. [6] and in SSG-12 [12].

2.3. Regulatory authorization for the stages in the lifetime of a nuclear facility that have a long duration (e.g. construction, operation, decommissioning) usually takes the form of a licence, whereas other forms of authorization (e.g. permits, regulatory approval) may be granted for specific actions (e.g. for loading or unloading fuel).

2.4. The objective of the authorization process is for the regulatory body to establish and maintain regulatory control over all facilities and activities for which nuclear security has to be considered. Paragraph 2.2 of SSG-12 [12] states:

> "[A]uthorization may take different forms, such as certification, granting of a permit, agreement, consent, regulatory approval or granting of another similar regulatory instrument, depending on the governmental and regulatory framework of the particular State."

2.5. A licence is a product of the authorization process and generally covers a particular stage in the lifetime of a nuclear facility. Licences and other forms of authorization are granted or denied in accordance with the national legislative and regulatory framework and should cover all stages in the lifetime of the nuclear facility.

BASIC PRINCIPLES FOR AUTHORIZATION

2.6. Principles for the authorization process should be established in the legislative and regulatory framework. The process should be well defined, clear, transparent and traceable to achieve the following:

(a) To minimize duplication of effort through the different steps;
(b) To allow for some steps to be conducted in parallel;
(c) To provide for a clear division of responsibilities, at the various steps, among the regulatory body, operators, other governmental stakeholders and, where appropriate, vendors, contractors and suppliers;
(d) To provide opportunities for early participation by the public in accordance with the national legislative and regulatory framework;
(e) To ensure that essential security issues are addressed early in the authorization process.

2.7. The authorization process is intended to ensure compliance with a set of regulatory requirements applicable to a nuclear facility through the review of applications formally submitted by an applicant or operator, and subsequently

through authorization, inspection and enforcement. The legislative and regulatory framework of the State should set out the responsibilities for the authorization process.

2.8. The regulatory body should authorize activities only when these activities comply with the national nuclear security regulations. The regulatory body should review and assess the proposed security measures and should grant authorization only when satisfied that the measures meet the relevant regulatory requirements. The regulatory body should also evaluate nuclear security measures whenever a significant change takes place, to ensure continued compliance with regulatory requirements. Where different competent authorities are responsible for different aspects of nuclear security, the State should consider appropriate arrangements for coordinating actions to avoid omissions or unnecessary duplication and to avoid conflicting requirements being placed on authorized parties.

2.9. The regulatory body should establish procedures for issuing licences or other forms of authorization for each stage in the lifetime of the facility and for each type of facility, to ensure that all necessary steps have been taken before granting authorization.

2.10. Licences and other authorization documents should state explicitly, or should include by reference or attachment, all conditions imposed by the regulatory body. These conditions are additional specific obligations and should cover, as appropriate, security related aspects to enable effective regulatory control at all stages.

2.11. The regulatory body may require prior review, assessment and approval of any changes or modifications to the site, nuclear facility, organizational structure, procedures, processes or plans for future activities that potentially affect nuclear security.

2.12. When different licences and other forms of authorization are granted for different facilities on a particular site, a process should be established for maintaining consistency between these different licences and other forms of authorization. In cases where the facilities of several licensees share common nuclear safety related features and nuclear security related features, arrangements should be made to ensure that neither nuclear safety nor nuclear security is compromised.

2.13. Safety measures and security measures should be designed and implemented in an integrated manner so that they do not compromise each other. Paragraph 2.22

of SSG-12 [12] states that "Potentially conflicting requirements resulting from safety and security considerations should be identified as early as possible in the licensing process and should be carefully analysed to provide an acceptable solution with respect to both safety and security."

ROLES AND RESPONSIBILITIES OF THE REGULATORY BODY

2.14. The regulatory body is responsible for verifying continued compliance with the nuclear security regulations and conditions of the licence or other form of authorization through regular inspections (planned or need based), performance testing and evaluations, and for ensuring that corrective action is taken when needed.

2.15. Before an applicant or operator submits an application for authorization, the regulatory body should communicate the established regulatory requirements for nuclear security and the steps that it will follow to process the application. The established regulatory requirements should be independent of design and not excessively prescriptive to allow for consideration of several designs of nuclear security systems at the beginning of a project to construct a nuclear facility.

2.16. The regulatory framework should empower the regulatory body to review, assess and inspect the following:

(a) Evidence of meeting, and plans to meet, regulatory requirements regarding the security of the nuclear facility and associated activities;
(b) Compliance with regulatory requirements, including applicable regulations, directions and conditions of authorization;
(c) The continued competence and capability of the operator to meet regulatory requirements and the conditions of the licence or other form of authorization.

2.17. The regulatory framework should also empower the regulatory body to make decisions and to grant, amend, suspend or revoke licences and other forms of authorization (or individual conditions thereof), as appropriate (see SSG-12 [12]).

2.18. The regulatory body may require the operator to reassess nuclear security at the nuclear facility, and the security of activities performed at the facility, periodically or on the basis of operating experience, information obtained from inspections and performance testing, new technical knowledge, changes in threat, changes in the regulatory framework and/or changes in the site conditions. Following such a reassessment, the operation of the nuclear facility may be

suspended or made subject to specific conditions, depending on the security issues involved. Such specific conditions may include measures to be taken within a specified time frame. The regulatory body should authorize operation to continue only when the operator has demonstrated satisfactorily that regulatory requirements are being met.

ROLES AND RESPONSIBILITIES OF THE APPLICANT OR OPERATOR

2.19. The applicant or operator has the following responsibilities:

(a) To prepare and submit a comprehensive application, in accordance with the regulatory framework, to the regulatory body to demonstrate that appropriate priority is being given to nuclear security and that this will be maintained at the site for the entire lifetime of the nuclear facility;
(b) To maintain responsibility for nuclear security at the nuclear facility until it is released from regulatory control;
(c) To maintain the capability to understand the design basis threat or representative threat statement for the nuclear facility, and the limits and conditions under which the facility should be operated;
(d) To exercise control and accountability over the work and conduct of contractors and take responsibility for the implementation of that work;
(e) To submit to the regulatory body a procedure or description of the process for dealing with modifications, which may be subject to approval by the regulatory body depending on national legislation, regulations and practices (see SSG-12 [12]);
(f) To have a design capability and a formal and effective external relationship with the original design organization or an acceptable alternative (see SSG-12 [12]);
(g) To assess nuclear security in a systematic manner and on a regular basis;
(h) To ensure nuclear security at the nuclear facility;
(i) To develop, implement and assess nuclear security related procedures for each stage in the lifetime of the nuclear facility;
(j) To demonstrate that it has and will continue to maintain adequate technical, financial and human resources throughout the lifetime of the facility.

3. SUBMISSION OF APPLICATIONS FOR AUTHORIZATION, AND RELATED REVIEW AND ASSESSMENT BY THE REGULATORY BODY

3.1. An appropriate regulatory review and assessment is a crucial part of determining whether the nuclear facility complies with the applicable nuclear security regulations. Nuclear security for nuclear facilities should follow a process for review and assessment similar to that for nuclear safety. Depending on the national legislative and regulatory framework, issues concerning the adequacy of nuclear security strategies, features and programmes at a nuclear facility should be identified and resolved by the operator as early as possible in the design process. The resolution of these issues should be documented. The documentation should include consideration of the potential impact of these issues on future stages in the lifetime of the facility.

3.2. Some States (usually those embarking on nuclear power programmes) may acquire 'turnkey' nuclear facilities and authorization documentation (usually from vendors in States with mature nuclear power programmes), while some States may acquire structures, systems and components, with the associated documentation, domestically. Although the operator has the prime responsibility for nuclear security, it is important in all cases to address responsibilities during the authorization process and confidentiality of information during the procurement, design, construction and commissioning processes in accordance with the regulatory requirements.

3.3. The regulatory authorization of nuclear security aspects for nuclear facilities may be integrated and coordinated with the authorization of nuclear safety aspects for these facilities. However, States usually apply different approaches for authorizing these aspects, primarily because nuclear security and nuclear safety have different performance goals and assessment criteria and involve different organizations in the authorization process. The regulatory body may need to coordinate and cooperate with relevant national organizations that have a role in nuclear security in the authorization of nuclear security aspects.

3.4. The security plan is the primary basis for decisions on authorization by the regulatory body as it demonstrates that the provisions for nuclear security at the nuclear facility are adequate. The security plan describes objectives, procedures to implement and maintain processes, methods for measuring progress and self-assessment of compliance, approaches for improving performance on the

basis of experience, and a process for configuration management and change management. The security plan should therefore describe in detail the physical protection system intended to meet the requirements specified by the regulatory body. The security plan should be supported by adequate information to confirm that regulatory requirements will be met when the plan is executed. Guidance on the structure and suggested contents of the security plan is provided in Ref. [3].

3.5. In addition to the security plan, the applicant or operator may need to prepare supplementary documentation, depending on the regulatory requirements of the State, legal decisions and/or bilateral discussions with the regulatory body.

3.6. Where there are interfaces between nuclear security and nuclear safety, it is necessary to avoid potential conflicts and to ensure that the nuclear security and safety functions are integrated so that they are mutually supportive and do not compromise each other. For example, an application for authorization describes structures, systems and components and programmes and procedures in the nuclear facility that have important nuclear security and nuclear safety functions. This application should be assessed by taking into consideration both nuclear security and nuclear safety. Additionally, the system for nuclear material accounting and control comprises measures for the timely detection of unauthorized removal of nuclear material, thereby enhancing nuclear security [7].

3.7. The review and assessment process followed by the regulatory body should have the following attributes:

(a) The process should be developed and implemented following a graded approach. For example, the regulatory body is expected to have a more thorough authorization process based on applicable regulatory requirements for nuclear facilities with Category I nuclear material, or with potential radiological consequences of sabotage that exceed the State's threshold for high radiological consequences, than for facilities with lower categories of nuclear material or lower levels of potential radiological consequences, as applicable.
(b) The process should have specific objectives for the review and assessment and these objectives should be consistent with the stage in the lifetime of the nuclear facility.
(c) The process should be properly managed within the regulatory body. The review and assessment activities should be planned, scheduled (including schedules for the receipt of the application), conducted in accordance with documented procedures, and monitored to ensure that the specific objectives for the review and assessment have been achieved. The regulatory body

should be adequately staffed with qualified personnel (including consultants, if needed) to conduct the review and assessment activities.

(d) The documentation relating to the process (including the information submitted by the applicant or operator in the application and the conclusions reached by the regulatory body) should be protected and controlled appropriately in accordance with the sensitivity of the security related information (see IAEA Nuclear Security Series No. 23-G, Security of Nuclear Information [13]).

(e) The decisions by the regulatory body should be made in accordance with defined criteria (such as applicable regulations and results of the reviews) that can be defended if the applicant or operator disagrees with the conclusions.

3.8. The review and assessment process may result in the following:

(a) Written questions from the regulatory body to the applicant or operator to obtain clarifications on the information submitted in the application;

(b) Discussions between the applicant or operator and the regulatory body on the adequacy of the information submitted in the application;

(c) Revisions by the applicant or operator to the application to reflect needed changes or clarifications.

3.9. A documented review and assessment process is considered to be good practice for regulatory authorization activities.

3.10. Depending on the types of nuclear facilities in the State, the regulatory body may have several different processes for the review and assessment of the applications submitted by the applicant or operator, or a flexible process that is adaptable to the specific attributes of the nuclear facility (e.g. type of facility, types and quantities of material, location).

3.11. The review and assessment process may differ between States, depending on several factors such as the following:

(a) The regulatory practice of the State or the regulatory body. For example, the process might focus on the regulatory body exercising extensive control to confirm that all regulatory requirements have been met by the applicant or operator before authorization is granted. Alternatively, the process might focus on the responsibility of the operator. Even in this case, the regulatory body should verify the capability of the applicant or operator to meet its responsibilities before granting authorization.

(b) The regulatory approach chosen by the regulatory body. For example, the regulatory body may choose to follow a prescriptive approach, a performance based approach or a combined approach to the authorization of nuclear facilities (see para. 3.13). Further guidance on regulatory approaches can be found in Ref. [3].
(c) The organization and operations of the regulatory body. The regulatory body may conduct the review using its own resources and personnel, or may use the results of an independent assessment by external experts (i.e. experts from dedicated technical support organizations, other governmental entities or agencies, or independent experts). Security related government organizations are very likely to be involved in the review and assessment process.

3.12. The review and assessment process should give the regulatory body sufficient confidence that the applicant or operator meets the regulatory requirements and is able to continue meeting them.

