IAEA
International Atomic Energy Agency

International Physical Protection Advisory Service (IPPAS) Guidelines

Vienna, November 2014

Services Series 29

IAEA NUCLEAR SECURITY SERIES AND RELATED PUBLICATIONS

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.

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.

RELATED PUBLICATIONS

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

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

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

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

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

INTERNATIONAL PHYSICAL PROTECTION ADVISORY SERVICE (IPPAS) GUIDELINES

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

AFGHANISTAN
ALBANIA
ALGERIA
ANGOLA
ARGENTINA
ARMENIA
AUSTRALIA
AUSTRIA
AZERBAIJAN
BAHAMAS
BAHRAIN
BANGLADESH
BELARUS
BELGIUM
BELIZE
BENIN
BOLIVIA
BOSNIA AND HERZEGOVINA
BOTSWANA
BRAZIL
BRUNEI DARUSSALAM
BULGARIA
BURKINA FASO
BURUNDI
CAMBODIA
CAMEROON
CANADA
CENTRAL AFRICAN REPUBLIC
CHAD
CHILE
CHINA
COLOMBIA
CONGO
COSTA RICA
CÔTE D'IVOIRE
CROATIA
CUBA
CYPRUS
CZECH REPUBLIC
DEMOCRATIC REPUBLIC OF THE CONGO
DENMARK
DOMINICA
DOMINICAN REPUBLIC
ECUADOR
EGYPT
EL SALVADOR
ERITREA
ESTONIA
ETHIOPIA
FIJI
FINLAND
FRANCE
GABON
GEORGIA
GERMANY
GHANA
GREECE
GUATEMALA
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, ISLAMIC REPUBLIC OF
MAURITIUS
MEXICO
MONACO
MONGOLIA
MONTENEGRO
MOROCCO
MOZAMBIQUE
MYANMAR
NAMIBIA
NEPAL
NETHERLANDS
NEW ZEALAND
NICARAGUA
NIGER
NIGERIA
NORWAY
OMAN
PAKISTAN
PALAU
PANAMA
PAPUA NEW GUINEA
PARAGUAY
PERU
PHILIPPINES
POLAND
PORTUGAL
QATAR
REPUBLIC OF MOLDOVA
ROMANIA
RUSSIAN FEDERATION
RWANDA
SAN MARINO
SAUDI ARABIA
SENEGAL
SERBIA
SEYCHELLES
SIERRA LEONE
SINGAPORE
SLOVAKIA
SLOVENIA
SOUTH AFRICA
SPAIN
SRI LANKA
SUDAN
SWAZILAND
SWEDEN
SWITZERLAND
SYRIAN ARAB REPUBLIC
TAJIKISTAN
THAILAND
THE FORMER YUGOSLAV REPUBLIC OF MACEDONIA
TOGO
TRINIDAD AND TOBAGO
TUNISIA
TURKEY
UGANDA
UKRAINE
UNITED ARAB EMIRATES
UNITED KINGDOM OF GREAT BRITAIN AND NORTHERN IRELAND
UNITED REPUBLIC OF TANZANIA
UNITED STATES OF AMERICA
URUGUAY
UZBEKISTAN
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 SERVICES SERIES No. 29

INTERNATIONAL PHYSICAL PROTECTION ADVISORY SERVICE (IPPAS) GUIDELINES

INTERNATIONAL ATOMIC ENERGY AGENCY
VIENNA, 2014

COPYRIGHT NOTICE

For further information on this publication, please contact:

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

INTERNATIONAL PHYSICAL PROTECTION ADVISORY SERVICE (IPPAS) GUIDELINES
IAEA, VIENNA, 2014
IAEA-SVS-29
ISSN 1816–9309

Printed by the IAEA in Austria
November 2014

FOREWORD

The International Physical Protection Advisory Service (IPPAS) was established by the IAEA in 1995 and is a fundamental part of the IAEA's efforts to assist States, upon request, to establish and maintain an effective national nuclear security regime to protect against the unauthorized removal of nuclear and other radioactive material, and against the sabotage of nuclear and other associated facilities, as well as material during transport, while recognizing that the ultimate responsibility for physical protection lies with the State.

IPPAS provides peer review on implementing relevant international instruments, in particular the Convention on the Physical Protection of Nuclear Material (CPPNM), together with the 2005 Amendment, and on implementing the IAEA Nuclear Security Series of guidance publications, in particular Fundamentals and Recommendations.

IPPAS missions compare (insofar as this is possible) the procedures and practices employed by a State with the obligations specified under the CPPNM and the 2005 Amendment, as well as with the existing international consensus guidelines provided in relevant IAEA Nuclear Security Series publications.

Since 1996, 63 IPPAS missions have been conducted in 40 countries, including 15 follow-up missions, as well as the recent mission to the IAEA Office of Safeguards Analytical Services laboratories, in Seibersdorf. More than 140 experts from 34 Member States have participated in the conduct of IPPAS missions as IPPAS team members or team leaders.

The updated IPPAS guidelines reflect a modular approach to make them more flexible and responsive to the needs of States. The modular approach is an innovation of great value, ensuring the degree of flexibility required to fit individual national contexts, practices and objectives as expressed by the requesting States. In particular, it also offers States the opportunity to expand the scope of a requested IPPAS mission to embrace its nuclear security regime for the protection of other radioactive material (in particular radioactive sources) and associated facilities, although it was originally designed to address only nuclear material and nuclear facilities. This publication supersedes the 1999 edition of the IPPAS guidelines published as IAEA Services Series No. 3.

The IPPAS guidelines provide overall guidance for the experts to ensure the consistency and comprehensiveness of the mission and have been prepared by the IAEA to complement the expertise of the IPPAS team members. This publication also provides suitable guidance to the host State in preparing for and receiving such missions.

IPPAS missions are performance oriented in that they accept different approaches to the implementation of a national nuclear security regime. Recommendations are made on items which could directly affect the nuclear security regime, whereas suggestions made might only indirectly contribute to improving the nuclear security regime. Commendable good practices identified may be communicated to other States for long term improvement.

These guidelines were compiled by experts in the Division of Nuclear Security with the assistance of experts from the Member States.

EDITORIAL NOTE

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

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

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

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

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

CONTENTS

1. GENERAL INFORMATION

1.1. INTRODUCTION

The International Physical Protection Advisory Service (IPPAS) programme, initiated in 1995, is a fundamental part of the IAEA's efforts to assist Member States to establish and maintain an effective nuclear security regime to protect against the unauthorized removal of nuclear material and the sabotage of nuclear facilities and material.

According to the request for developing guidance and advisory services (GC(47)/17 dated 20 August 2003), the IAEA has decided to expand the scope of the IPPAS programme to include the security of radioactive material, associated facilities and transport.

The IPPAS programme is offered to assist Member States, upon request, with an assessment of their State physical protection regime. This assessment includes a national level review of the legal and regulatory framework, and implementation measures and procedures in place to execute this framework at facilities and during transport. Detailed guidance on the review of the national physical protection regime, a nuclear facility's physical protection system, security of nuclear material during transport, security of radioactive material and computer security is provided in modular form in this publication. The module on security of radioactive material, associated facilities and associated activities is a stand-alone module, encompassing the national regime, the security of radioactive material and associated facilities and security during transport.

All terms used in these guidelines are identical to the definitions contained in the relevant IAEA Nuclear Security Series publications (hereafter abbreviated to IAEA NSS). For the purpose of this publication, the word 'materials' will be used when 'nuclear material' or 'radioactive material' can be used interchangeably. In addition, the term 'competent authority', as defined in the 2005 Amendment of the Convention on the Physical Protection of Nuclear Material (CPPNM), will also cover the term of 'regulatory authority' as defined in the Code of Conduct on the Safety and Security of Radioactive Sources.

The desired outcome is for an IPPAS expert team, made up of nuclear security and other relevant specialists selected from Member States, to provide advice on implementing international instruments and guidance on the protection of nuclear and other radioactive material and associated facilities. The IPPAS team can and should be judgmental in evaluating the State nuclear security regime with regard to these instruments, guidelines and practices; it can also provide recommendations and suggestions for improvement and acknowledge good practices. For this evaluation, the IPPAS team may consider the arrangements of the competent authority at its headquarters and should visit one or several facilities and/or see materials in transport in order to observe the implementation of nuclear security requirements as defined in the national nuclear security regime.

1.2. PURPOSE

These guidelines have been prepared to provide a basic structure and a common reference for IPPAS missions. As such, they are addressed principally to the team members of IPPAS missions, although, they

also provide guidance to a Member State that may consider hosting an IPPAS mission, or information to a host country on preparing for (including a self-assessment) and receiving a mission.

The guidelines are intended to assist an IPPAS team in formulating its review in light of its own experience. It is not all-inclusive and should not limit the experts' review, but rather be considered as elaborating on the requirements for an adequate review.

An IPPAS review is based on the requirements set out in international instruments and in IAEA recommendations and guidance. The IPPAS national review module is the recommended starting point for those host countries wishing to have their nuclear security regime reviewed against international instruments and guidance.

For IPPAS missions, the main reference sources are:

- *The Convention on the Physical Protection of Nuclear Material* (CPPNM, INFCIRC/274) and its *Amendment* (GOV/INF/2005/10-GC(49)/INF/6)
- *The Physical Protection Objectives and Fundamental Principles* (IAEA-GOV/2001/41)
- *Code of Conduct on the Safety and Security of Radioactive Sources* (IAEA, 2004)
- *IAEA NSS No. 20, Objective* and *Essential Elements of a State's Nuclear Security Regime*
- *IAEA NSS No. 13, Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities* (INFCIRC/225/Revision 5)
- *IAEA NSS No. 14, Nuclear Security Recommendations on Radioactive Material and Associated Facilities*

Other relevant documents include:

- *IAEA NSS No. 15, Nuclear Security Recommendations on Nuclear and Other Radioactive Material out of Regulatory Control*
- *IAEA NNS No. 4, Engineering Safety Aspects of the Protection of Nuclear Power Plants against Sabotage*
- *IAEA NSS No. 7, Nuclear Security Culture*
- *IAEA NSS No. 8, Preventive and Protective Measures against Insider Threats*
- *IAEA NSS No. 10, Development, Use and Maintenance of the Design Basis Threat*
- *IAEA NSS No. 9, Security in the Transport of Radioactive Material*
- *IAEA NSS No. 11, Security of Radioactive Sources*
- *IAEA NSS No. 16, Identification of Vital Areas at Nuclear Facilities*
- *IAEA NSS No. 17, Computer Security at Nuclear Facilities*
- *IAEA-TECDOC-1276, Handbook on the Physical Protection of Nuclear Materials and Facilities*
- *IAEA Safety Standards Series No. RS-G-1.9, Categorization of Radioactive Sources*
- *Guidance on the Import and Export of Radioactive Sources*
- *Handbook on Nuclear Law, Vols 1 and 2*

1.3. OBJECTIVES

The key objectives of the IPPAS programme are to provide advice to:

- The national competent authorities (such as relevant regulatory bodies, law enforcement agencies, customs and border agencies and coast guards, intelligence agencies, response organizations, judicial entities) and operators, carriers and other regulated entities based on an objective assessment of the status of the nuclear security regime through an evaluation of the implementation of international instruments, IAEA guidance and taking account of international good practices;
- Operators and shippers and/or carriers on their physical protection systems and various methods by which international recommendations and good practices can be satisfied;
- Key staff of the national competent authorities, operators and shippers and/or carriers with an opportunity to discuss their practices with the team of international experts who have experience in the field.

Additionally, the IPPAS team promotes the identification, in the course of the mission, of good practices that could be communicated to other Member States for long term improvement. The nuclear security specialists who participate on the IPPAS teams also have opportunities to broaden their experience and knowledge in their own field.

IPPAS is intended to be a peer review of the State nuclear security regime conducted by a team of international nuclear security and other relevant experts who will also use their extensive experience and international guidance to suggest improvements to that system. Judgments are made on the basis of the combined expertise of the international team.

The mission is, therefore, not a regulatory inspection or an audit against set codes and standards. Rather, it is an assessment of the existing practices of a country, in the light of relevant international instruments and IAEA nuclear security publications, and an exchange of experience and accepted international practices aimed at strengthening the security organization and the procedures and practices being followed.

The IPPAS team reviews the *processes* for evaluating effectiveness of a facility or transport physical protection system and, where necessary, makes recommendations and/or suggestions to improve these processes. An IPPAS team may not have either the time or access to the necessary sensitive information (e.g. design basis threat (DBT), barrier delay/response times) to allow it to assess the effectiveness of a facility or transport physical protection system.

These guidelines do not yet include a dedicated module to provide advice to States on their plans to introduce nuclear power for the first time. However, existing modules could be used to provide advice on the development of an appropriate nuclear security regime.

1.4. PROTOCOL AND CONFIDENTIALITY

An IPPAS mission will be initiated only after the IAEA has been approached formally by an interested State at the appropriate governmental level. The scope of each mission will be as agreed between the host country and the IAEA.

The mission is performed by a team of nuclear security and other relevant experts selected by the IAEA in consultation with the host country. Personal data concerning these experts will be submitted to the host country in advance of the mission for formal confirmation before official team member invitations are issued. All team members are treated at the same level of trustworthiness during the mission.

The provision of sensitive information to the IPPAS team is at the discretion of the host government. However, the release of appropriate sensitive information assists the IPPAS team in conducting a more thorough evaluation. IPPAS team members are required to protect all information obtained during the course of the mission and to sign the IAEA form entitled Confidentiality Undertaking for Non-Staff Members. In addition, IPPAS team members may be asked by the host country to sign a declaration of confidentiality.

Team members, when producing technical notes or draft sections of the report must take adequate precautions, as defined by the host country according to its national regulation for protection of sensitive information, to ensure the security of such information. Sensitive information generated or received by the IPPAS team, including electronic data, will be destroyed, deleted or returned to the host organization at the end of the mission.

The IAEA provides one copy of the mission report to the host country and retains one copy of the mission report to be used for any future cooperative activities with the host country. IPPAS mission reports are classified by the IAEA as highly confidential and marked accordingly. IPPAS mission reports are handled by IAEA staff members on a strict 'need-to-know' basis, in accordance with IAEA established information security procedures and responsibilities.

The IAEA will not distribute the report (or parts thereof) to any third parties without the express permission of the host government.

The implementation of recommendations and suggestions presented by the IPPAS mission is strongly encouraged, but the decision to do so is at the discretion of the relevant authorities in the host country.

1.5. SCOPE AND STRUCTURE

The intent of the IAEA's Division of Nuclear Security is that this advisory service be useful to and serve the needs of all Member States with nuclear programmes. Thus, the advice rendered must address the physical protection regime and physical protection systems and measures for a wide range of nuclear programmes that include a variety of nuclear and other radioactive material, including radioactive sources, and different types of nuclear and radioactive material facility, including power and research reactors and nuclear fuel cycle facilities. Many Member States have a subset of these materials and facilities while a few have all types. Thus, the IPPAS programme was designed for flexibility and specificity in the conduct of IPPAS missions for a Member State and its nuclear programme. To achieve this objective, the IPPAS programme and missions are based on a modular approach; the current set of five modules is:

(i) National review of nuclear security regime for nuclear material and nuclear facilities;
(ii) Nuclear facility review;
(iii) Transport review;
(iv) Security of radioactive material and associated facilities and associated activities;
(v) Information and computer security review.

Consistent with this modular approach for the IPPAS programme, these IPPAS Guidelines are organized in a similar manner. The structure of this publication is:

- General information
- IPPAS process
- Module 1: National review of nuclear security regime for nuclear material and nuclear facilities
- Module 2: Nuclear facility review
- Module 3: Transport review
- Module 4: Security of radioactive material and associate facilities and associated activities
- Module 5: Information and computer security review

It should be noted that Module 4 is a stand-alone module that includes reviews of the nuclear security regime, facilities and transport for those Member States that only have radioactive material, facilities, and activities (no nuclear material). Module 5 on cyber security is a new module that addresses an increasingly important topic that was incorporated into INFCIRC/225 for the first time in Revision 5 (IAEA NSS No. 13).

The national review of the nuclear security regime is the natural first review topic for any Member State. Sometimes, multiple missions are requested to address different parts of a Member State's nuclear programme. On the basis of its unique nuclear programme, each Member State may request an IPPAS mission that addresses one or more subject areas. As examples:

- A State with a nuclear programme consisting of radioactive sources for use in areas such as medicine, mining and agriculture may be interested in requesting an IPPAS mission based on Modules 4 and 5.
- A State that is embarking on the development of a nuclear programme for nuclear energy may be interested in requesting an IPPAS mission based on Module 1.
- A State with an existing nuclear programme that includes nuclear research reactors, nuclear power reactors and/or nuclear fuel cycle facilities may be interested in embarking on an IPPAS mission(s) based on all five modules.

1.6. IPPAS PROCESS

1.6.1. Overview

The IPPAS mission process proper — commencing with a formal request leading to the formation of an IPPAS team, and continuing with the conduct of the mission, submission of draft final report and completion of the final report — usually takes nine to twelve months.

Figure 1 summarizes the IPPAS process. Details on each phase are described in the paragraphs that follow.