3.13. The regulatory body may take various approaches, or combinations thereof, to the review and assessment process, including the following:

(a) Prescriptive approach. The regulatory body checks that the operator meets all applicable regulatory requirements before granting authorization. This approach may be based on declarations and justifications provided in the documentation submitted by the applicant or operator, or on inspections conducted by the regulatory body at the facility. The regulatory body may also decide to subject the operator to performance testing and evaluation to confirm that regulatory requirements are being met. This approach is well suited to simple facilities.
(b) Performance based approach. The regulatory body expects the operator to meet the regulatory requirements with limited independent oversight. This approach is well suited to facilities at which operators need to build their own physical protection system, based primarily on the design basis threat. With this approach, the applicant or operator describes the methodology used to build and assess its physical protection system on the basis of a set of performance based requirements specified by the State or its regulatory body. The regulatory body then assesses the methodology to verify that the performance based requirements (see Ref. [3]) have been satisfied. This approach allows the regulatory body to conclude that the operator has the capability to build an effective physical protection system. The regulatory body may also require the operator to conduct performance testing and evaluation to confirm that regulatory requirements are being met. This

approach may involve fewer human resources, thus allowing the regulatory body to assign more to other tasks.

(c) Independent review and assessment by external experts. In this approach, the regulatory body uses external experts for the review and assessment of the design of the physical protection system and the implementation documentation of the operator, while taking into consideration the confidentiality of sensitive information. This could lead to a technical debate between the experts and the operator on the advantages and disadvantages of the operator's choices and on alternative solutions. As part of this approach, the operator may be required to amend its documentation to take into account relevant inputs from the independent assessment. This approach might be time consuming; nevertheless, it might result in new or optimal solutions for improving security, particularly for challenging issues when obvious solutions do not exist.

3.14. The granting of a licence or other form of authorization is only the beginning of a continuing cycle of regulatory supervision responsibilities during the lifetime of a nuclear facility. The regulatory body may choose to use any of the above approaches, or a combination of them, at different stages during the lifetime of a nuclear facility in an ongoing process to evaluate applications from the operator for new or amended authorizations.

PLANNING STAGE

3.15. Although the authorization process for a nuclear facility usually begins at the siting stage, the State and the competent authorities should complete the following actions during the planning stage:

(a) Define and assign roles and responsibilities for review and assessment of applications, granting of licences and other forms of authorization, and inspection of nuclear facilities and associated activities.
(b) Recruit, train and qualify staff with adequate nuclear security knowledge and expertise to regulate nuclear facilities and associated activities and to implement a sustainability programme.
(c) Ensure that relevant information from the design basis threat or representative threat statement, as appropriate, is communicated to the applicant or operator.
(d) Develop regulatory requirements to protect against the unauthorized removal of nuclear material and the sabotage of nuclear material and nuclear facilities.

(e) Develop regulatory requirements for information security, computer security, sustainability, contingency planning, emergency preparedness, incident reporting, trustworthiness, quality assurance, nuclear security culture and nuclear material accounting and control.
(f) Define thresholds for potential radiological consequences of sabotage at the nuclear facility.
(g) Establish a sustainability programme to ensure that regulatory control and oversight remains effective over time.

3.16. The applicant or operator should undertake the following actions during the planning stage:

(a) Determine the expected quantity and type of nuclear material at the facility, its associated category and the potential radiological consequences from sabotage.
(b) Develop a nuclear security policy and strategy, and identify the resources and organizational structure needed to implement it.
(c) Promote nuclear security awareness among organizations and individuals involved in facility planning, with the aim of ensuring their full understanding of security policies and responsibilities.
(d) Involve all organizations with nuclear security responsibilities associated with the facility in all facility planning activities, including off-site organizations such as organizations involved in response, as appropriate.
(e) Coordinate the nuclear security planning activities at the facility with the planning activities associated with nuclear safety, safeguards and facility operations in order to avoid or resolve conflicts and to find synergies.
(f) Plan measures to protect sensitive information.
(g) Take into account regulatory requirements applicable to nuclear security.

SITING STAGE

3.17. Site evaluation takes place during the siting stage in the lifetime of a nuclear facility. Site selection is the first step in the site evaluation process and generally consists of an investigation of a large region to select one or more preferred candidate sites, followed by a detailed evaluation of those candidate sites. For a site in close proximity to a State's national border, consultation with neighbouring countries is an important step in the site selection process.

3.18. Site evaluation includes an analysis of those factors at a site that could influence decisions on the design, construction and operation of the nuclear

facility. It is important to take into account any local installations (e.g. dams and dikes upstream or near gas, oil or chemical facilities) that could be used by adversaries to create incidents that could adversely affect the nuclear facility. Also, if the Member State's response forces contribute to the site's security and are stationed off the site, their access to the site should not be vulnerable to attack. A local law enforcement agency or local police that can provide reinforcements are an asset for the security of a given site.

3.19. The analysis conducted by the applicant or operator should be based on the State's current threat statements such as design basis threats and representative threat statements.[3] The analysis should determine whether effective nuclear security strategies and features that comply with the legislative and regulatory requirements for the nuclear facility can be implemented. The analysis should also take into consideration the transport of nuclear material to and from the nuclear facility as well as the movement of nuclear material on the site.

3.20. Once the regulatory body has assessed the site evaluation, it may issue a siting licence or other form of authorization, including any conditions that might be necessary.

3.21. The operator should take into account regulatory requirements applicable to nuclear security during the siting stage, including requirements for information security, computer security, sustainability, contingency planning, emergency preparedness, incident reporting, trustworthiness, quality assurance, nuclear security culture and nuclear material accounting and control, as applicable.

Submission of the application for authorization

3.22. Because nuclear security measures are influenced by the location of the site, the application for a siting licence or other form of authorization usually includes an assessment of the site characteristics and the environment. The site evaluation aims to verify that nuclear security measures in accordance with regulatory requirements can be established and implemented effectively at the proposed site.

[3] If a design basis threat is not established at this stage, the applicant or operator needs to take into account nuclear security considerations, such as information on national and local threats, in the site selection.

The site evaluation process should address the technical aspects of the nuclear facility and the surrounding environment, taking into account the following:

(a) A description of site topography demonstrating that sufficient distances exist between security areas and the outer boundary. This description should confirm that sufficient space is available at the site to construct security infrastructure (e.g. physical barriers, access control points, alarm stations) and to install physical protection systems and components.
(b) A description of the site topography for which the implementation of access control measures might be needed to prevent possible penetration into the facility's limited access area (e.g. barge slips, transport routes, cliffs, depressions, hills, mounds, open waterways, roads, railways).
(c) A description of other facilities (e.g. gas or chemical plants) and pipelines in proximity to the site.
(d) An overview of the planned drains and unattended ducts, supply systems (e.g. electricity supply, ventilation) and water source channels that penetrate the proposed protected area.
(e) A description of meteorological conditions, including extreme weather hazards.
(f) An overview of the socioeconomic situation in the vicinity of the site.

3.23. The proposed location of the site should also be described with the aid of illustrations and topographical maps, and the description should address all relevant threats associated with the site of the facility. The applicant or operator should also submit maps and layouts, showing the following:

(a) All configurations of site structures being considered;
(b) Pedestrian land approaches (e.g. proximity to public parks, lakes, beaches, resorts and other tourist attractions);
(c) Vehicular land approaches and routes;
(d) Railway approaches including nearby stations and terminals;
(e) Water-borne vessel approaches including nearby harbours, ports and terminals;
(f) Air traffic and airports;
(g) High ground areas from which an adversary might gain advantage;
(h) Existing and planned drains;
(i) The provisional location of vital areas and associated equipment;
(j) Nearby facilities where hazardous materials are stored, used or processed;
(k) The location of the proposed intake structures for the heat transport systems associated with the ultimate heat sink;

(l) The location of the proposed boundary for power block and safety related water sources;
(m) The locations of vehicle checkpoints;
(n) Proximity to other critical infrastructure (e.g. other power plants, power transmission lines, telecommunication lines).

3.24. In compiling, evaluating and preparing documentation relevant to the siting process, the applicant or operator should include objective evidence that the design basis threat or representative threat statement, as appropriate, was considered in the siting process. Although the siting stage is early in the lifetime of the nuclear facility, the applicant or operator needs to plan for, and prepare documentation relevant to, the nuclear security functions for the nuclear facility, including the following:

(a) Programmes for the selection, qualification, trustworthiness checks and training of security personnel who will design the physical protection system;
(b) The identification of nuclear security considerations that could influence site selection and site evaluation;
(c) The availability of local and planned facility infrastructure, including response capabilities for a nuclear security event.

Review and assessment by the regulatory body

3.25. The evaluation criteria for the siting of a nuclear facility may vary from State to State. However, the general considerations described in paras 3.26–3.31 could form a basis for the review and assessment by the regulatory body of the application for siting.

Programmatic criteria

3.26. During the review and assessment of an application for authorization at the siting stage, the regulatory body should verify that the following programmatic criteria have been satisfied:

(a) Information on national and local threats, including design basis threats and representative threat statements, has been considered in the siting process.
(b) Security related site characteristics have been considered during site selection.
(c) Where possible, and subject to the confidentiality of information, the applicant or operator will share information on nuclear security events with

the operators of nuclear or high hazard facilities that are collocated on the proposed site or in close proximity to it.

(d) The applicant or operator is capable of developing and implementing management programmes (e.g. for quality assurance, for maintenance and testing, for the selection, qualification and training of security personnel to support the design effort).

Site location

3.27. During the review and assessment of an application at the siting stage, the regulatory body should verify that the following site location criteria have been satisfied:

(a) Sufficiently detailed information has been provided to demonstrate that the site characteristics will support the development and implementation of the security plan for the nuclear facility.

(b) The proposed site provides enough space or distances to allow for the design, installation and implementation of a physical protection system to protect the facility against potential threats, including the design basis threat.

(c) In the case of limited spatial distances because of the natural topography or because of existing or planned structures at a proposed site, a detailed description is provided to demonstrate that adequate security boundaries, physical barriers and access control points can be designed and implemented.

(d) Roads, railways and waterways that pass through the limited access area are at a sufficient distance from the planned location(s) of the nuclear facility. Specific site characteristics and facility operations on the proposed site are configured so that routine use of these routes will not interfere with or impede the design of the physical protection system or affect the planned normal and contingency security operations for the facility.

(e) The necessary logistical support is available to sustain operation of the physical protection system if the proposed site is at a remote location and if material, equipment or services might be needed before an off-site response can arrive on the site.

Hazardous materials on the site, in the vicinity and at nearby facilities

3.28. During the review and assessment of an application at the siting stage, the regulatory body should verify that the following criteria relating to hazardous materials have been satisfied:

(a) Potential hazardous gaseous, liquid or solid materials — such as chemicals, flammables, explosives and radioactive material — in the vicinity or on the site (including in pipelines and storage tanks) do not impede the design of, or plans for, the engineered and administrative controls of the facility's physical protection system.
(b) Postulated credible accidents and their effects from on-site or nearby hazards have been analysed for potential impediments to implementing nuclear security at the nuclear facility. Some of the considerations for review may be as follows:
    (i) Security structures such as guard towers and fighting positions can be located at safe distances to protect nuclear security personnel from the effects of such hazards.
    (ii) Engineered features and systems can be designed to protect against the potential hazardous and corrosive environments from such hazards to ensure that the facility's nuclear security capabilities (i.e. physical protection system and response forces) can continue to function effectively to mitigate threats within the design basis threat.

Regional climatological and local meteorological conditions

3.29. During the review and assessment of an application at the siting stage, the regulatory body should verify that evaluation criteria regarding climatological and meteorological conditions have been met. The application should identify and consider acute and prolonged exposure to severe weather and resulting environmental conditions that could present challenges to the design of the physical protection system and subsequent implementation of the security plan. Examples of such conditions include extremely low or high temperatures, strong winds, heavy rain, snow or ice, high humidity, dense fog, corrosive salt environments, lightning strikes and sand or dust particles.

Floods and low water conditions

3.30. During the review and assessment of an application at the siting stage, the regulatory body should verify that the following criteria for floods and low water conditions have been met:

(a) The maximum probable flood levels for individual types of flood causing phenomena and combinations of flood causing phenomena have been identified and analysed to establish the design basis flood for the nuclear facility. Operational challenges to the security system during such situations have been considered.
(b) Information provided by the applicant or operator demonstrates that engineered physical protection systems and related structures, central alarm stations and backup alarm stations and other security structures are designed and configured such that they can perform their intended security functions in the event of flooding. Engineered physical protection systems can be designed to protect digital, electronic and communication signal transmission lines in areas subject to flooding. In addition, a contingency plan, in line with regulatory requirements, is established for anticipated acute or prolonged flood conditions.
(c) Changes to site topography caused by low water conditions are considered when determining whether resulting conditions would challenge or impede the design of engineered and administrative controls for security. Low water conditions include drought, drawdown resulting from surges or tsunamis, ice, dams and dam failures, diversions and low tide. It should be demonstrated that security measures can provide continuous protection against attacks during potential low water conditions, which can result in pathways that are otherwise inaccessible because of water.