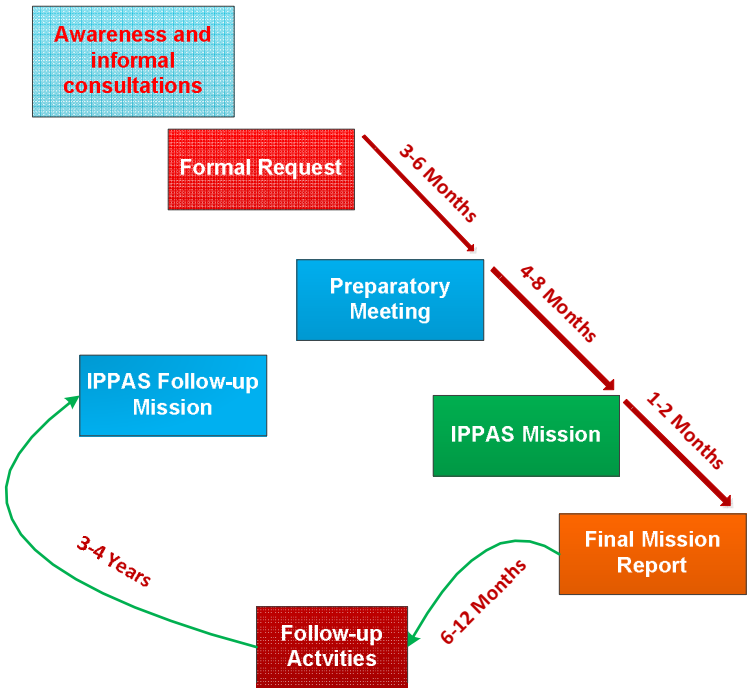

FIG. 1. Flowchart of IPPAS process.

An interested State can request a meeting with an IAEA representative to discuss the IPPAS programme with all the relevant State authorities and, as appropriate, other stakeholders that might participate in such a mission. An IPPAS workshop can be also conducted, on request, to provide detailed information on the issues related to IPPAS.

If the State decides to proceed, the appropriate State official makes a formal request for an IPPAS mission (through or copied to its Permanent Mission) to the IAEA's Division of Nuclear Security. The host country should designate a point of contact (name/organization) responsible for further communication with the IAEA on planning the mission and making practical arrangements. In acknowledgement of, and response to, the formal request, the IAEA will designate its point of contact: the technical officer.

1.6.2. Formal request

The following is an example of a formal request for an IPPAS mission from an interested State to the IAEA to be submitted to the IAEA's Division of Nuclear Security (through or copied to the State's Permanent Mission).

DRAFT LETTER

Ms/Mr ……., Director

Division of Nuclear Security

Department of Nuclear Safety and Security

International Atomic Energy Agency

P.O. Box 100

1400 Vienna, Austria

Dear Ms/Mr ……

I have the honour to refer to the IAEA's International Physical Protection Advisory Service (IPPAS) programme. We are aware that this programme can be useful in assisting States in the assessment of their nuclear security regime and in the development of future activities in support of nuclear security issues. In this regard, my Government respectfully requests that the IAEA arranges for an IPPAS mission to assess our nuclear security regime at the earliest opportunity.

We have identified Ms/Mr as being the point of contact responsible for making detailed arrangements for the organization of the mission. His/her contact information is as follows:

1.6.3. Designation of technical officer and team leader

On receipt of a formal request for an IPPAS mission, the IAEA will designate a staff member to act as technical officer responsible for coordinating the preparatory work and making the necessary arrangements to conduct an IPPAS mission.

With the consent of the host country, the IAEA will select a Member State expert with recognized leadership qualities and very broad experience in nuclear security as the IPPAS team leader.

1.6.4. Preparatory meeting

Prior to the preparatory meeting with, and in, the host country, the IAEA technical officer should convene a meeting involving various interested Divisions within the IAEA in order to harmonize the IAEA's approach to the proposed mission and review existing information related to the host country.

The preparatory meeting, involving the IAEA technical officer and the team leader, should be held in the host country approximately three to four months before the IPPAS mission to allow governmental organizations, including the competent authority and representatives of relevant facilities, to participate. At this meeting, the IAEA should present a briefing to foster a clear understanding of the IPPAS process and methodology. In a complementary manner, the host country should provide a briefing on its nuclear programme and its physical protection regime. A record of the meeting will be exchanged.

The meeting will address:

- The main features of the IPPAS programme;
- The scope of the mission (e.g. facilities to be visited, desirability of having a State legal expert);
- The topics, corresponding to IPPAS programme modules, about which the host country is particularly seeking advice;
- Identification and scheduling of all persons and organizations to be interviewed;
- Preparation of an advance information package for the mission team, including a description of the national security regime, relevant laws, regulations etc., information on facilities to be visited and activities to be observed, as well as a list of documents relevant to nuclear security;
- Logistical support required, e.g. team office, computer, printer, copier, local transportation, accommodation;
- IPPAS team composition;
- Provision of translation/interpretation services;
- Preparation, review and confidentiality of technical notes and of the IPPAS mission final briefing and report;
- Finalization of the detailed mission schedule.

1.6.5. Host country responsibilities

As part of the discussions at the preparatory meeting, the IAEA technical officer and the team leader will make arrangements with the host country to ensure the provision of necessary support facilities. The host country will be expected to provide in-country transportation for team members to all required venues and to assist in obtaining suitable accommodation and in other related aspects.

IPPAS reviews are conducted in English. The host country should provide any necessary interpretation to allow team members to do their work. At all times, there should be at least one meeting room at the disposal of the team, of sufficient size to enable them to work and to hold discussions in reasonable privacy. The room should be equipped with sufficient electrical outlets to allow each member to work independently. A computer printer and a photocopying machine and paper should also be readily available to team members.

Documents, or their relevant sections, identified during the preparatory meeting should be supplied in English. If necessary, the host country should translate pertinent documents to be used during the mission into English. In order to save time during the mission and to allow IPPAS team members to gain a good understanding of the government organization, regulatory authorities and their legal basis, the host

country, should provide these documents to the IAEA for transmittal to IPPAS team members at least one month prior to the conduct of IPPAS mission.

Relevant non-confidential information should be available in advance of the mission, and should include:

- Overview of the nuclear security regime.
- National legislation:
    - Law(s) governing security of nuclear material and/or other radioactive material and associated facilities;
    - Synopsis of the responsibilities and structure of the various governmental organizations (specifying relevant departments) that deal with the nuclear security issues and how they interrelate;
    - Regulations on the security of nuclear material and/or other radioactive material and associated facilities.
- Competent authority(ies):
    - Organizations and entities involved at the State level in nuclear security matters;
    - Legal status and responsibilities assigned to the competent authority;
    - Structure, organization and staffing of the competent authority;
    - Interagency agreements regarding coordination of nuclear security activities;
    - Description of the licensing procedures, where applicable;
    - Inspection and enforcement practices;
    - List of applicable codes and standards.
- General, publicly available information on facility and/or transport, technical description of plant, site plans and procedures.

Additional relevant information, which might be sensitive, will be provided during the IPPAS mission. For facility and transport reviews, the host government should help ensure the full cooperation of the operator and the carrier.

A good practice for the host country is to plan carefully and thoroughly and prepare for the IPPAS mission as a means of supporting an efficient and productive information exchange. The host country should identify in advance the agency officials and facility/operator representatives who will participate in the IPPAS team visit. They should all familiarize themselves with the main reference documents and other relevant documents appropriate to the mission's scope. They should consider how the recommendations in these documents are addressed in their country, and they should present their major, general information as part of the country briefing and be prepared to discuss the specific, detailed information during the interview process. Preparing answers to the specimen questions in each topical area would facilitate a more effective and efficient IPPAS mission. The host country may choose to go one step further by conducting a prior self-assessment with respect to country obligations and IAEA recommendations documents or methodologies and associated tools. These activities have added value in terms of security awareness, human resource development and nuclear security regime sustainability.

1.6.6. IPPAS team formation

The team should comprise a team leader and team experts with expertise in the following areas, as appropriate: nuclear law, regulatory matters, the type(s) of facility and/or activity to be reviewed, physical

protection systems and their evaluation, nuclear material accountancy and control, response forces, computer security, security of radioactive material including categorization of radioactive material, transport security and other relevant areas as required. A technical writer to assist the team in developing technical notes and the mission report and an information technology (IT) expert may be included. The IAEA technical officer is also part of the team. More generally, the team should be composed of several experts with complementary skills according to the needs expressed by the host country for the mission.

1.6.6.1. Team leader

The team leader is particularly important for the success of the mission. The team leader must have recognized leadership qualities and very broad experience in the full scope of review activities in nuclear security areas that are likely to confront an IPPAS team. Preferably, the team leader is a former IPPAS team member/expert.

The team leader has overall responsibility for:

- Representing the IPPAS team;
- Orientation of IPPAS team experts;
- Leading the IPPAS team review activities, including conducting daily team meetings, ensuring that schedules are met, and providing debriefings and interacting with host government officials and facility and transport operators, as necessary;
- Coordinating the review of all technical notes and production of the draft mission report;
- Leading the team discussions and analyses that result in a consensus set of recommendations, suggestions and good practices;
- Preparing and presenting the mission results (briefing and report) at the exit meeting;
- Producing, with the IAEA, the final IPPAS mission report.

1.6.6.2. Team experts

The IAEA selects team experts in consultation with the team leader and with the consent of the host country to which information on the expertise and experience of potential team experts should be provided in advance (e.g. short curriculum vitae). The experts are invited from Member States, have recognized broad knowledge and extensive experience in nuclear security, and are able to commit to approximately three weeks for the preparation, conduct of the mission and mission reporting. All formal requests for persons to become team experts should be made through the respective Permanent Mission or other agreed official channels.

Team experts are selected so as to ensure that a variety of national approaches to regulation and implementation are represented. Each of the experts is likely to have, in addition to their particular area of expertise, knowledge of other national approaches and other relevant areas. This knowledge, combined with knowledge of the international instruments and guidance, allows good practices to be provided.

1.6.6.3. Technical officer

The IAEA technical officer has overall responsibility for:

- Confirming with the host country who will be the primary contact for planning and conduct of the mission;
- Identifying, in consultation with the host country, a nuclear security expert to be designated as the team leader for the IPPAS mission;
- Arranging, in conjunction with the team leader, for a preparatory meeting with the host country;
- Making proposals regarding selection of IPPAS team members (final IPPAS team composition requires formal approval by the host country);
- Arranging to receive an advance information package from the host government;
- Coordinating necessary logistical arrangements for support of the IPPAS team.

The appointed IAEA technical officer will accompany the IPPAS team throughout the mission to liaise with the host government counterparts and to provide any other administrative or expert support that may be required. The IAEA technical officer will ensure that the IPPAS team members are provided with instructions for the formation of the team and its arrival at the site of the mission. Additional to the advance information provided by the host country, the technical officer will research and collect the current edition of relevant IAEA reference documents and any other material pertinent to the mission, providing it to the team leader and/or team in an appropriate form, time and place.

The IAEA technical officer will be responsible for collecting and destroying or returning to the host organization all sensitive information before the team leaves the host country.

Finally, the IAEA technical officer has overall responsibility for coordinating and transmitting the final IPPAS mission report.

1.6.6.4. Technical writer

A technical writer may join the IPPAS team at the end of the first week of the mission and accompany it until the end of the mission to assist in the development and timely completion of the IPPAS draft report and exit presentation. The technical writer gathers written input from the team and formats and edits the material, as appropriate.

1.6.7. IPPAS mission

An IPPAS mission typically lasts ten working days in the host country, but this duration may be adapted to the scope of the mission.

1.6.7.1. Team organizational meeting

On arrival in a host country, prior to the official commencement of an IPPAS mission, the IAEA technical officer and team leader provide a briefing to the team experts with the aim of familiarizing them with the objectives and overall scope, as well as the conduct of the mission.

The briefing may last only a few hours or up to one day and should address the following topics:

- Introduction of team members;
- Purpose and mission objectives;
- Scope of the mission;
- Roles and responsibilities of each team member;
- Mission schedule and team meetings;
- Review methodology;
- Reporting;
- Confidentiality; and
- Observance of safety and security rules.

The team leader should encourage experienced IPPAS experts to participate actively in this session so that all team experts can benefit from their past experience.

1.6.7.2. Opening meeting

The IPPAS mission starts with an opening meeting with representatives of the host country, during which the programme for the mission is confirmed. An overview of the State's nuclear security regime, nuclear programme and facilities to be visited during the mission should be presented by the host country.

1.6.7.3. Information collection

The IPPAS team uses the following methods to acquire the information needed to develop its conclusions and recommendations, as set out in the IPPAS report:

- A review of written material provided as pre-mission documentation and material provided by the host country during the mission, e.g. legislation, regulations, facility information. During the mission, national authorities and facility management should make an effort to provide all documents considered essential for the IPPAS team to carry out its work.
- Interviews with competent authority personnel, facility operators and representatives of other relevant organizations.
- Direct observation of the organization, practices and systems in place for the State and the implementation of the physical protection system and measures at facilities and during transportation activities.

Team members are expected to consider, to the extent necessary, all aspects of nuclear security within the scope of the mission in order to make an assessment. Matters of concern (e.g. deviations from provisions of international instruments and IAEA nuclear security documents) should be assessed to the extent required to document them accurately. Recommendations and suggestions should be formulated on the basis of the review. Similarly, good practices encountered during the review should be documented and described in the mission report in sufficient detail as to be readily understood.

While conducting a mission, the IPPAS team will collect the information necessary to assess the State's nuclear security regime and its implementation at facilities and during transport, in accordance with the mission scope. Written material provided by the host country, as well as all information derived from interviews with personnel and observations made by team members, contribute to the mission results. Of particular interest are the observations related to organization, to allocation of responsibilities at the State level, at facilities and for the secure transport of nuclear or radioactive material, and to practices in use.

The handling and distribution of field notes of the individual experts must fulfill rules as determined by the host country according to its requirements for protection of sensitive information. If no specific rule is defined by the State, field notes are treated as sensitive information and restricted on a 'need-to-know' basis, in accordance with IAEA procedures.

(a) Documents and briefings

Written material of general interest to the expert team that should be provided prior to the mission is listed in Section II-5 (host country responsibilities).

The documentation sections of the modules include those documents that may be requested by the team during the mission from the host country or from the operators, shippers and/or carriers to be visited.

In addition to these documents, briefings by relevant representatives of competent authorities of the host country and facilities and transports to be reviewed will help the IPPAS experts in their understanding of the specific conditions and practices of the host country's nuclear security regime.

(b) Interviews

After consideration of the relevant written material, interviews with the competent authority, relevant organizations and facility and transport personnel should then be used to:

- Obtain additional information by eliciting individual opinions;
- Clarify and/or review issues arising from previously provided documents or briefings;
- Support, confirm or refute observations made during the on-site observation of nuclear security measures in place.

Specific guidance on how data can be collected is contained in the relevant modules. Interviews will also provide an opportunity for important information to be exchanged between IPPAS team members and their host country counterparts. An interview is an open discussion between host country counterparts and team members. Properly conducted, these interviews are possibly the most important part of the IPPAS

mission. The interviews should not be conducted nor construed as being an interrogation or test of the host country's representatives.

(c) Direct observation

Direct observation of how nuclear security measures have been implemented at a facility or during transport is an important aspect of the review process. A substantial part of the review should be devoted to practices in use. In agreement with the host organization, observation may cover nuclear security practices including the use of physical protection equipment and exercise of contingency plans, regulatory inspections, etc.

1.6.7.4. Evaluation methodology

On the basis of advance information, briefings, interviews and observations, the team forms an assessment of the host country's nuclear security regime and systems. If more information is needed, it may be necessary to conduct additional document reviews, interviews and observations in order to form a sound assessment.

For each working day of the IPPAS mission, the team leader should conduct a team meeting during which the team members individually summarize their findings and concerns developed during the day, including perceived strengths and weaknesses. This environment provides an opportunity for all team members to contribute their views, further strengthening the experience base of the assessment, and to identify topics needing further information or clarification.

During the course of the review, individual team members will write detailed technical notes on their observations and conclusions on the areas assigned to them, including any recommendations, suggestions or instances of good practices. These technical notes are then the subject of peer review by all team members.

1.6.7.5. Draft report

The IPPAS team review, reflected in a Working Draft Report, compares national legislation and regulation, as well as observed practices with existing international instruments, guidance and good practices. The review:

- Assesses national practices with respect to Member State obligations, guidance and accepted international practices;
- Considers laws and regulation requirements as well as procedures, and how effectively these are implemented in practice; and
- Provides proposals for change, when appropriate.

The comparisons usually result in recommendations or suggestions or the identification of good practices in accordance with the following definitions:

- ✓ **Recommendation**: A recommendation is an advice on improvements that should be made in the areas that have been evaluated and discussed with the host country. Such advice must be based on CPPNM and its 2005 Amendment, security provisions of the Code of Conduct on the Safety and Security of Radioactive Sources, IAEA Nuclear Security Fundamentals and IAEA Nuclear Security Recommendations. Recommendations are specific, realistic and designed to result in tangible improvements.