Geology and seismology

3.31. During the review and assessment of an application at the siting stage, the regulatory body should verify that evaluation criteria regarding geological and seismological conditions have been met. The geological and seismological characteristics of the proposed site support the determination of the adequacy of conclusions concerning the suitability of the site. In addition, information should establish the ground motion environment for the seismic design of the nuclear facility that could challenge or impede engineered and administrative controls necessary for the physical protection system.

DESIGN STAGE

3.32. Once the regulatory body grants authorization for the siting of a nuclear facility, the operator should establish the preliminary design of the physical protection system for the facility in accordance with the legislative and regulatory framework and ensuring compatibility with the site of the facility. As noted in Ref. [6], the design stage is, in some cases, an iterative process from a preliminary design to a final design. In other cases, when the facility design is procured from a vendor, the preliminary design of the physical protection system may be developed and approved in accordance with the regulatory requirements.

3.33. The preliminary design of the physical protection system should ensure that regulatory requirements can be met in accordance with the State's current design basis threat or representative threat statement.

3.34. Security costs can be optimized by taking nuclear security into account during the design of the nuclear facility rather than adding security systems and measures after the construction has been initiated. For example, the design should reduce the number of possible access points to vital areas; it should separate vital areas from areas accessed by large numbers of personnel; and it should consider the hardening of structures in accordance with the design basis threat. Such decisions during the design stage can make the protection of the vital areas much easier.

3.35. The physical protection system should be designed (based on a graded approach) by identifying the level and effectiveness of nuclear security measures, according to the design basis threat or representative threat statement, that provide protection against unauthorized removal of nuclear or other radioactive material and sabotage of the nuclear material or nuclear facility. The design of the physical protection system should incorporate the defence in depth principle in order to provide (a) reliability that the failure of a single security component does not result in the failure of the security function and (b) adequate security through equivalent protection measures regardless of which path or scenario the adversary might employ.

3.36. The applicant or operator should submit its preliminary security plan for the nuclear facility to the regulatory body for approval along with an application for authorization for construction. The preliminary security plan should contain the design of the physical protection system; training and qualification plan for security personnel; trustworthiness plan; information and computer security plan; and provisions for contingency planning and response. The preliminary security plan should also identify security areas of the facility and should include an initial

assessment of the radiological consequences of sabotage irrespective of whether the performance objective is or is not consequence based. This information should typically be provided to the regulatory body using the format and content prescribed by the regulatory body well in advance of the planned date to begin construction.

3.37. The regulatory body should review and assess the acceptability of the design of the physical protection system. On the basis of the review and assessment, the regulatory body should approve, comment on, question or reject the design or parts thereof, as necessary. Once the regulatory body has approved the preliminary security plan, it can issue a licence or other form of authorization to the applicant or operator for construction. The regulatory body may specify conditions to the licence or other form of authorization. In case the applicant or operator needs to revise the approved preliminary security plan as a result of changes to the threat environment, design modifications or compliance with new or revised regulations, it should receive the necessary approval from the regulatory body.

3.38. The security plan should be developed by the applicant or operator on the basis of the current threats, such as the design basis threat or representative threat statement. Various aspects of the design of the physical protection system may be reviewed against the recommendations provided in Ref. [2], such as consideration of the following:

(a) Credible scenarios by which adversaries could carry out acts of unauthorized removal of nuclear material or sabotage of nuclear facilities and nuclear material;
(b) Both external and insider adversaries who attempt to remove and/or disperse nuclear material or other radioactive material;
(c) Damage to, or interference with, structures, systems, components, equipment or devices important to nuclear safety and nuclear security, including a possible stand-off attack specified in the State's threat statements.

Submission of the preliminary security plan

3.39. The applicant or operator should prepare a preliminary security plan for review and assessment by the regulatory body. At a minimum, the preliminary security plan at this stage should address the physical protection elements that are included in the design of the nuclear facility and how the regulatory requirements associated with these elements are met. Reference [3] provides additional guidance on the suggested contents of the security plan.

3.40. At the design stage, the preliminary security plan should also describe the response strategy chosen by the operator and the initial deployment and location of response force personnel. The response strategy, depending on the intentions of adversaries (e.g. theft, sabotage) should include aspects such as denial of access, denial of task and containment. The preliminary security plan should describe how the various security functions will contribute to the response strategy (e.g. response timelines and performance expectations based on the detection, delay and response elements).

3.41. As far as possible, the preliminary security plan should be supported by more detailed information, which could include the following:

(a) The organizational structure of the applicant or operator, with defined roles and responsibilities for the implementation of the security plan.
(b) Provisional processes (both initial and continuing) for monitoring the trustworthiness and reliability of personnel, including checks on character, reputation, history, psychology and behaviour, and a fitness for duty plan.
(c) A provisional process for access authorization, which includes performance objectives and procedures for granting escorted and unescorted access to different areas.
(d) Provisional measures for searching personnel and vehicles for prohibited items in different security areas, including protected areas and vital areas.
(e) A training and qualification plan for security personnel.
(f) A contingency plan.
(g) Proposed response capabilities and protective strategy for the response forces (including the guard force) and liaison arrangements with external law enforcement or military agencies, as applicable.
(h) A description of computer security measures to demonstrate conformity with national regulations. This description should include the following information regarding computer security:
    (i) Identification of roles and responsibilities;
    (ii) Risk identification and management strategy;
    (iii) System security design and configuration management;
    (iv) Implementation of multiple layers and methods of protection (i.e. structural, technical and organizational);
    (v) Operational security procedures for access control, data security, communications security, platform and application security, continuity of operations, system monitoring, maintenance, incident handling and system backup;
    (vi) Personnel management through selection, training and qualification, transfer or termination of employment;

(vii) Periodic review and approval process;
(viii) Audit and review process and deficiency tracking and correction.

(i) An information security programme based on requirements established by the State or regulatory body for the protection of sensitive information used or generated during the design stage in accordance with Ref. [13].

(j) Details of buildings, site layout, civil construction aspects of the perimeter fence, physical barriers and barrier systems to be used as well as their functions within the physical protection system, including their locations and selection criteria based on their contribution to measures for delay.

(k) Categorization of nuclear material (in accordance with regulatory requirements) to design a related security system, including the design of material balance areas for nuclear material accounting and control, as applicable [7].

(l) Identification of the number and type of security areas (i.e. limited access areas, protected areas, inner and vital areas), including material balance areas for nuclear material accounting and control.

(m) A description of the protected area perimeter and the measures for deterrence, detection, delay, assessment and response to intrusion.

(n) Information on the evaluation of technologies and components (e.g. barriers, sensors, assessment systems) to determine which might best meet regulatory requirements for physical protection and nuclear material accounting and control (e.g. controls to enforce a two person rule).

(o) Information demonstrating that the operator reviews all engineering and design packages to ensure that nuclear security measures are included.

(p) Information showing that changes to the final facility design, and any subsequent facility design that affects nuclear security, meet regulatory requirements.

(q) A detailed description of lighting arrangements.

(r) A detailed description of the central alarm station, backup alarm station and how activities such as surveillance, observation and monitoring are performed in accordance with regulatory requirements.

(s) Proposed arrangements for on-site and off-site communications considering redundant and diverse provisions.

(t) A quality assurance plan with necessary provisions for the audit and review of the security plan at regular intervals.

(u) A plan for corrective and preventive maintenance and periodic testing of the physical protection system.

(v) Arrangements for record keeping and maintenance of the security plan.

(w) Information showing the coordination of design measures for nuclear security with other areas (e.g. safety, safeguards, operations) and allowing

for a comparison of relevant regulatory requirements, an identification of synergies and a resolution of potential safety and security conflicts.

3.42. It is unlikely that the security plan can be developed fully at this stage. The operator and the regulatory body should therefore expect the preliminary security plan to need revision. Additional reviews and assessments by the regulatory body may be needed as the design, construction and commissioning activities at the nuclear facility progress towards completion.

Review and assessment by the regulatory body

3.43. References [3, 6] present proposals for the review and assessment of the physical protection system (including structures, systems and components with nuclear security functions) to be performed by the regulatory body at the design stage of a nuclear facility.

3.44. The general considerations described in paras 3.45–3.49 present areas of review and assessment by the regulatory body and are intended to elaborate the proposals in Refs [3, 6].

Programmatic criteria

3.45. As part of its regulatory infrastructure, each State should develop standards for conducting reviews and assessing the applications for authorization submitted by operators, and for deciding whether these applications will be approved. The criteria in the following areas may be considered for use by the regulatory body in evaluating the adequacy of the applications submitted by operators at the design stage:

(a) Security plan. Once the preliminary security plan has been prepared and submitted as part of the application to obtain authorization for the construction of a nuclear facility, it should be reviewed against the established regulatory requirements related to the design basis threat or representative threat statement. The plan should include the contents specified in the regulatory framework and should be in the requested format.
(b) Integrated management system. The regulatory body should ensure that a management system is in place at the design stage and that the security plan and security management system are included in the overall integrated management system. Quality assurance policies and programmes should be prepared for ensuring that the physical protection system will be designed to address the design basis threat or representative threat statement and other

applicable regulatory requirements. The regulatory body should ensure that the operator has a security management system in which policies and procedures are established that (i) give due priority to security, (ii) define clear lines of authority for decisions on security, (iii) identify the security responsibilities of all facility personnel, and (iv) ensure that all facility personnel are suitably trained and qualified.

(c) Contingency plan. The regulatory body should ensure that the operator has included a contingency plan as a part of the security plan. The regulatory body should specify the principles to be applied in the development of the contingency plan and approve its implementation.

(d) Information security. The operator should identify all information whose unauthorized disclosure could compromise the physical protection system and the system, programme and set of rules in place to ensure the protection of information in any form during the design stage (and beyond). The regulatory body should evaluate the adequacy of the information security measures employed by the operator. The regulatory body and the operator should limit access to sensitive information to only those individuals who have a 'need to know' and the appropriate security clearance.

(e) Computer security. The operator should protect computer based systems used to generate sensitive information about the security plan and physical protection system of the facility. Computer based systems to be protected should also include systems used by vendors or subcontractors to the operator. The regulatory body should evaluate the adequacy of the protective strategies and systems employed by the operator to guard this information. Operators should limit access to sensitive computer systems to only those individuals who have a 'need to know' and the appropriate security clearance.

(f) Trustworthiness of personnel. The regulatory body should ensure that the operator has prepared a programme that meets the regulatory requirements for determining and ensuring the trustworthiness of personnel. Only personnel who have been determined to be trustworthy should be granted authorized (unescorted) access to protected areas, to sensitive information (e.g. the design of the physical protection system), to facility equipment or systems, including computer based systems, and to nuclear or other radioactive material.

(g) Reporting of nuclear security events. The operator should comply with the reporting procedures specified in the security plan if nuclear security events occur or in the case of any failure to comply with applicable regulatory requirements. For example, any compromise of sensitive information during the design stage should be considered a nuclear security event.

(h) Compensatory measures and corrective actions. If for any reason the physical protection system is not capable of providing the required level of protection, the operator should immediately implement compensatory measures to provide adequate protection. During the design stage, it is possible to identify a number of typical cases that can occur during the lifetime of the facility and to identify planned compensatory measures for such situations. The regulatory body may identify a list of such situations to be covered by the security plan and compensatory measures may be approved as part of the security plan.

3.46. The regulatory body should ensure that design modifications remain in compliance with regulatory requirements. Such a review by the regulatory body could also help to determine if a revision to the preliminary security plan is needed and if another assessment is needed.

3.47. The regulatory body should ensure that the operator has the necessary financial capabilities to begin and subsequently complete the establishment of the physical protection system in accordance with the construction schedules provided by the operator.

Technical criteria

3.48. For applicants or operators of existing facilities where the application for authorization will add a new facility to the site, the regulatory body should ensure that the following are addressed:

(a) The security design incorporates the specific design principles for each security area.
(b) The operator evaluates the impact of facility construction activities on the security of any nuclear facilities collocated on the site and any interfaces with other competent authorities.
(c) The operator provides the results of this evaluation to the regulatory body for review and approval.
(d) The operator identifies and implements corrective actions to resolve any potential issues with the nuclear security interface between the nuclear facility that is being constructed and any facilities collocated on the same site.