- ✓ **Suggestion**: A suggestion may either be an additional proposal in conjunction with a recommendation or a stand-alone item following discussion of the associated topic with the host country. It contributes to improvements in the State nuclear security regime by indicating useful expansions of existing programmes and pointing to better alternatives to current work practices. In general, it should stimulate the competent authority, other relevant entities and the facility or transport operator's management and staff to consider ways and means of enhancing nuclear security. Suggestions are based on international good practices and/or IAEA nuclear security implementing guides and technical guides.

- ✓ **Good practices**: A good practice is an indication of an outstanding organizational arrangement, programme or performance that is more than just the fulfilment of current international obligations and IAEA recommendations. It should be worthy of bringing to the attention of other Member States as a model in the general drive for excellence.

The Working Draft Report is discussed with the host country counterparts to seek clarification regarding any subject that may have been misinterpreted, and to consider the wording from a presentational standpoint. Host country agreement is required for the inclusion of any photographs, diagrams, drawings, etc., in the Draft Report.

After the IPPAS team has reviewed and discussed the Working Draft Report with the host country counterparts, it will develop its evaluation in the form of a Draft Report for presentation to the competent authority and other host country relevant entities at the exit meeting.

1.6.7.6. Exit meeting

At the exit meeting, the team leader presents a briefing on the outcome of the mission and hands over a Draft Report to the representatives of the host country. The exit meeting provides a forum for both parties to discuss the mission's findings, in particular, recommendations and suggestions. At this time, a copy of the Draft Report is given to the host country's point of contact. The host country's point of contact is requested to provide the IAEA with additional consolidated host country's comments, if any, during the next four weeks after the meeting.

The exit meeting marks the completion of the IPPAS mission in the host country.

1.6.8. Final report

The relevant State authority and, as decided by the host country, other authorities/agencies will review the Draft Report provided at the exit meeting. The relevant State authority will transmit consolidated comments to the IAEA technical officer within four weeks following conclusion of the mission.

On the basis of these comments, and on the outputs of the exit meeting, the IAEA technical officer, in consultation with IPPAS team leader, will finalize the IPPAS mission report. The IPPAS mission report is then sent through official channels to the host country.

The IAEA technical officer will have overall responsibility for transmitting the final mission report to the host country counterparts and ensuring that the objectives of the mission have been adequately addressed.

1.6.9. Follow-up activities

The State/facility will normally handle most of the recommendations and suggestions resulting from a mission without any external assistance. However, in some cases, external resources may be needed to assist with implementing the recommendations and suggestions. In such cases, the State may obtain assistance through the IAEA or through bilateral support programmes.

The IAEA remains ready to coordinate follow-up activities. A post-mission consultation may be initiated by the host country or by the IAEA after submission of the IPPAS report to the host country in order to discuss whether any advice or assistance can be provided to help implement the mission recommendations and suggestions.

At the request of a Member State that has been the recipient of an IPPAS mission, a number of follow-up support activities may be pursued, such as:

- Additional IPPAS missions that address additional review modules;
- Training national authority and facility/transport personnel in physical protection system design, analysis and implementation;
- Assistance in the development or revision of legislation;
- Assistance of Member State competent authorities and facility/transport operators in developing nuclear security regulatory guidance and facility/transport procedures;
- Assistance in the development, use and maintenance of the DBT;
- Assistance in upgrading the physical protection system at the facility or during transport;
- Advice on methodology to assess the effectiveness of physical protection systems;
- IAEA fellowship awards to State representatives;
- Assistance in the arrangement of scientific visits on nuclear security issues, by host country representatives to other countries;
- Incorporation of actions arising from the recommendations and suggestions into an Integrated Nuclear Security Support Plan (INSSP).

1.6.10. Follow-up missions

The IAEA recommends an IPPAS follow-up mission that allows the host country to have an assessment of the adequacy of its response to the recommendations and suggestions of the previous IPPAS mission(s). Ideally, such a mission should be conducted within a period of three to five years.

The scope of a follow-up mission can be tailored to accommodate the particular concerns of the host country. At a minimum, the mission should review the host country's response to the recommendations and suggestions made during the initial mission. The host country may also request advice on additional nuclear security topics. A review of another facility or transport can be included as part of the follow-up mission.

1.6.10.1. Follow-up mission objectives

Possible objectives of a follow-up mission are to:

- Review the implementation of recommendations and suggestions of the previous IPPAS mission(s), taking into account the current status of the State's nuclear security regime and its implementation at the facilities or during transport;
- Respond to specific host country requests for further advice;
- Continue the exchange of information on international nuclear security practices.

1.6.10.2. Follow-up mission methodology

The methodology of the follow-up mission is essentially the same as an IPPAS mission, with the following differences.

The length of an IPPAS follow-up mission is expected to be shorter than the initial IPPAS mission. However, its duration depends on the amount of work undertaken to address the recommendations and suggestions made by the initial IPPAS mission and any additional scope of the mission, such as the number of facilities and/or transports that the host country and the IAEA agree to review. The IPPAS follow-up mission team is, as nearly as possible, made up of the IAEA technical officer, team leader and selected experts of the original IPPAS review mission and supplemented, as required, by experts with relevant expertise.

At the start of the follow-up mission, the host country should make available to the team the initial IPPAS mission report and pertinent information regarding actions taken to implement the recommendations and suggestions developed by the initial IPPAS mission. New documentation on developments since the last mission (e.g. amendments to legislation and regulations) and additional follow-up mission topics should be provided in advance of the follow-up mission.

1.6.10.3. Conduct of the follow-up mission

On the basis of the relevant previous mission, IPPAS team members will address the following questions to the host country's relevant organizations and facility operator, as appropriate:

- Have all the recommendations/suggestions been addressed (e.g. new or revised legislation, enhanced arrangements with other related organizations, implementation of physical protection measures)?

- What changes have already been made or implemented (e.g. physical protection system modifications, establishment of new physical protection systems and procedures, or inspection and enforcement)?
- If so, were the changes evaluated and how?
- Has overall effectiveness of the physical protection regime been improved?
- What difficulties were encountered and how were they resolved?
- Is there a plan to continue with improvements to the physical protection regime?
- What difficulties remain unresolved and how will these problem areas be addressed (e.g. using bilateral support programmes or IAEA assistance will be requested)?

In undertaking the above review, consideration should also be given to pertinent developments since the initial IPPAS mission, such as:

- New or amended international instruments and guidance;
- Changes in the facility/transport physical protection system;
- Changes in the legal framework and regulations, governmental organization;
- Changes in the DBT (e.g. changes in the nature of the threats and the consequences to the physical protection system);
- Changes in the State nuclear programme and implications for physical protection;
- Any other significant incidents or events that have affected the nuclear security regime and/or the facility or transport organization since the previous IPPAS mission;
- Any other enhancement in the global/national nuclear security regime; and
- Any significant changes to technical approaches, to security technologies or to equipment.

2. NATIONAL REVIEW OF NUCLEAR SECURITY REGIME FOR NUCLEAR MATERIAL AND NUCLEAR FACILITIES (MODULE 1)

2.1. INTRODUCTION

The IPPAS national review module is the primary IPPAS review that evaluates a host country's physical protection regime. It is a broad based review of physical protection elements ranging from governmental organization and legislation relevant to physical protection, through the competent authority's regulatory role and processes, procedures and practices for inspection and enforcement and its integration with other organizations, to the sustainability of the regime.

In order to allow time for consideration of these fundamental issues, the background information necessary to enable team members to begin to formulate views on this area will need to be provided by the host country in advance of the IPPAS mission. Arranging for the appropriate documentation is the responsibility of the IAEA technical officer and the team leader.

There may be areas where review questions impinge on matters which are sensitive (e.g. threat assessment and DBT). It is not necessary that the IPPAS team have detailed information on their content to ascertain that they are addressed using a systematic process.

General information and details on purpose, objectives and methodology of conducting an IPPAS mission are laid down in chapter 1 of the IPPAS Guidelines.

2.2. PURPOSE

An IPPAS national review mission is the recommended starting point for host countries that wish to have their physical protection regime reviewed against international instruments and guidance.

Guidance outlined in the following sections is considered by the IPPAS team members during the course of the mission. The competent authority and other relevant authorities can use this guidance for self-assessment purposes. The review points/specimen questions should not be used as a simple yes/no checklist but rather questions which allow the interviewer to gain an appreciation of the subject and, as appropriate, to compare implementation with international instruments, IAEA recommendations and accepted international good practices. The specimen questions posed below are not an exhaustive list and team members are encouraged to ask additional questions as necessary.

2.3. SCOPE OF MISSION

The IPPAS national review includes the following areas:

- Government organization, assignment of responsibilities, and international obligations.
- Legal and regulatory framework:
    - Primary legislation (including criminal law/code);
    - Secondary legislation (regulations/decrees/orders).
- Roles and responsibilities of the competent authority.