3.49. For applications for authorization of new facilities, with no pre-existing facility on the site, the regulatory body should ensure that the following security areas are established:

(a) Limited access area:
    (i) Provisions are made for detecting intrusion into the limited access area.
    (ii) Provisions are made for appropriate actions by guards or response forces in case of intrusion into the limited access area.
    (iii) Technical means and procedures for access control are established and protected against compromise.
(b) Protected area:
    (i) The protected area perimeter includes appropriate physical barriers.
    (ii) The protected area perimeter includes arrangements for monitoring with equipment for intrusion detection and assessment.
    (iii) The equipment for intrusion detection and assessment has the following properties:
        — It is tamper protected, tamper indicating and self-checking (including transmission lines);
        — It is provided with an uninterruptible power supply;
        — It provides an automatic indication when the alarm system or a component of the alarm system fails or when the system is operating on the backup power supply.
    (iv) The design provides adequate lighting to allow observation and assessment by patrolling guards and/or a surveillance system.
    (v) The number of access points and the number of personnel who need access to the protected area are kept to the minimum necessary. All points of potential access are secured and linked to an alarm system to detect attempts of unauthorized access.
    (vi) The design ensures effective access control measures for the identification of authorized persons entering the protected area, for escorted and unescorted access and for keeping appropriate records.
    (vii) The design provides for searches of all personnel, vehicles and packages entering the protected area, including searches for firearms, explosives or incendiary devices.
    (viii) The design of the central alarm station provides for the following:
        — The establishment of a permanently and adequately staffed central alarm station for monitoring and assessing alarms, initiating response and communicating with guards, response forces, facility management and local law enforcement;
        — Access to an uninterruptible power supply and tamper protection against unauthorized monitoring, manipulation and falsification;
        — Dedicated, redundant, secure and diverse transmission systems for two way voice communication between the central alarm station and the response forces;

— Dedicated two way secure voice communication between guards and the central alarm station.

(ix) For guards and response forces, the design provides for the following:
— The presence of a 24 hour guard service and response forces that are trained and equipped to ensure an adequate and timely response to prevent action by an adversary;
— Random patrols of the protected area.

(c) Vital areas:
(i) The process of vital area identification is verified (see IAEA Nuclear Security Series No. 48-T, Identification and Categorization of Sabotage Targets, and Identification of Vital Areas at Nuclear Facilities [14]).
(ii) Arrangements are made by the applicant or operator to maintain the records of all persons who have access to or possession of keys, keycards and/or other systems, including computer systems, that control access to nuclear material or to vital areas.
(iii) The design provides for:
— Vital areas that are appropriately secured and linked to an alarm system;
— The timely detection of tampering or interference with equipment or systems in the vital areas;
— Sufficient delay and/or denial measures against unauthorized access that consider the capabilities of both an insider and an external adversary;
— The installation of vehicle barriers at an appropriate distance from the vital areas;
— Measures to determine trustworthiness of personnel for authorized access to vital areas;
— Adequate searches on entering and exiting vital areas.

3.50. Once the regulatory body has reviewed and approved the preliminary security plan and granted the relevant licences or other forms of authorization, the applicant or operator may start construction and installation activities relating to the physical protection system in parallel with the construction and installation of the facility's structures, systems and components.

CONSTRUCTION STAGE

3.51. The construction stage includes the manufacture and assembly of the structures of the nuclear facility and the installation of systems and equipment at the facility, including the physical protection system. Authorization for

the construction of a nuclear facility is usually granted only after successful demonstration by the applicant or operator that (a) the security plan meets the applicable regulatory requirements and (b) all considerations relating to the influence of the site characteristics on the facility design (and any corresponding impacts of the facility design on the site) have been addressed satisfactorily.

3.52. The implementation of security measures during the construction stage presents unique challenges. Depending on the number and extent of facility construction activities, many people might be on the site, and the flow of persons, vehicles and materials entering and exiting the construction site on a daily basis might be significant. The operator should implement measures to meet regulatory requirements for nuclear security during the construction stage, including for access control, computer security, sustainability, contingency planning, emergency preparedness, reporting of nuclear security events, trustworthiness, the management system, nuclear security culture and nuclear material accounting and control, as applicable. The applicant, operator or other entity responsible for facility construction should maintain continuous vigilance to ensure the following:

(a) Protection against delayed impact threats, such as the possible planting of sabotage initiating devices or explosives for a future sabotage attempt, or malicious software programmed to act at a later time;
(b) Security in the supply chain, which includes guarding against the procurement of flawed components or software that, when installed, might adversely affect nuclear security or nuclear safety at a later date;
(c) Implementation of information security and trustworthiness programmes to limit access to sensitive information to only those individuals who have a 'need to know' and the appropriate security clearance.

3.53. The applicant or operator should take the following actions:

(a) Evaluate the impact of facility construction activities on the security of any nuclear facilities collocated on the site and any interfaces with other regulatory bodies.
(b) Provide the results of this evaluation to the regulatory body for review and approval.
(c) Identify and implement corrective actions to resolve any issues with the nuclear security interface between the nuclear facility that is being constructed and any facilities collocated on the same site.

3.54. Important milestones in the construction of the physical protection system may be identified as 'hold points' that are subject to additional regulatory approvals

as part of the licence or other form of authorization for construction. These hold points should be identified during the regulatory review and assessment of the security plan and the design of the physical protection system.

3.55. The identification of hold points can be useful for both the operator and the regulatory body, especially in the following situations:

(a) If checks or verifications cannot be made later (e.g. if the regulatory body wants to monitor the installation of underground equipment or components);
(b) If certain regulatory requirements should be met before beginning another phase of the construction (e.g. completing the installation of a perimeter for the protected area before beginning or continuing other security sensitive activities).

3.56. Examples of important milestones and potential hold points in the construction of a nuclear facility include the following:

(a) The approval of the schedule for the construction and acquisition of structures, systems and components important to nuclear security and nuclear safety;
(b) The installation of equipment for intrusion detection and assessment, such as cameras or lighting systems;
(c) The testing of physical protection system components to confirm system functionality in preparation for commissioning;
(d) The verification of adherence to system design specifications throughout the construction stage to ensure that the acceptance criteria associated with specific performance standards have been satisfied;
(e) The installation and testing of the fire protection system and other safety systems that support the physical protection system.

3.57. The regulatory body should review, assess and inspect, if necessary, each defined hold point before granting authorization to proceed to the next step of the construction process.

3.58. The operator should ensure that the appropriate features of the security plan are implemented and remain in effect at the site during the construction of the facility. The elements of nuclear security that are necessary during the construction stage should be included in the security plan and reviewed prior to authorization for construction (i.e. during the design stage).

3.59. The operator may propose changes to the approved design of the physical protection system and security plan during construction; significant changes should be submitted to the regulatory body. The regulatory body should then review and assess the justification provided by the operator for the changes against the original design, applicable regulatory requirements and existing licence conditions before approving the changes.

3.60. The operator and the regulatory body need to recognize that adversaries might attempt to create vulnerabilities during the construction stage for possible exploitation at a later date. For example, explosives or weapons might be introduced and hidden within the site if proper boundaries and access controls are not in place. The operator should conduct a final inspection at the end of the construction stage to confirm that no prohibited items have been introduced into the facility.

Submission of updated information and additional documentation

3.61. During the construction stage, the operator should submit updated quality assurance plans for security related structures, systems and components, as well as reports on the status and progress of the construction of these elements, as agreed by the regulatory body. The operator should also submit any documentation or information regarding the security plan and related physical protection system that was not available during the design stage. As defined in the State's legislative and regulatory framework, the regulatory body may require the operator to provide additional documentation or information needed to conduct the review and assessment.

3.62. The security plan should include procedures for developing and implementing measures to ensure the adequate protection of facilities, equipment and other assets during the construction stage. The security plan should also include procedures on information security and computer security to ensure the protection of computer based systems and sensitive digital assets (including safety systems, operational systems and security systems).

3.63. The operator should submit the following additional information during the construction stage:

(a) A framework and schedule for the construction and acquisition of nuclear security related structures, systems and components.
(b) Periodic reports of construction progress, confirming that nuclear security related structures, systems and components are being constructed in

accordance with the design parameters identified by the operator and approved by the regulatory body. Any deviations from the approved design should be analysed fully in relation to the original design intentions, and the operator should submit analyses of the deviations and any conclusions drawn from the analyses (including needed corrective action) to the regulatory body for review, assessment and subsequent approval.

(c) Reports on the resolution of any issues relating to the interfaces between nuclear security and nuclear safety.

(d) Reports on the implementation by the operator of a programme for trustworthiness assessment of personnel with access to sensitive information during the construction stage, such as facility drawings, secured computer network equipment and physical protection systems. The operator should also have a system in place, or use an existing system, for the classification of sensitive information as prescribed by the regulatory body, consistent with the State's legislative and regulatory framework, to determine the level of sensitivity of information relating to the facility's design and the use of nuclear material.

(e) The configuration management programme. Changes in the design during the construction stage should not be implemented until they have been reviewed and approved by the regulatory body to ensure that these changes do not affect the ability of the operator to meet regulatory requirements.

(f) The procurement programme and information about controls. These controls ensure that physical protection system equipment as well as other systems and equipment that contribute to nuclear security and nuclear safety are procured in accordance with established procedures and kept in secure storage until installation. The controls also ensure that the procurement process includes the use of vendors approved in advance of the procurement process and no public bidding.

(g) Documentation of post-installation acceptance tests of physical protection system equipment, information and computer security systems and other systems or equipment that contribute to nuclear security and nuclear safety (including support systems such as backup power). This documentation ensures that the equipment meets defined functional, operational and performance criteria.

Review and assessment by the regulatory body

3.64. During the construction stage, the regulatory body might not need to perform additional reviews and assessments after the licence or other form of authorization for construction has been granted. However, in certain cases the regulatory body might find it necessary to conduct additional activities for review

and assessment. Examples of such cases include changes to the approved design of the physical protection system or any part of the security plan. To support the review and assessment, the regulatory body may require progress reports to track, witness, and verify or inspect any hold points and conditions of authorization, as specified in the licence or other form of authorization for construction, to confirm that the conditions of authorization are being fulfilled by the operator.

3.65. Using the information submitted by the operator (see paras 3.61–3.63), the regulatory body may consider additional activities for review and assessment during the construction stage, such as the following:

(a) Review and assess, as appropriate, the activities conducted by the operator in accordance with the approved facility construction schedule, including the construction and installation of nuclear security related structures, systems and components.
(b) Ensure that control is exercised by the operator over contractors and suppliers that are performing tasks in support of nuclear security related structures, systems and components.
(c) Review and approve, in accordance with the regulatory framework of the State, any significant changes to the security plan or any modifications to the design of the physical protection system.
(d) Assess the adequacy of nuclear security evaluations performed by the operator.
(e) Assess periodically the financial capability of the operator to establish the physical protection system in accordance with the licence or other form of authorization granted by the regulatory body and the construction schedules provided by the operator.
(f) Ensure that the operator has identified and resolved satisfactorily any issues relating to the interfaces between nuclear security, nuclear safety and nuclear material accounting and control.

COMMISSIONING STAGE

3.66. The operator should implement measures to meet the regulatory requirements for nuclear security during the commissioning stage, including requirements for computer security, sustainability, contingency planning, emergency preparedness, incident reporting, trustworthiness, quality assurance, nuclear security culture and nuclear material accounting and control, as applicable. Before nuclear material arrives on the site, the approved physical protection system should be commissioned (i.e. put into operation and verified to be in

accordance with the design and to have met the defined performance criteria for protection against the unauthorized removal of nuclear material and sabotage). Testing through drills and exercises should be conducted by the operator, and witnessed by the regulatory body, if required, before nuclear material is received and introduced into the facility's process systems. Subject to the regulatory requirements, the regulatory body may also require the operator to conduct performance testing and evaluation of the physical protection system.

3.67. Before the end of the construction stage and well before the facility is commissioned, the operator should ensure that the security plan has been implemented and should request authorization for commissioning by submitting the nuclear security commissioning programme to the regulatory body. The nuclear security commissioning programme should include information on the specific commissioning activities for nuclear security related structures, systems and components and information on security focused programmes and protocols. Some individual security related structures, systems and components may need to be commissioned before the end of the construction stage. For example, access control may be needed from the start of the construction stage. The nuclear security commissioning programme should provide evidence that the physical protection system will be fully tested against approved acceptance criteria and in accordance with a management system, ensuring that any non-compliance will be detected and addressed adequately.

3.68. The regulatory body may require the operator to obtain prior approval for certain steps in the commissioning process. As such, the regulatory body should consider introducing hold points at key steps in the commissioning programme (e.g. acceptance testing of physical protection system components to confirm system functionality).

3.69. By approving the commissioning programme, the regulatory body allows commissioning to commence. The operator should conduct drills and exercises to test the validity of operational plans and procedures and provide an opportunity for security personnel to learn skills and to acquire experience in operating the security systems. The results of the drills and exercises and of the personnel training should be documented and made available to the regulatory body for review.

Submission of the commissioning programme and the updated security plan

3.70. Before construction is completed, the operator should submit the commissioning programme to the regulatory body for approval to proceed to the commissioning stage.

3.71. If required by the regulatory body, the operator should submit a revised security plan, including the following sub-plans, that reflects experience from construction activities or changes to the facility's mission, features or programmes:

(a) Training and qualification plan;
(b) Insider threat mitigation plan, including a programme to confirm trustworthiness of personnel and an access control programme;
(c) Information and computer security plan, including procedures for information security and computer security to ensure the protection of computer systems and sensitive digital assets (including safety systems, operational systems and security systems);
(d) Contingency plan;
(e) Performance testing and maintenance programme, including drills and exercises;
(f) Documentation on compensatory measures that provide equivalent levels of protection in case the elements of the physical protection system do not function properly during commissioning or at any time after commissioning;
(g) List of all implementing procedures for the nuclear security plan;
(h) Documentation of the management system for operation.

3.72. The operator's performance testing programme should include the implementation of measures to meet the regulatory requirements for the timely detection of, and appropriate response to, computer security incidents and the unauthorized removal of nuclear material or sabotage. Furthermore, if the operator needs to receive and store nuclear material before the facility is commissioned, the regulatory body may require the operator to provide a separate security plan to address specifically how the operator will meet the regulatory requirements for protecting the material during storage.

3.73. The operator should also provide documentation showing that adequate provisions have been made to ensure the availability of resources necessary for commissioning and during operation. These include human resources, support systems, emergency preparedness, infrastructure, financing and materials.

3.74. After the operator has installed the access control system, but before the system is put into operation, the operator should search the entire facility for any contraband or prohibited items (e.g. explosives, incendiary devices). The regulatory body should receive a statement from the operator confirming that this activity has been completed. The regulatory body may consider conducting an inspection to verify that the activity has been performed satisfactorily.

3.75. If deviations from design specifications for nuclear security related structures, systems and components are identified during the commissioning process, the operator should document the deviations and provide the information to the regulatory body. Documentation should include an assessment of the deviation (i.e. accept as is, rework or redesign) that clearly demonstrates that the approved design of the physical protection system remains valid and that nuclear security has not been compromised.

Review and assessment by the regulatory body

3.76. The regulatory body should review and approve the nuclear security commissioning programme (including procedures and evaluation criteria for the physical protection system) before the facility is commissioned. The regulatory body may also verify, through inspections, performance testing and evaluation, that the commissioning tests of the physical protection system have been completed.

3.77. Before nuclear material arrives on the site, the operator should assess the structures, systems and components important to nuclear security after their construction and installation have been completed and confirm that they satisfy the approved design.

3.78. The regulatory body should track and confirm the satisfactory completion of work at hold points agreed with the operator. Any deficiency identified by the regulatory body should be communicated to the operator. If a deficiency is expected to have a significant impact on the approved design of the physical protection system, the regulatory body may decide to withhold or suspend authorization until the deficiency has been corrected and the work has been verified to be acceptable.

3.79. If an identified deficiency is not significant, the regulatory body may consider allowing the operator to continue the commissioning process, if the operator agrees to correct the deficiency within a specified time frame or before the next hold point. The regulatory body may require the operator to communicate periodically the status and disposition of identified deficiencies. Furthermore, the regulatory body may concur with the disposition of any deviations from the design identified by the operator or require further action for resolution.

3.80. Before authorizing the receipt of nuclear material on the site or the introduction of nuclear material in the facility's process systems, the regulatory body should complete a review and assessment of the following:

(a) Physical protection system:
    (i) The as-built design of the physical protection system;
    (ii) Evaluation of system effectiveness by the operator (i.e. vulnerability analysis and performance testing);
    (iii) The results of individual component tests and the system full functionality test, including verification processes and acceptance criteria for physical protection equipment and other systems and equipment that contribute to nuclear security.
(b) Management aspects:
    (i) The security plan, including the sub-plans presented in para. 3.71;
    (ii) The facility's management system, including procedures for implementing and maintaining the security plan;
    (iii) The organizational structure of the applicant or operator, including the training and qualification of personnel whose positions contribute to nuclear security in accordance with their assigned responsibilities;
    (iv) The recording and reporting systems, as required, including those for operational data of the physical protection system, maintenance and test results, reporting of deviations and nuclear security events, and nuclear material accounting and control;
    (v) Evidence of the completion of training and qualification for key nuclear security personnel and other personnel whose positions contribute to nuclear security;
    (vi) The access control and trustworthiness programme (as part of an overall insider threat mitigation plan) and nuclear security culture programme of the applicant or operator;
    (vii) Programmes or agreements for sharing information on nuclear security events with the operators of nuclear facilities or high hazard facilities that are either collocated with or in close proximity to the nuclear facility being commissioned for operation;
    (viii) The applicant or operator's financial capability of completing the commissioning and subsequently implementing the security plan in accordance with the licence or other form of authorization granted by the regulatory body, and with the schedules provided by the operator.
(c) Operational provisions:
    (i) The adequacy of operating instructions and procedures needed to implement the security plan.
    (ii) Arrangements for contingency planning (i.e. for on-site and off-site response to emergencies and nuclear security events) and confirmation that the contingency plan for the facility is consistent with the State's response plan.

(iii) The implementation of safety arrangements important for nuclear security (i.e. interfaces between nuclear safety and security).
(iv) Measures for accounting and control of nuclear and other radioactive material (e.g. systems for nuclear material accounting and control (see Ref. [7])).
(v) Results of performance tests for the timely detection of unauthorized removal of nuclear material or sabotage of nuclear material or the nuclear facility. The review should consider whether the scenarios for unauthorized removal and sabotage are comprehensive, whether the analysis methodology applied is appropriate and whether the conclusions reached by the operator are correct.

3.81. The regulatory body should include the implementation of the security plan as one of the conditions in the operating licence issued to the operator of the nuclear facility.

OPERATION STAGE

3.82. The security plan, as approved by the regulatory body, is the basis for implementing the physical protection system on the site during the operation stage (i.e. during operational states and accident conditions). Consequently, the regulatory requirements for operation should require the operator to establish procedures for the continued implementation of the security plan, including the maintenance and performance testing of structures, systems and components of the physical protection system. The regulatory body should require the operator to conduct periodic reviews of the security plan and to test the physical protection system and procedures at a defined frequency. If deficiencies are found in the procedures or in the operation of the physical protection system, the operator should take corrective action and, if necessary, update the procedures. The operator should maintain and update all procedures in its management system that are necessary for implementing the security plan.

3.83. The operator should conduct periodically a detailed review of the facility's physical protection system to demonstrate that the facility remains in compliance with regulatory requirements for nuclear security and is protected against the design basis threat or representative threat statement, as applicable. This review should include an assessment of the following aspects of the physical protection system: structures, systems and components; procedures; and interfaces with safety and with nuclear material accounting and control.

3.84. Before making significant modifications to arrangements detailed in the approved security plan, the regulatory body should require the operator to submit the revised security plan for approval by the regulatory body. These modifications involve revisions of the security plan to address (a) changes in the configuration of the physical protection system that could affect its effectiveness, (b) changes in the design basis threat or representative threat statement, or (c) new performance tests needed to confirm that the revised security plan and physical protection system will be able to address successfully a new threat environment. The regulatory body should verify through inspections the operator's compliance with the revised security plan and procedures. If, during periods of extended shutdown, there are changes important to nuclear security, the operator should submit a revised security plan to the regulatory body for approval.

3.85. Where several collocated facilities share common security related features, the operator should ensure that nuclear security is not compromised in any of the facilities and that adequate measures are in place for simultaneous response to nuclear security events and emergencies at each of the collocated facilities.

3.86. During the operation stage, all applicable regulatory requirements and conditions of the licence or other form of authorization have to be met at all times, including during periods of extended shutdown such as for refuelling, refurbishments, major maintenance or modification activities or recovery from a significant event.

3.87. The operation stage can last for several decades and this period might include technological improvements and the evolution of threats and regulatory requirements. Thus, the security plan and the physical protection system might need to undergo several major reviews and revisions during the operation stage. Furthermore, the operator should pay attention to obsolescence issues caused by technological improvements and supply chain interruptions caused by the shutdown of major vendors. When possible, these issues should be anticipated and plans should be established to mitigate the impacts of their occurrence.

Submission of periodic updates and reports

3.88. During the operation stage, the operator should sustain the effectiveness of the security plan, the physical protection system, and the information security and computer security management systems. The security plan should be reviewed periodically by the operator's personnel, independent of those personnel who are responsible for management and implementation of the security plan. The independent review should be performed only by individuals who have a

'need to know' and whose trustworthiness has been established. The results of and recommendations from the review of the security plan and a record of any corrective actions taken should be submitted to the regulatory body.

3.89. In addition to confirming that the nuclear security strategy for the facility addresses satisfactorily the design basis threat or the representative threat statement, the operator should describe arrangements for implementing measures that will provide additional protection from temporary increases in the threat environment.

3.90. The operator should make appropriate arrangements for reporting to the regulatory body any deviation from the approved security plan. The operator should also provide routine reports, as required by the regulatory body, on security performance, periodic performance testing of the physical protection system, adherence to regulatory requirements, compensatory measures implemented to address identified deficiencies and efforts being made to enhance security.

3.91. The operator should implement a programme for nuclear material accounting and control for nuclear security purposes to update information such as type, form, quantity and location of nuclear material, as well as a system of approvals and record keeping at the facility. The operator's programme for nuclear material accounting and control should include measures implemented to meet the State's requirements for the timely detection of unauthorized removal of nuclear material and for protection against insider threats.

3.92. The operator should establish a testing protocol for conducting regular evaluations, including periodic performance testing, to validate the effectiveness of individual nuclear security measures as well as the efficiency of the overall nuclear security system. The testing protocol should assess the performance of physical protection measures and security personnel, including response forces. Furthermore, the operator should conduct regular security exercises and drills, which should include coordination with off-site resources, for all potential operating conditions to ensure the continued validity of the contingency plan and procedures. The operator should provide documentation of the results of the tests conducted, including corrective actions taken, to the regulatory body.

Review and assessment by the regulatory body

3.93. The regulatory body usually performs a review and assessment of the documents identified in paras 3.88–3.92. The review and assessment activities

during the operation stage (including for the renewal of the operating licence) include the following:

(a) The regulatory body should review, assess and reapprove the revised security plan to confirm that the plan addresses the current threat statements, meets the objectives of the nuclear security system and meets established evaluation criteria.
(b) The regulatory body may decide to review the procedures relating to the security plan or to verify compliance with these procedures during an inspection.
(c) The regulatory body should review and assess the operator's arrangements for protection from temporary increases in the threat environment.
(d) If aspects of the approved security plan are not being met because part of the physical protection system is not functioning, the operator should implement compensatory measures that provide equivalent levels of protection. The regulatory body should assess the effectiveness of any compensatory measures implemented.
(e) The regulatory body should require the operator to regularly review and update the security plan to ensure that it reflects current conditions at the facility and changes in the design basis threat, the representative threat statement or regulatory requirements.
(f) The regulatory body should periodically review the interface between the national response plan and the operator's contingency plan for the facility to ensure that they are consistent and provide the appropriate interfaces with nuclear safety and with nuclear material accounting and control.
(g) The regulatory body may periodically review the operator's activities to ensure the following:
    (i) That the scenarios for the unauthorized removal of nuclear material and sabotage are comprehensive;
    (ii) That the analysis methodology applied is appropriate;
    (iii) That the conclusions reached by the operator are correct.
(h) The regulatory body should evaluate the effectiveness provided through multiple protection elements and whether the operator needs to take steps to increase the effectiveness of those intrusion detection elements.
(i) The regulatory body should periodically assess the operator's ability to continue operation, and eventually decommission the nuclear facility in accordance with the operator and authorization schedules.
(j) The regulatory body should be assured that the operator is continually sharing information, in accordance with national laws and regulations as applicable, on nuclear security events with the operators of nuclear or high

hazard facilities that are either collocated with or in close proximity to the nuclear facility.

(k) The regulatory body should continue to assess the potential impact on the operation of the nuclear facility arising from the operation of nuclear facilities or high hazard facilities that are either collocated with or in close proximity to the nuclear facility.

(l) The regulatory body should review the operator's compliance with the trustworthiness programme.

CESSATION OF OPERATION STAGE

3.94. Paragraph 2.10 of Ref. [6] states:

> "The cessation of operation stage describes a planned condition at a nuclear facility in which facility operations have ceased either permanently in preparation for decommissioning or for an extended period of time for major modifications, maintenance or repair."

In such circumstances, the regulatory requirements for the facility are not expected to change significantly until the nuclear material utilized by the facility is moved either off the site or to a protected storage location on the site. However, before the location of the nuclear material changes from that normally used for facility operations, the operator and the regulatory body should consult and agree on the set of actions to be taken by the operator. These actions should be consistent with the applicable regulations and authorization conditions. The operator should submit information to the regulatory body describing the activities taken at the facility to ensure that nuclear security measures are being maintained to address the current threat statement, to meet the objectives of the nuclear security system and to accord with written agreements and commitments made between the regulatory body and the operator.