- Licensing/authorization process.
- Coordination with other State organizations that contribute to nuclear security (law enforcement agencies, customs and border control, intelligence agencies, judicial entities).
- Threat assessment and DBT.
- Risk informed approach:
    - Risk management;
    - Graded approach;
    - Defence in depth.
- Sustaining the physical protection regime:
    - Security culture;
    - Quality assurance;
    - Confidentiality;
    - Sustainability programme.
- Planning and preparation for, and response to, nuclear security events.

2.4. GOVERNMENT ORGANIZATION, ASSIGNMENT OF RESPONSIBILITIES, INTERNATIONAL OBLIGATIONS AND INTERNATIONAL COOPERATION

2.4.1. Objectives

- Establish whether the State has identified and defined those organizations responsible for nuclear security within the State and has made arrangements to provide for international cooperation and assistance.

2.4.2. Basis

- CPPNM Amendment, Art. 2A:

"Each State Party shall establish, implement and maintain an appropriate physical protection regime applicable to nuclear material and nuclear facilities under its jurisdiction, with the aim of:

(a) protecting against theft and other unlawful taking of nuclear material in use and storage, and during transport;

(b) ensuring the implementation of rapid and comprehensive measures to locate and, where appropriate, recover missing or stolen nuclear material;

(c) protecting nuclear material and nuclear facilities against sabotage; and

(d) mitigating or minimizing the radiological consequences of sabotage."

- Nuclear Security Fundamentals, IAEA NSS No. 20: Essential Element 1: State Responsibility:

"Responsibility rests with the State for meeting the objective set forth in Section 2 by establishing, implementing, maintaining and sustaining a *nuclear security regime* applicable to *nuclear material*, *other radioactive material*, *associated facilities*, and *associated activities* under a State's jurisdiction."

- Nuclear Security Fundamentals, IAEA IAEA NSS No.20: Essential Element 2: Identification and Definition of Nuclear Security Responsibilities:

"Nuclear security responsibilities of *competent authorities* designated by the State, as described in Essential Element 3, including *regulatory bodies* and those *competent authorities* related to border control and law enforcement, and responsibilities for all *authorized persons*, are clearly identified and defined. Provisions are identified and defined for appropriate integration and coordination of responsibilities within the *nuclear security regime*, as well as for the State's oversight to ensure the continued appropriateness of the nuclear security responsibilities."

- Nuclear Security Fundamentals, IAEA NSS No. 20: Essential Element 4: International Transport of Nuclear Material and Other Radioactive Material:

"The responsibility of a State for ensuring that *nuclear material* and *other radioactive material* are adequately protected extends to the international transport thereof, until that responsibility is properly transferred to another State, as appropriate."

- CPPNM Amendment, Fundamental Principle A: Responsibility of the State:

"The responsibility for the establishment, implementation and maintenance of a physical protection regime within a State rests entirely with that State."

- CPPNM Amendment, Fundamental Principle B: Responsibilities during International Transport:

"The responsibility of a State for ensuring that nuclear material is adequately protected extends to the international transport thereof, until that responsibility is properly transferred to another State, as appropriate."

- INFCIRC/225/Rev.5, para. 2.1:

"The overall objective of a State's nuclear security regime is to protect persons, property, society, and the environment from *malicious acts* involving *nuclear material* and other radioactive material. The objectives of the State's *physical protection regime*, which is an essential component of the State's nuclear security regime, should be:

  - To protect against *unauthorized removal*. Protecting against theft and other unlawful taking of *nuclear material*.
  - To locate and recover missing *nuclear material*. Ensuring the implementation of rapid and comprehensive measures to locate and, where appropriate, recover missing or stolen *nuclear material.*
  - To protect against *sabotage*. Protecting *nuclear material* and *nuclear facilities* against *sabotage.*
  - To mitigate or minimize effects of *sabotage*. Mitigating or minimizing the radiological consequences of *sabotage*."

- INFCIRC/225/Rev.5, para. 2.2:

"The State's *physical protection regime* should seek to achieve these objectives through:

- Prevention of a *malicious act* by means of deterrence and by protection of sensitive information;
- Management of an attempted *malicious act* or a *malicious act* by an integrated system of *detection*, delay, and response;
- Mitigation of the consequences of a malicious act."

- INFCIRC/225/ Rev.5, para. 2.3:

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

- INFCIRC/225/Rev.5, para. 3.1:

"The State's *physical protection regime* is intended for all *nuclear material* in use and storage and during *transport* and for all *nuclear facilities*. The State should ensure the protection of *nuclear material* and *nuclear facilities* against *unauthorized removal* and against *sabotage*."

- INFCIRC/225/Rev.5, para. 3.2:

"The State's *physical protection regime* should be reviewed and updated regularly to reflect changes in the *threat* and advances made in physical protection approaches, systems, and technology, and also the introduction of new types of *nuclear material* and *nuclear facilities*."

- INFCIRC/225/Rev.5, para. 3.3:

"A State's responsibility for physical protection should be determined either by the borders of its sovereign territory or the flag of registration of the transport vessel or aircraft. A State's *physical protection regime* for *nuclear material* in international *transport* should extend to the carriage of material on board ships or aircraft registered to that State while in international waters or airspace and until the receiving State acquires jurisdiction."

- INFCIRC/225/Rev.5, para. 3.4:

"The State's *physical protection regime* should ensure that *nuclear material* is always under the jurisdiction and continuous control of the State and that the point at which responsibility for physical protection is transferred from one State to another and from one carrier to another is clearly defined and implemented by all concerned. International transport operations should be overseen by one or more government organizations having the relevant authority and competence in transport security and/or the appropriate mode of *transport*."

- INFCIRC/225/Rev.5, para. 3.5:

"The shipping State should consider, before allowing international *transport*, if the States involved in the *transport*, including the transit States:

- Are Parties to the Convention on the Physical Protection of Nuclear Material (INFCIRC/274/Rev.1); or
- Have concluded with it a formal agreement which ensures that physical protection arrangements are implemented in accordance with internationally accepted guidelines; or

- Formally declare that their physical protection arrangements are implemented according to internationally accepted guidelines; or
- Have issued licences or other authorizing documents which contain appropriate physical protection provisions for the *transport* of *nuclear material*."

- INFCIRC/225/Rev.5, para. 3.6:

"When international shipments transit the territory of States other than the shipping State and the receiving State, the shipping State should, in advance, identify and inform the other States involved in such transit in order that the transit States can ensure that the proposed arrangements are in accordance with their national law."

- INFCIRC/225/Rev.5, para. 3.7:

"During the international *transport* of Category I nuclear material, and possibly other categories of *nuclear material*, especially if accompanied by armed *guards*, the responsibility for *physical protection measures* should be the subject of written arrangements accepted by the States concerned. The relevant *competent authority* of the shipping, receiving, and transit States, and the flag State of the *conveyance* should establish specific measures to ensure the maintenance of communication regarding the continued integrity of the shipment in order to ensure that responsibility for response planning and capabilities is defined and fulfilled. Additionally, any sensitive information shared by States concerned should be protected and the overall arrangements for the shipment should be in accordance with the relevant States' national laws. The point at which responsibility for physical protection is transferred from one State to another should be stated in advance and in sufficient time to enable the relevant State to make adequate physical protection arrangements."

- INFCIRC/225/Rev.5, para. 3.8:

"The State should clearly define and assign physical protection responsibilities within all levels of involved governmental entities including response forces and for *operators* and, if appropriate, carriers. Provision should be made for appropriate integration and coordination of responsibilities within the State's *physical protection regime*. Clear lines of responsibility should be established and recorded between the relevant entities especially where the entity responsible for the armed response is separate from the *operator*."

- INFCIRC/225/Rev.5, para. 3.10:

"The State should define requirements — based on the *threat assessment* or *design basis threat* — for the physical protection of *nuclear material* in use, in storage, and during *transport*, and for *nuclear facilities* depending on the associated consequences of either *unauthorized removal* or *sabotage*. The State should ensure that the more stringent requirements for physical protection — either those against *unauthorized removal* or those against *sabotage* — are applied."

- INFCIRC/225/Rev.5, para. 3.13:

"The State should ensure that evaluations include exercises to test the *physical protection system*, including the training and readiness of *guards* and/or *response forces*."

- INFCIRC/225/Rev.5, para. 3.14:

  "Taking into consideration State laws, regulations, or policies regarding personal privacy and job requirements, the State should determine the trustworthiness policy intended to identify the circumstances in which a trustworthiness determination is required and how it is made, using a *graded approach*. In implementing this policy, the State should ensure that processes are in place to determine the trustworthiness of persons with authorized access to sensitive information or, as applicable, to *nuclear material* or *nuclear facilities*."