3.95. The operator should ensure that the security plan remains valid and the physical protection system remains intact until the nuclear material used at the facility has been moved off the site.

Submission of updated information

3.96. Typical operator submissions to the regulatory body during the cessation of operation stage should include the following information:

(a) A formal notice from the operator that the nuclear facility is transitioning to the cessation of operation stage. This notice is more likely to be needed when the facility's operating licence has expired or the need for the facility has ended, and when the commencement of decommissioning activities is not expected in the near future. Such a notice is usually not needed in situations in which the operator intends to resume facility operations.
(b) Documentation of any changes to the nuclear material (e.g. inventory, location) or nuclear facility during this stage. This includes a re-evaluation of the risk of unauthorized removal and sabotage, and the implementation of any new physical protection measures using a graded approach.
(c) A revised security plan that addresses changes in operation, facility configuration and compensatory measures.

Review and assessment by the regulatory body

3.97. The regulatory body should perform the following review and assessment activities during the cessation of operation stage:

(a) Issue a specific authorization under the current licence, or under a new licence, for changes in the nuclear security of the facility during the cessation of operation stage, in accordance with regulatory requirements and taking into account the reason for the shutdown of the facility.
(b) Review and approve the revised security plan, including the contingency plan, before its implementation.
(c) Verify that the new nuclear security configuration at the facility complies with regulatory requirements and the operator's security plan.
(d) Adapt inspection activities (including type and frequency of the inspections) to the needs of the cessation of operation stage.

DECOMMISSIONING STAGE

3.98. Paragraph 3.30 of Ref. [6] states:

> "The decommissioning stage involves activities that will ultimately lead to the removal of all nuclear material and other radioactive material from

the facility. However, as long as a risk of unauthorized removal of nuclear material or of sabotage leading to unacceptable radiological consequences remains, nuclear security measures should be maintained. The application of these measures should be based on a graded approach, taking account of the category of nuclear material and its potential for sabotage leading to unacceptable radiological consequences."

3.99. The decommissioning stage usually consists of one or more substages, each of which may be subject to regulatory authorization. Different human resources and competencies are needed for the decommissioning stage than for the operation stage. The regulatory requirements for nuclear security during the decommissioning stage should depend on the inventory of nuclear and other radioactive material present on the site, which may vary according to the decommissioning substage, and should be developed in accordance with a graded approach.

3.100. The decommissioning process usually involves the gradual removal of nuclear and other radioactive material, including waste material, and might necessitate the implementation of changes to the security plan and physical protection strategies and systems. The level of nuclear security measures is determined taking into account changes to the inventory of nuclear and other radioactive material and the attractiveness of this material to an adversary. The type and quantity of material present on the site may vary depending on how much time has passed since the nuclear facility last operated. The regulatory body should ensure that the operator maintains an adequate level of nuclear security for the nuclear and other radioactive material, which might include maintaining response protocols as part of the contingency plan. Furthermore, specific protection strategies may be required by the regulatory body because the removal of material during decommissioning can lead to extensive transport activities that represent an opportunity for adversaries.

3.101. Based on the status of facility decommissioning activities, changes to the existing licence or its conditions relating to nuclear security may be needed once the material has been removed from the site. The regulatory body may use a graded approach to evaluate the adequacy of nuclear security measures, taking into account the site conditions (e.g. unauthorized removal and sabotage scenarios no longer apply after the nuclear material has been removed from the site).

3.102. The regulatory body should ensure that the operator continues to protect the inventory of nuclear and other radioactive material remaining on the site in accordance with the legislative and regulatory framework. Following completion of the decommissioning programme, the operator should demonstrate to the

regulatory body that all nuclear and other radioactive material has been removed from the site, and that no security related concerns exist. The regulatory body might then perform a confirmatory review (depending on the State's regulatory requirements) before releasing the site from regulatory control.

3.103. Insider threats might evolve during the decommissioning stage because of the following:

(a) An increased number of workers on the site from organizations other than the operator;
(b) The short term nature of work assignments during decommissioning;
(c) The large number of decommissioning activities, which increases the opportunities for malicious acts;
(d) A decreased workforce and potentially disgruntled employees facing unemployment who might attempt to use their knowledge for financial gain or to sabotage the facility.

3.104. Changes in material inventories during the decommissioning process can result in the following:

(a) New targets for adversaries;
(b) Different levels of radiological consequences associated with sabotage;
(c) Different attractiveness levels for unauthorized removal of nuclear material.

3.105. After nuclear material has been removed and when only radioactive material remains on the site, different regulatory requirements may apply, and the operator should revise the security plan to comply with any new regulatory requirements. The operator may consider the protection of radioactive material on the site in the revised security plan, on the basis of the guidance provided in IAEA Nuclear Security Series No. 11-G (Rev. 1), Security of Radioactive Material in Use and Storage and of Associated Facilities [15]. The original physical protection system may be retained or modified in accordance with Ref. [15]. The need to retain or modify the physical protection system is determined by the location and amount of radioactive material and the potential for unauthorized removal or sabotage leading to unacceptable radiological consequences.

3.106. The operator should not be permitted to lower the performance level of the facility's physical protection system, even after nuclear material has been removed, without prior authorization by the regulatory body.

Submission of the application for authorization

3.107. To shut down the nuclear facility permanently, the operator should request authorization for decommissioning from the regulatory body. This authorization should be requested well before operation is terminated.

3.108. The operator should notify the regulatory body of the intent to transition to the decommissioning stage.

3.109. The application for authorization for decommissioning should include a revised security plan and associated sub-plans that should address the following:

(a) The identification of any new areas for the temporary storage of nuclear material and of existing (or a reduced number of) vital areas based on the inventory of nuclear and other radioactive material and the potential radiological consequences of sabotage;
(b) A personnel screening and reliability programme for vendors and subcontractors engaged in decommissioning activities.

3.110. Updates to the inventory of nuclear and other radioactive material should be submitted to the regulatory body as decommissioning proceeds. The inventory may also include radioactive material in stored containers resulting from the waste management activities of the decommissioning process.

3.111. The operator should identify any new potential targets for an adversary resulting from decommissioning activities, re-evaluate the risk of unauthorized removal or sabotage, and develop physical protection measures using a graded approach in accordance with regulatory requirements. This information should be submitted to the regulatory body.

3.112. The operator should revise the security plan before moving to the decommissioning stage and submit it to the regulatory body for approval. The revision should take into consideration facility operations and regulatory requirements for nuclear safety and should be coordinated with other interested parties to avoid conflict.

3.113. The operator should adjust the measures for the protection of sensitive information assets as the classification of information changes and the assets are removed from service.

3.114. Finally, the operator should submit a report to the regulatory body indicating that all nuclear and other radioactive material with the potential for unauthorized removal or sabotage leading to unacceptable radiological consequences has been properly removed from the site. Before termination of the licence and release of the site from regulatory control, the operator should conduct a verification of the inventory. This should be verified by the regulatory body to ensure that the regulatory exemption criteria and decommissioning objectives have been fulfilled.

Review and assessment by the regulatory body

3.115. Based on the security plan for the decommissioning stage, the regulatory body should either issue a new authorization or modify an existing one, as appropriate for this stage. The regulatory body should review and approve the security plan for the decommissioning stage and should ensure that the operator's contingency plan is consistent with the national response plan. The regulatory body should adapt its inspection activities for the decommissioning stage, including the scope and frequency of inspections, taking into account other interested parties.

3.116. The regulatory body should review the report submitted by the operator indicating that all nuclear and other radioactive material with the potential for unauthorized removal or sabotage leading to unacceptable radiological consequences has been properly removed from the site. As a result of this review, the regulatory body may release the facility from regulatory control for nuclear security.

4. AUTHORIZATION OF DESIGN MODIFICATIONS

4.1. As the nuclear facility moves through the different stages in its lifetime, there may be a need to reassess and, when appropriate, to modify the security plan, physical protection system and information security and computer security management system because of changes to the design of the facility, its operating practices or the threat profile. Design and operating practices may change because of new missions, identified deficiencies or operating experience. The threat profile may change as a result of a changing threat environment and a revised design basis threat or the representative threat statement.

4.2. Before making a significant modification or change that affects the nuclear security of the nuclear facility, the operator should seek prior approval from the regulatory body by submitting supporting documents for such a modification or change.

4.3. Computer simulation applications that provide appropriate models of the facility, along with the results of performance tests, drills and exercises, could assist the operator with the evaluation of the effectiveness of the physical protection system.

4.4. The operator should implement processes for configuration management to ensure that the security plan and related procedures are developed, assessed and updated as necessary. The following information should be collected and documented by the operator in the configuration management plan (and in the configuration management procedures, as appropriate) and provided to the regulatory body:

(a) The results of the evaluation of the impacts on facility operations or safety of proposed nuclear security changes before these changes are implemented;
(b) The results of the evaluation of the impacts on nuclear security of proposed operational changes, changes in safety measures or facility modifications before these modifications or changes are implemented.

4.5. Modifications or changes affecting the nuclear security of the nuclear facility may range from minor (e.g. editorial changes to the security plan) to significant (e.g. modifications to the facility perimeter to improve the detection and assessment of nuclear security events) and may involve one or more of the following situations:

(a) Changes to the facility's mission, such as the use of a new type of material at the facility or new activities not addressed in the approved security plan;
(b) Changes to the design basis threat or the representative threat statement;
(c) Changes to regulatory requirements or conditions of the licence or other form of authorization;
(d) Significant changes planned by the operator to the physical protection system;
(e) A significant security event for which the nuclear security strategy defined by the approved security plan was inadequate;
(f) Renewal of the facility's operating licence.

4.6. The State's regulatory framework should define the criteria that are needed by the operator to identify modifications and changes that have an impact on the security plan or on the design of the physical protection system. In addition, the operator should identify whether other documentation that has already been reviewed and approved by the regulatory body could be affected by these modifications and changes, and should obtain reapproval of this documentation by the regulatory body before the modifications and changes are implemented.

4.7. As a result of such modifications and changes, the operator may need to develop and maintain supporting documentation for review by the regulatory body. The operator should use the following questions to identify the documentation to be submitted for review by the regulatory body:

(a) Does the major modification or change at the facility reduce the level of nuclear security below that previously approved by the regulatory body? If yes, then the modification or change should be submitted to the regulatory body for approval before it is implemented at the facility. If there are major changes to the design of the physical protection system, the operator should verify the effectiveness of the physical protection system in the new configuration and should consider if the safety–security interface is properly addressed.
(b) Does the change at the facility result in a change to documentation that has already been approved by the regulatory body? If yes, then the change (including the proposed revisions to the security plan or design of the physical protection system) should be submitted to the regulatory body for approval before it is implemented at the facility. A graded approach to determining and evaluating risk can be applied to define a threshold for involving the regulatory body in the change process. Such a graded approach could be applied as follows:
    (i) A complete regulatory review (similar to the initial authorization process for a new facility) is needed for major changes, as defined by the regulatory body. For such cases, a complete revision of the security plan and review and reapproval by the regulatory body should be conducted.
    (ii) A limited regulatory review may be needed for significant changes. Examples include changes that are limited to specific security functions, specific physical protection system equipment and changes to the security management system.
    (iii) Minor changes (e.g. minor additions to existing equipment, changes in equipment technology without any change to the security function or effectiveness) could be submitted to the regulatory body for

information purposes. These changes might be submitted by electronic mail if allowed by the State's regulatory requirements for information security. Some minor changes may require regulatory review and approval. For example, the regulatory body could be informed by the operator when changes in security equipment need to be reassessed to verify that the replacement components can perform their intended function and are equally effective. To ensure the effective management of safety–security interfaces, the regulatory body should review changes to the security plan that affect safety systems (from both the safety and security perspective).

(c) Does the change at the facility create a non-compliance between the applicable regulations and the approved security plan or design of the physical protection system? If yes, then the operator should decide if the non-compliance can be justified under exceptional circumstances without taking any further action, or if corrective action is needed to resolve the non-compliance. In either case, the regulatory body should be informed of the operator's analysis and decision before the change is implemented. If the operator intends to justify the existing non-compliance without corrective action, then the justification may be submitted as a request for an exemption from the regulatory requirements.

(d) Do alternative measures, not previously reviewed and approved by the regulatory body, have to be implemented to maintain the nuclear security measures at the facility? If yes, then information on these alternative measures should be submitted to the regulatory body for review and approval. This information should include a technical basis demonstrating an equivalent level of protection provided by each measure (e.g. analyses of controls for construction equipment brought on the site that could be used by adversaries).

4.8. The operator should be required to maintain records of changes to the nuclear facility for later inspection by the regulatory body, if needed. The records should cover both physical changes to the facility and programmatic changes, such as revised organizational charts and responsibilities, procedures and training.

4.9. If the State has different regulatory bodies for authorizing nuclear safety and nuclear security activities, close communication and coordination between these bodies is essential to ensure that safety related changes to the nuclear facility are reviewed for possible impacts on the security plan or physical protection system. Such changes could affect the category and amount of nuclear material at the facility, approaches to nuclear material protection, insider threats and mitigation strategies.

4.10. Using nuclear material accounting and control measures at the facility, the operator should continually monitor changes to the categories and amounts of nuclear and other radioactive material at the facility, as required by the applicable regulations for protection against unauthorized removal, and should adjust physical protection measures as necessary. The operator should also perform analyses to determine whether changes in the inventory of nuclear and other radioactive material, or modifications to plant equipment, systems or devices, have the potential to result in unacceptable radiological consequences from sabotage. The results of such analyses should be provided to the regulatory body, if required under applicable regulations.

5. REGULATORY INSPECTION AND ENFORCEMENT

5.1. One of the key functions of the regulatory body is the conduct of inspections of the nuclear security of a nuclear facility, including its physical features, design documentation, programme descriptions and procedures for compliance with applicable regulatory requirements. The principal objective of regulatory inspection and follow-up actions in the area of nuclear security is to provide a high level of assurance that the operator has performed nuclear security related activities as required during the various stages in the lifetime of the nuclear facility. As part of the authorization process, the regulatory body reviews the information submitted by the operator and verifies its accuracy by conducting inspections at the facility before issuing a licence or other form of authorization.

5.2. The regulatory body conducts inspections at nuclear facilities to achieve the following objectives:

(a) To obtain satisfactory evidence that the operator is operating the nuclear facility in compliance with the conditions set out in the licence or authorization document;
(b) To verify compliance with relevant laws, regulations, authorization conditions, codes, guides, specifications and practices;
(c) To check that the operator is implementing an effective management system, has an appropriate nuclear security culture, implements nuclear security measures satisfactorily and has sufficient personnel with the competencies necessary for fulfilling nuclear security responsibilities;
(d) To check that the operator promptly evaluates and takes corrective action to address deficiencies and abnormal conditions.

5.3. If a non-compliance is identified, the regulatory body ensures that corrective actions are implemented to bring about compliance, or that alternative measures are implemented.

5.4. A regulatory inspection programme includes a range of announced and unannounced inspections over the lifetime of a nuclear facility to ensure compliance with regulatory requirements. Reactive inspections may also be necessary from time to time, such as after a nuclear security event at a nuclear facility or a change in the threat environment. Regulatory inspections may be carried out at any time, during or outside normal working hours, and may include all routine and non-routine operational activities undertaken at the nuclear facility at that time (e.g. during reactor shutdown for maintenance and refuelling). The inspection programme should include review, verification and performance testing of the physical protection measures, including technical, procedural and administrative provisions.

5.5. The regulatory body should consider using a graded approach to define the frequency of inspections. The frequency should be based on several factors, such as the category of the material being protected, regulatory requirements for unauthorized removal and sabotage, the design basis threat or the representative threat statement, the history of compliance of the operator, and other sources of information collected and evaluated by the regulatory body.

5.6. The methods of inspection of nuclear security activities may vary in scope and depth during the different stages in the lifetime of the facility and may include the following:

(a) Observations to evaluate the actual condition of structures, systems and components (scheduled at agreed hold points or ongoing), and observations of tests or measurements;
(b) Review of documentation and records as specified in the management system;
(c) Interviews or discussions with facility personnel and security personnel;
(d) Performance testing, as necessary.

5.7. For a more effective inspection programme, the regulatory framework should define the methods for identifying the significance of inspection findings (on a scale of increasing significance) and the expectations for follow-up by both the operator and the regulatory body. The scope of regulatory inspections should include the security plan as well as security related technical areas and authorization conditions covering activities by the operator and contractors.

5.8. The findings of regulatory inspections, corrective actions and areas of improvement are usually documented in inspection reports that are issued by the regulatory body. The inspection reports may also include applicable regulatory requirements, a timeline for the operator to submit additional information or to respond to the report, and submission, if needed, to the relevant organizations.

5.9. The operator should support the inspections by the regulatory body by providing the following:

(a) Access to on-site working facilities, including the provision of workspace for the inspectors that provides for adequate information security;
(b) Transport on the site;
(c) Access to means of communication;
(d) Access to all pertinent information;
(e) Copies of relevant documentation;
(f) Meetings with appropriate facility personnel;
(g) Personal protective equipment (e.g. protective clothing, respirators) to be used by inspectors if needed in the conduct of inspection activities.

BASIC PRINCIPLES AND CONSIDERATIONS FOR INSPECTION ACTIVITIES

5.10. As part of the review and assessment process, the regulatory body reviews the information submitted by the operator and verifies its accuracy through inspections at the facility. These inspections may allow the regulatory body to identify supplemental information and data needed for the review and assessment. Additionally, the regulatory body may be able to improve its practical understanding of the facility's managerial, engineering and operational aspects and foster links with experts in the nuclear facility.

5.11. Paragraphs 5.15–5.27 describe inspection activities that the regulatory body may conduct during each stage in the lifetime of the nuclear facility.

5.12. During inspections, the regulatory body may identify non-compliances with regulatory requirements, with information submitted by the operator and/or with licence conditions, or may identify other issues of concern for nuclear security. In such cases, procedures for subsequent inspections should include verification in a graded manner that the operator has taken all the corrective actions required. If necessary, the regulatory body may initiate enforcement actions and may require the operator to modify, correct or curtail any aspect of a facility's operation,

procedures or practices, as necessary, to ensure that the required level of nuclear security is achieved. The State's legal and regulatory framework should describe in sufficient detail how the regulatory enforcement function is accomplished. The regulatory body should be able to determine the following:

(a) The significance of any deficiencies relating to nuclear security and the complexity of the corrective actions or compensatory measures that are needed;
(b) The potential implications of the identified violation (e.g. security violations might also affect nuclear safety, in which case enforcement actions may need to be coordinated among the responsible regulatory bodies);
(c) Whether the security violation represents the recurrence of a situation that should already have been corrected;
(d) Whether there has been a deliberate or wilful violation of regulatory requirements for nuclear safety or nuclear security, or of licence conditions;
(e) The person who identified and reported the deficiency or the violation;
(f) The past performance of the operator and the trend in the performance;
(g) The need for consistency in the treatment of operators.

5.13. In accordance with the legal provisions, the regulatory body should prescribe enforcement actions with specific conditions for non-compliance, and these actions should be commensurate with the significance of the non-compliance. There are different types of enforcement actions, ranging from written warnings to penalties (including financial, civil and criminal penalties) and, ultimately, to the withdrawal of a licence or other form of authorization. However, caution should be exercised in considering the imposition of penalties. In many cases, it may be possible to resolve the non-compliance through discussion with the operator, but if discussion is inappropriate or has been unsuccessful, it might be necessary to invoke a formal measure. In all cases, the regulatory body should expect the operator to remedy the non-compliance, perform a thorough investigation in accordance with an agreed schedule and take all necessary measures to prevent recurrence. The regulatory body should ensure that the operator has effectively implemented any corrective actions or compensatory measures.

5.14. The regulatory body should have a system to audit, review and monitor all aspects of its inspection activities and enforcement actions to ensure that they are being carried out in a suitable and effective manner. The system should have the following aspects:

(a) Internal guidance for conducting inspections, including documented inspection methods.

(b) Processes for determining and allocating resources for inspections.
(c) Procedures relating to inspection activities, such as:
    (i) Planning inspections and dealing with outstanding issues;
    (ii) Coordinating the timing of the conduct of inspection activities with the regulatory review and assessment process;
    (iii) Involving consultants in inspection activities;
    (iv) Taking enforcement actions and evaluating their effectiveness;
    (v) Record keeping and documentation.

INSPECTION ACTIVITIES DURING THE SITING STAGE

5.15. As part of the inspection activities during site evaluation, the regulatory body mainly examines procedures, records and documentation. Site inspections might not be typical during the siting stage. However, during this stage, the regulatory body might verify that the operator is undertaking siting activities in full conformity with existing regulatory requirements and the design basis threat, and that on-site preparation does not proceed beyond that permitted by any authorization in force. The regulatory body should consider undertaking the following activities:

(a) Ensuring opportunities to witness activities relating to the implementation of the site evaluation (e.g. surveys, sampling, tests) and verifying that on-site work does not proceed beyond that permitted;
(b) Verifying that the characteristics of the proposed site match those provided in submissions, to the extent practicable;
(c) Conducting interviews and discussions with individuals responsible for and participating in the implementation of the site survey for site evaluation following site selection;
(d) Examining the reports, procedures, quality processes, records and other documentation relating to the site survey.

INSPECTION ACTIVITIES DURING THE DESIGN STAGE

5.16. During the design stage, the preliminary security plan, which also includes the design of the physical protection system, is usually submitted to the regulatory body. The regulatory body performs the review and assessment of the operator's submissions. Depending on the State's legislative and regulatory framework,

inspection activities might not be required during this stage. However, the regulatory body may consider undertaking the following activities:

(a) Visiting the site to verify site specific parameters used in the preliminary security plan.
(b) Checking that the State's requirements for information security — including physical protection and computer security measures — are met.
(c) Discussing security concerns with facility personnel involved in establishing the design of the physical protection system. Such concerns may include the basic parameters and key assumptions that influenced the security plan and the design of the physical protection system.
(d) Reviewing the operator's analyses that were used to determine the nuclear security measures against unauthorized removal or sabotage included in the design. The determination may include an analysis of the numbers and types of security areas (i.e. limited access areas, protected areas, and inner and vital areas), and of the material balance areas for nuclear material accounting and control.
(e) Reviewing the bases for:
    (i) The categorization of nuclear material;
    (ii) The development of the information security programme;
    (iii) The development of the security management system.
(f) Discussing how the operator has coordinated nuclear security design measures with other areas (e.g. safety, safeguards, operations) to compare relevant regulatory requirements, identify synergies and resolve potential conflicts.
(g) Reviewing the operator's evaluation of technologies and components such as barriers, sensors and assessment systems to determine whether the operator has implemented effective nuclear security strategies and designs that meet regulatory requirements. In addition, the regulatory body may review:
    (i) Engineering and design packages used by the operator;
    (ii) The operator's arrangements for ensuring that the final facility design meets regulatory requirements for nuclear security;
    (iii) The operator's arrangements for ensuring that changes to the design of the physical protection system incorporate the concept of configuration management.
(h) Requesting tests or the qualification of experimental installations of physical protection measures before the start of the construction to check the performance of those measures against threats.

INSPECTION ACTIVITIES DURING THE CONSTRUCTION STAGE

5.17. The inspection programme may include provisions for hold points and for general site surveillance during construction and equipment installation. Operators should submit quality assurance plans for facility construction activities relevant to nuclear security. Specific activities in the quality assurance plans can then serve as hold points for regulatory inspections.

5.18. Facility construction activities relevant to nuclear security include the construction of facility structures such as walls and containment that also provide protection against a range of attacks by adversaries, and the construction of openings and communication lines for the physical protection system.

5.19. During preparations on the site for the construction of the facility, the regulatory body should confirm that the site characteristics remain consistent with the description presented by the operator in the application for authorization and supporting documentation subsequently submitted.

5.20. During the construction stage, the regulatory body may conduct inspections of the security measures, including the following inspection activities:

(a) Observing the actual layout of the overall physical protection system and individual elements of the system.
(b) Monitoring the security personnel who are implementing the security plan.
(c) Interviewing, if needed, the security personnel who are implementing the security plan during the construction stage.
(d) Reviewing the following:
    (i) The implementation of the management system by the construction organization and any subcontractors engaged in the construction and installation of nuclear security features, such as structures, systems and components that make up the physical protection system;
    (ii) The implementation of the configuration management programme, including how changes to the approved facility design are developed and assessed for adequacy from both a nuclear safety and a nuclear security perspective;
    (iii) The training and qualification programme and procedures for the operator's personnel who are responsible for implementing the physical protection system;
    (iv) Reports on construction deficiencies and corrective actions;
    (v) The reporting channel of the facility's security organization.

(e) Witnessing or conducting tests to confirm compliance with agreed facility construction standards.
(f) Checking information security procedures that will be implemented during the installation and commissioning of related systems.

INSPECTION ACTIVITIES DURING THE COMMISSIONING STAGE

5.21. During the commissioning stage, the inspectors verify the proper functioning of the structures, systems and components that make up the physical protection system by witnessing the operator's tests and exercises. The inspection programme for the commissioning stage may also include provisions for mandatory hold point inspections, for witnessing important tests and for reviewing inspection records.