- INFCIRC/225/Rev.5, para. 3.31:

"States are encouraged to cooperate and consult, and to exchange information on physical protection techniques and practices, either directly or through the International Atomic Energy Agency and other relevant international organizations."

- INFCIRC/225/Rev.5, para. 3.32:

"States should inform the International Atomic Energy Agency, and other States as applicable, of appropriate points of contact for matters related to the physical protection of *nuclear material* and *nuclear facilities*."

- INFCIRC/225/Rev.5, para. 3.33:

"In the case of *unauthorized removal* or *sabotage* or credible threat thereof, the State should provide appropriate information as soon as possible to other States which appear to it to be concerned, and to inform, where appropriate, the International Atomic Energy Agency and other relevant international organizations."

- INFCIRC/225/Rev.5, para. 6.45:

"The State should ensure that its *physical protection regime* includes rapid response and comprehensive measures to locate and recover missing or stolen *nuclear material* during *transport*."

- INFCIRC/225/Rev.5, para. 6.48:

"The responsible State organizations should develop *contingency plans* for the rapid location and recovery of *nuclear material* which has been declared missing or stolen during *transport*."

- INFCIRC/225/Rev.5, para. 6.50:

"The State should ensure that appropriate State response organizations, carriers and/or other relevant entities conduct exercises to assess and validate the *contingency plans* and also to train the various participants on how to react in such a situation."

- INFCIRC/225/Rev.5, para. 6.68:

"The State should ensure that joint exercises, which simultaneously test emergency and *contingency plans* and actions for *transport* of *nuclear material* are regularly carried out in order to assess and validate the

adequacy of the interfaces and response coordination of emergency and security organizations involved in responding to various scenarios, and should have a method for incorporating lessons learned to improve both management systems."

2.4.3. Documentation

- Synopsis and organization chart of the structure and responsibilities of the various government organizations (specifying relevant departments) that deal with the physical protection of nuclear material and nuclear facilities and how they interrelate.
- It would be helpful to provide a diagram that distinguishes between direct lines of control and lines that show where advice is given and/or received. (Such authorities will include those with responsibilities for regulations, trustworthiness determinations, threat assessments and provision of response forces.)

2.4.4. Review points/specimen questions

- How is your nuclear security programme organized?
- Which governmental organization(s) have responsibilities for physical protection and what are their responsibilities?
- What are the reporting lines of the various authorities or bodies within the legislative and regulatory framework?
- What is the extent of your nuclear programme?
- What are the numbers and types of facility and/or transports that are located in the State or are being planned?
- What nuclear material is in use, storage and transport?
- What relevant international obligations has the State undertaken?
- Which organization is currently registered with the IAEA as the point-of-contact for the CPPNM?
- How does the State ensure protection of nuclear material during international transport until responsibility is transferred to another State?

2.5. LEGAL AND REGULATORY FRAMEWORK

2.5.1. Objectives

- Verify whether the State has established, and is maintaining, a comprehensive and effective legislative and regulatory framework to govern physical protection.

2.5.2. Basis

- CPPNM Amendment, Fundamental Principle C: Legislative and Regulatory Framework:

"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."

- INFCIRC/225/Rev.5, para. 3.9:

"A State should take appropriate measures within the framework of its national law to establish and ensure the proper implementation of the State's *physical protection regime.*"

- INFCIRC/225/Rev.5, para. 3.11:

"The State's legislation should provide for the comprehensive regulation of physical protection and include a licensing requirement or other procedures to grant authorization. The State should promulgate and review its regulations for the physical protection of *nuclear material* and *nuclear facilities* regularly. The regulations should be applicable to all such materials and facilities regardless of whether under State or private ownership."

- INFCIRC/225/Rev.5, para. 3.14:

"Taking into consideration State laws, regulations, or policies regarding personal privacy and job requirements, the State should determine the trustworthiness policy intended to identify the circumstances in which a trustworthiness determination is required and how it is made, using a *graded approach*. In implementing this policy, the State should ensure that processes are in place to determine the trustworthiness of persons with authorized access to sensitive information or, as applicable, to *nuclear material* or *nuclear facilities*."

- INFCIRC/225/Rev.5, para. 3.15:

"Enforcement of physical protection regulations should be a part of a State's legislative and regulatory framework."

- INFCIRC/225/Rev.5, para. 3.16:

"Sanctions against the *unauthorized removal* and against *sabotage* should be part of the State's legislative or regulatory system."

2.5.3. Laws

2.5.3.1. Documentation

National legislation:

- Law(s) and orders/decrees governing the physical protection of nuclear material and facilities;
- Law(s) and orders/decrees governing the determination of personnel trustworthiness;
- Laws relevant to the classification and protection of sensitive information;
- Penal (criminal) code as far as it governs sanctions against theft of nuclear material and sabotage of nuclear material and nuclear facilities and unauthorized disclosure of sensitive information; and
- Laws relating to guard and response force and use of arms/force.

2.5.3.2 Review points/specimen questions

- What is the principal legislation (laws, decrees or other legally binding provisions) which establishes the State physical protection regime?
- How does this legislation require appropriate administrative and technical measures for the physical protection of nuclear material and nuclear facilities as a prerequisite to obtaining a licence?
- Is there a (periodic) review process of the principal legislation to reflect the introduction of new types of nuclear material and nuclear facility, changes in the threat, and advances made in physical protection approaches, systems and technology?
- Describe how the current legislation requires the government to establish or designate a competent authority(ies) responsible for comprehensive governmental regulation of all aspects of physical protection of nuclear material and nuclear facilities, including protection of sensitive information.
- Does the current legislation empower the competent authority to issue physical protection secondary (subordinate) legislation, e.g. regulations, directions and orders? If not the competent authority, then who has these powers?
- How does the legislation provide for the identification of licensing authorities and which organizations are parts of the process?
- Does this legislation require satisfactory physical protection prior to granting licences or authorizations?
- How does the legislation ensure new facilities are 'secure by design', i.e. include security in the facility design process?
- Does the current legislation empower the competent authority to carry out inspections and enforcement?
- Does the current legislation ensure measures to determine the trustworthiness of personnel?
- Does the current legislation include provisions for classification and protection of sensitive information?
- Does the current legislation (penal code) provide for sanctions against theft of nuclear material and the sabotage of nuclear material and nuclear facilities and unauthorized disclosure of sensitive information?
- Does the current legislation require the preparation of periodic reports on the physical protection of nuclear facilities and transport, and if so, by whom, and to whom are these reports addressed?
- Is the above legislation applicable to all nuclear facilities and to all nuclear material in use, storage and transport?
- Which laws and regulations ensure the obligations of the CPPNM are met?

2.5.4. Regulations

2.5.4.1. Documentation

- List of all relevant regulations, guides and/or technical standards that are required to be used or complied with by the applicant(s)/licensee(s).

2.5.4.2. Review points/specimen questions

- What is the principal secondary legislation (regulations, orders or other provisions) which establishes the State physical protection regime?
- Is this body of secondary legislation satisfactory and does it require appropriate administrative and technical measures for the physical protection of nuclear material and nuclear facilities as a prerequisite to obtaining a licence?
- Is there a (periodic) review process of the secondary legislation to reflect the introduction of new types of nuclear material and nuclear facility, changes in the threat, and advances made in physical protection approaches, systems and technology?
- Are there any undue impediments to the necessary amendment of secondary legislation?
- What is the hierarchy of regulations, guides and standards that are to be used by the applicant(s)/licensee(s)?
- Is there a system of consultation with other State organizations involved in nuclear security and/or applicant(s)/operator(s) in place to obtain feedback on standards or guides produced by the competent authority? Is this voluntary or required by legislation?
- Is the above secondary legislation applicable to all nuclear facilities and to all nuclear material in use, storage and transport?
- Does the secondary legislation adopt a performance based approach, a prescriptive approach or a combination of both?
- Does the secondary legislation require operators and carriers to develop and maintain security plans?
- Does the secondary legislation require the preparation and coordination of contingency plans by the operator, shipper and/or carrier and other relevant entities?
- Does the secondary legislation require the operator/carrier to account for all nuclear material at all times?

2.6. ROLES AND RESPONSIBILITIES OF THE COMPETENT AUTHORITY

2.6.1. Objectives

- Assess whether the competent authority has been provided with the adequate authority, competence, effective independence, and the financial and human resources necessary to fulfil its assigned responsibilities of regulation, oversight, and enforcement of relevant physical protection legislation.

2.6.2. Basis

- CPPNM Amendment, Fundamental Principle D: Competent Authority:

"The State should establish or designate a competent authority which is responsible for the implementation of the legislative and regulatory framework, and is provided with adequate authority, competence and financial and human resources to fulfil its assigned responsibilities. The State should take steps to ensure en effective independence between the functions of the State's competent authority and those of any other body in charge of the promotion or utilization of nuclear energy."