5.22. The nuclear material to be used in the nuclear facility usually arrives on the site at the end of the commissioning stage. However, there are instances when the material may already be on the site before commissioning activities have been finished completely. This can occur when the storage of the nuclear material does not need the same level of protection as it does when it is in use (e.g. in nuclear power plants). Before the material arrives on the site, the regulatory body should verify that adequate physical protection measures have been commissioned for service. If this is the case, then a hold point for security should be included in the nuclear security commissioning programme.

5.23. During the commissioning stage, the regulatory body should conduct the following inspection activities:

(a) Verify that the operation of the nuclear security systems and components complies with the approved security plan to ensure that they reflect the current conditions and configurations at the site.
(b) Select specific physical protection system or critical components as candidates for performance testing.
(c) Verify that any operational issues with nuclear safety and nuclear security considerations have been identified and addressed satisfactorily. For example, this may include confirming that communications occur between the central alarm station and the facility's main control room during events, if necessary.
(d) Review physical protection measures for the on-site storage of nuclear material to confirm compliance with regulatory requirements and the applicant's or operator's security plan.

(e) Inspect the following facility features and commissioning activities as they relate to the security plan and physical protection system:
    (i) Locations and boundaries of nuclear security areas;
    (ii) Locations of access points to different nuclear security areas;
    (iii) The general quality and condition of physical barriers;
    (iv) Locations and types of nuclear security equipment installed;
    (v) Entry control procedures and methods employed at access points (e.g. special purpose detection equipment and procedures, badge checks, badge exchanges, card readers, biometrics);
    (vi) Locations of the alarm stations;
    (vii) Types of storage area (e.g. vaults, vault-type rooms, rooms equipped with alarms, safes, locked filing cabinets, locked rooms);
    (viii) Locations of and security arrangements for emergency exits;
    (ix) Types and approximate quantities of nuclear material in use or being processed and important equipment to be protected in accordance with the regulatory requirements for vital areas;
    (x) Lighting arrangements;
    (xi) Communication means;
    (xii) Maintenance procedures;
    (xiii) Training programmes for nuclear security personnel;
    (xiv) Evaluation of the effectiveness of the physical protection system;
    (xv) Guard and response force performance, including interfaces between on-site and off-site response personnel such as local law enforcement agencies tasked with conducting and supporting the response.
(f) Conduct interviews and discussions with facility security personnel to achieve the following:
    (i) To confirm the working knowledge of the nuclear security personnel responsible for the operation of the facility's physical protection system;
    (ii) To review contingency planning and response;
    (iii) To discuss with nuclear security personnel how they evaluate and address operational issues that might affect both nuclear safety and nuclear security.
(g) Review the following:
    (i) The implementation of the management system by the operator and any subcontractors engaged in the commissioning of nuclear security features, such as the structures, systems and components that make up the physical protection system or are important to nuclear security (e.g. safety systems);
    (ii) The implementation of security procedures;

(iii) The documentation of the physical protection system, especially of those elements of the system that provide protection for the storage of nuclear material;
(iv) The status of the management system, including quality assurance, organization and staffing, training and qualification, emergency preparedness, information security and performance testing programmes;
(v) Arrangements for maintaining logs and records.

(h) Conduct performance testing activities, including the following:
(i) Observing performance testing of the structures, systems and components of the physical protection system and information security processes that should be operational before the arrival on the site of nuclear material;
(ii) Observing full functionality tests of the overall physical protection system and, if applicable, force-on-force exercises;
(iii) Identifying anomalies or deficiencies that necessitate further investigation after performance testing of the facility's nuclear security systems and ensuring that the operator identifies any corrective actions that might be needed, including retesting.

INSPECTION ACTIVITIES DURING THE OPERATION STAGE

5.24. The regulatory body completes most of the inspection activities to verify the proper functioning of the structures, systems and components that make up the physical protection system during the commissioning stage, before issuing the operating licence. However, the regulatory body continues to implement the inspection programme during the operation stage to achieve the following objectives:

(a) To verify systematically the operator's continued compliance with regulatory requirements, approved plans and conditions set out in the operating licence;
(b) To verify that the general security objectives have been met;
(c) To detect potential problems with nuclear security measures.

5.25. The inspections during the operation stage could be similar to the inspections conducted during the commissioning stage. During the operation stage, the regulatory body may undertake the following inspection activities:

(a) Verify that the operation of the nuclear security systems and components complies with regulatory requirements, approved plans and conditions

set out in the operating licence to ensure that they continue to reflect the current conditions and configurations at the site and the current situational awareness regarding the threat environment.

(b) Observe the process of assessment and continuous development of the nuclear security system at the facility.

(c) Verify that interfaces between facility operations, nuclear safety and nuclear security have been satisfactorily identified and addressed.

(d) Review physical protection measures for the on-site storage of nuclear material to confirm continued compliance with regulatory requirements and operator commitments to inspection findings.

(e) Inspect those facility features and activities that relate to the implementation of the security plan.

(f) Inspect the implementation and maintenance of the information security management system.

(g) Conduct interviews and discussions with facility security personnel to achieve the following:
    (i) To confirm the continued working knowledge of the nuclear security personnel responsible for the operation of the facility's physical protection system;
    (ii) To review contingency planning and response by checking that up to date plans are maintained and assuring the readiness of response capabilities to address evolving threats;
    (iii) To confirm that any nuclear safety and nuclear security interface issue continues to be properly evaluated and addressed.

(h) Review the following:
    (i) The implementation of the management system;
    (ii) The implementation of security procedures;
    (iii) The maintenance of the physical protection system, including those elements that provide protection for the storage of nuclear material;
    (iv) The status of the management system, including quality assurance, organization and staffing, training and qualification, emergency preparedness, information security and performance testing programmes;
    (v) Arrangements for maintaining logs and records.

(i) Conduct performance testing activities, including the following:
    (i) Verifying that performance testing of the physical protection system and information security measures is conducted periodically and in accordance with regulatory requirements, and that the operator identifies and resolves anomalies or deficiencies;

(ii) Observing performance testing of the structures, systems and components of the physical protection system, including measures for information security.

INSPECTION ACTIVITIES DURING THE CESSATION OF OPERATION STAGE

5.26. The inspections conducted during the cessation of operation stage should be similar to the inspections conducted during the operation stage. However, any security related inspections conducted during this stage should focus on changes by the operator to the facility's configuration and business practices. The regulatory body should note any changes that could affect the operator's ability to successfully protect the facility (and its nuclear material) from the unauthorized removal of nuclear material or sabotage.

INSPECTION ACTIVITIES DURING THE DECOMMISSIONING STAGE

5.27. During the decommissioning stage, the regulatory body may conduct inspection activities to achieve the following objectives:

(a) To verify the operation of nuclear security systems and components in accordance with regulatory requirements, approved plans and conditions set out in the authorization for decommissioning to protect nuclear or other radioactive material that is on the site or in the facility during the decommissioning process.
(b) To confirm that no nuclear or other radioactive material remains on the site before the release of the site from regulatory control.
(c) To conduct interviews and discussions with facility security personnel to achieve the following:
    (i) To confirm that personnel involved with the decommissioning of the facility are knowledgeable of the revised security plan;
    (ii) To check that the facility's emergency preparedness and response capabilities continue to be maintained for nuclear material and other radioactive material that could remain on the site or in the facility during the decommissioning process;
    (iii) To verify that any decommissioning issues with both nuclear safety and nuclear security considerations continue to be identified and resolved.

(d) To review documents and records to achieve the following:
    (i) To confirm that the security plan has been revised for decommissioning;
    (ii) To verify statements (with supporting documentation) from the operator that the nuclear facility has been decommissioned and the site is ready for release from regulatory control.
(e) To observe performance tests, if needed as per regulatory requirements.

REFERENCES

[1] INTERNATIONAL ATOMIC ENERGY AGENCY, Objective and Essential Elements of a State's Nuclear Security Regime, IAEA Nuclear Security Series No. 20, IAEA, Vienna (2013), https://doi.org/10.61092/iaea.ajrj-ymul

[2] 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), https://doi.org/10.61092/iaea.ko2c-dc4q

[3] INTERNATIONAL ATOMIC ENERGY AGENCY, Physical Protection of Nuclear Material and Nuclear Facilities (Implementation of INFCIRC/225/Revision 5), IAEA Nuclear Security Series No. 27-G, IAEA, Vienna (2018).

[4] INTERNATIONAL ATOMIC ENERGY AGENCY, Developing Regulations and Associated Administrative Measures for Nuclear Security, IAEA Nuclear Security Series No. 29-G, IAEA, Vienna (2018).

[5] INTERNATIONAL ATOMIC ENERGY AGENCY, Establishing the Nuclear Security Infrastructure for a Nuclear Power Programme, IAEA Nuclear Security Series No. 19, IAEA, Vienna (2013).

[6] INTERNATIONAL ATOMIC ENERGY AGENCY, Security During the Lifetime of a Nuclear Facility, IAEA Nuclear Security Series No. 35-G, IAEA, Vienna (2019).

[7] INTERNATIONAL ATOMIC ENERGY AGENCY, Use of Nuclear Material Accounting and Control for Nuclear Security Purposes at Facilities, IAEA Nuclear Security Series No. 25-G, IAEA, Vienna (2015).

[8] INTERNATIONAL ATOMIC ENERGY AGENCY, Security of Nuclear Material in Transport, IAEA Nuclear Security Series No. 26-G, IAEA, Vienna (2015).

[9] INTERNATIONAL ATOMIC ENERGY AGENCY, Computer Security for Nuclear Security, IAEA Nuclear Security Series No. 42-G, IAEA, Vienna (2021).

[10] INTERNATIONAL ATOMIC ENERGY AGENCY, Computer Security Techniques for Nuclear Facilities, IAEA Nuclear Security Series No. 17-T (Rev. 1), IAEA, Vienna (2021).

[11] INTERNATIONAL ATOMIC ENERGY AGENCY, Computer Security of Instrumentation and Control Systems at Nuclear Facilities, IAEA Nuclear Security Series No. 33-T, IAEA, Vienna (2018).
[12] INTERNATIONAL ATOMIC ENERGY AGENCY, Licensing Process for Nuclear Installations, IAEA Safety Standards Series No. SSG-12, IAEA, Vienna (2010). (A revision of this publication is in preparation.)
[13] INTERNATIONAL ATOMIC ENERGY AGENCY, Security of Nuclear Information, IAEA Nuclear Security Series No. 23-G, IAEA, Vienna (2015). (A revision of this publication is in preparation.)
[14] INTERNATIONAL ATOMIC ENERGY AGENCY, Identification and Categorization of Sabotage Targets, and Identification of Vital Areas at Nuclear Facilities, IAEA Nuclear Security Series No. 48-T, IAEA, Vienna (2024), https://doi.org/10.61092/iaea.74e6-e2yc
[15] INTERNATIONAL ATOMIC ENERGY AGENCY, Security of Radioactive Material in Use and Storage and of Associated Facilities, IAEA Nuclear Security Series No. 11-G (Rev. 1), IAEA, Vienna (2019).

IAEA
International Atomic Energy Agency

No. 27

ORDERING LOCALLY

IAEA priced publications may be purchased from our lead distributor or from major local booksellers.

Orders for unpriced publications should be made directly to the IAEA.

Orders for priced publications

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

Eurospan
1 Bedford Row
London WC1R 4BU
United Kingdom

Trade orders and enquiries:
Tel: +44 (0)1235 465576
Email: trade.orders@marston.co.uk

Individual orders:
Tel: +44 (0)1235 465577
Email: direct.orders@marston.co.uk
www.eurospanbookstore.com/iaea

For further information:
Tel. +44 (0) 207 240 0856
Email: info@eurospan.co.uk
www.eurospan.co.uk

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

Publishing Section
International Atomic Energy Agency
Vienna International Centre
PO Box 100
1400 Vienna, Austria
Telephone: +43 1 2600 22529 or 22530
Email: sales.publications@iaea.org
www.iaea.org/publications

The development of a nuclear facility needs careful planning, adequate preparation and substantial investment. This includes the establishment of a legislative and regulatory framework with provisions to assess the adequacy of nuclear security and authorize activities at nuclear facilities at key stages in their lifetimes. This publication provides guidance to regulatory bodies responsible for the nuclear security of nuclear facilities on the authorization process for the operation of such facilities and for related activities. The guidance addresses nuclear security aspects that may require regulatory authorization during different stages in the lifetime of a nuclear facility, identifies the elements included in applications for authorization by the applicant or operator in each of these stages, and provides guidance to the regulatory body on the review and assessment of these applications and on related inspections as a basis for authorization decisions.

International Atomic Energy Agency
Vienna, 2024
www.iaea.org