- INFCIRC/225/Rev.5, para. 3.18:

"The State's *competent authority* should have a clearly defined legal status and be independent from applicants/*operators*/*shippers*/carriers and have the legal authority to enable it to perform its responsibilities and functions effectively."

- INFCIRC/225/Rev.5, para. 3.19:

"The State's *competent authority* should have access to information from the State's *system for nuclear material accountancy and control*."

- INFCIRC/225/Rev.5, para. 3.20:

"The State's *competent authority* should be responsible for verifying continued compliance with the physical protection regulations and licence conditions through regular inspections and for ensuring that corrective action is taken, when needed."

- INFCIRC/225/Rev.5, para. 3.21:

"To ensure that *physical protection measures* are maintained in a condition capable of meeting the State's regulations and of effectively responding to the State's requirements for physical protection, the State's *competent authority* should ensure that evaluations based on *performance testing* are conducted by *operators* at *nuclear facilities* and, as appropriate, by *shippers* and/or carriers for *transport*. Evaluations should be reviewed by the State's *competent authority*, and should include administrative and technical measures, such as testing of *detection*, assessment, delay and communications systems, and reviews of the implementation of physical protection procedures. When deficiencies are identified, the *competent authority* should ensure that corrective action is taken by the *operator*, *shipper* and/or carrier."

- INFCIRC/225/Rev.5, para. 3.22:

"The State's *physical protection regime* should include requirements for timely reporting of *nuclear security events* and information which enables the State's *competent authority* to be informed of any changes at *nuclear facilities* or related to *transport* of *nuclear material* that may affect *physical protection measures*."

- INFCIRC/225/Rev.5, para. 3.35:

"The State should ensure that the *competent authority* has access to information from other organizations in the State on present and foreseeable threats to nuclear activities."

2.6.3. Documentation

- Description of the competent authority's legal status, powers, duties and responsibilities, as defined by law;
- Description of how the competent authority coordinates, liaises with and relates to each of the other government ministries, agencies or organizations involved with physical protection, e.g. Memorandum of Agreement;
- Description of inspection and evaluation practices by the competent authority.

2.6.4. Review points/specimen questions

- What are the statutory responsibilities of the competent authority?
- Is the statutory responsibility of the competent authority institutionally separate from that of the applicant(s)/licensee(s)? Is the competent authority independent of bodies responsible for developing and promoting nuclear energy? If not, what is the relationship?
- If the competent authority comprises more than one organization what is the relationship between these bodies having responsibility for the physical protection of nuclear material and nuclear facilities? Are their respective responsibilities established by legislation? Is there a Memorandum of Agreement/Understanding in use to ensure cooperation? If the competent authority is not a point of contact under the CPPNM, how does it liaise with that point of contact?
- Does the competent authority possess the following powers of regulatory licensing, inspection and enforcement to:

    - Establish and/or issue binding requirements and standards which, among other things, serve as the basis for inspection;
    - Require preparation of, and access to within a reasonable time, such reports and documents from operators and carriers as are essential for the performance of its inspection responsibilities;
    - Enter at any time for inspection purposes the premises of any nuclear facility or carrier's premises;
    - Communicate to authorized organizations inspection information, findings, recommendations and conclusions;
    - Require licensees to comply, within a reasonable period of time, with all decisions and enforcement actions of the competent authority; and
    - Apply appropriate sanctions to responsible persons (e.g. licensees) in the case of non-compliance with the legislation on physical protection? If not, what role does the competent authority play in enforcement actions?
- Does the competent authority maintain an inspection programme and does this include unannounced inspections?
- What are the competent authority's responsibilities for informing other relevant governmental organizations and the public of regulatory activities and physical protection related issues? How are these responsibilities discharged?
- What are the competent authority's international contacts in the field of physical protection for:

    - Exchange of information;
    - Meeting obligations to comply with the requirements of the CPPNM;
    - Notification of criminal incidents or abnormal occurrences; and
    - Mutual assistance in the event of a nuclear related incident, e.g. cooperation in the recovery and protection of stolen material?
- Are these contacts based upon formal exchange agreements, by international treaty, or are they on an ad hoc basis?
- At what levels are international contacts made?
- Does the competent authority actively participate in the activities of international organizations?
- Has the competent authority clearly stated the physical protection objectives and are they readily understood? Do they provide a good balance between being too general and too prescriptive, and between innovation and reliance on proven techniques?

- Is the budget for the competent authority adequate?
- Does the competent authority have an adequate number of suitably qualified and experienced physical protection staff?
- Does the competent authority have timely access to nuclear material accountancy records? Does the competent authority maintain a national inventory of nuclear material, including owner/licensee?
- Are the operators, shippers and carriers required to inform the competent authority promptly of nuclear security events and other relevant information or developments which may affect the physical protection measures of nuclear facilities and transports?
- Does the competent authority require that evaluations based on performance testing be conducted by operators, shippers and/or carriers? Does the competent authority review the evaluations conducted by operators, shippers and/or carriers?
- Does the competent authority ensure corrective actions are taken by the operator, shipper and/or carrier when deficiencies are identified?
- Has the competent authority established a system of internal scrutiny and assessment to confirm the adequacy of any standards or guide prior to its implementation?

2.7. LICENSING/AUTHORIZATION PROCESS

2.7.1. Objectives

- Determine how and what physical protection regulations, requirements and associated procedures are developed for evaluating applications and granting authorizations or licences.

2.7.2. Basis

- CPPNM Amendment, Fundamental Principle C: Legislative and Regulatory Framework:

"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."

- CPPNM Amendment, Fundamental Principle E: Responsibility of the Licence Holders

"The responsibilities for implementing the various elements of physical protection within a State should be clearly identified. The State should ensure that the prime responsibility for the implementation of physical protection of nuclear material or of nuclear facilities rests with the holders of the relevant licences or of other authorizing documents (e.g. operators or shippers)."

- INFCIRC/225/Rev.5, para. 3.11:

"The State's legislation should provide for the comprehensive regulation of physical protection and include a licensing requirement or other procedures to grant authorization. The State should promulgate and review its regulations for the physical protection of *nuclear material* and *nuclear facilities* regularly.

The regulations should be applicable to all such materials and facilities regardless of whether under State or private ownership."

- INFCIRC/225/Rev.5, para. 3.12:

"The State should licence activities or grant authorization only when such activities comply with its physical protection regulations. The State should make provisions for a detailed examination, made by the State's *competent authority*, of proposed *physical protection measures* in order to evaluate them for approval of these activities prior to licensing or granting authorization, and whenever a significant change takes place, to ensure continued compliance with physical protection regulations."

- INFCIRC/225/Rev.5, para. 3.24:

"The *operator*, *shipper* and carrier should comply with all applicable regulations and requirements established by the State and the *competent authority*."

- INFCIRC/225/Rev.5, para. 3.25:

"The *operator*, *shipper* and carrier should cooperate and coordinate with all other State entities having physical protection responsibilities, such as off-site *response forces*."

- INFCIRC 225/Rev.5, para. 3.26:

"The *operator* should ensure control of, and be able to account for, all *nuclear material* at a *nuclear facility* at all times. The *operator* should report any confirmed accounting discrepancy in a timely manner as stipulated by the *competent authority*."

- INFCIRC/225/Rev.5, para. 3.27:

"The *operator* should prepare a security plan as part of its application to obtain a licence. The security plan should be based on the *threat assessment* or the *design basis threat* and should include sections dealing with design, evaluation, implementation, and maintenance of the *physical protection system*, and *contingency plan*s. The *competent authority* should review and approve the security plan, the implementation of which should then be part of the licence conditions. The *operator* should implement the approved security plan. The *operator* should review the security plan regularly to ensure it remains up to date with the current operating conditions and the *physical protection system*. The *operator* should submit an amendment to the security plan for prior approval by the *competent authority* before making significant modifications, including temporary changes, to arrangements detailed in the approved security plan. The *competent authority* should verify the *operator's* compliance with the security plan."

- INFCIRC 225/Rev.5, para. 3.28:

"For a new *nuclear facility*, the site selection and design should take physical protection into account as early as possible and also address the interface between physical protection, safety and nuclear material accountancy and control to avoid any conflicts and to ensure that all three elements support each other."

- INFCIRC 225/Rev.5, para. 3.29:

"The *operator* should develop and implement means and procedures for evaluations, including *performance testing*, and maintenance of the *physical protection system*."

- INFCIRC 225/Rev.5, para. 3.30:

"Whenever the *physical protection system* is determined to be incapable of providing the required level of protection, the *operator*, *shipper* and/or carrier should immediately implement compensatory measures to provide adequate protection. The *operator* and/or *shipper* should then — within an agreed period — plan and implement corrective actions to be reviewed and approved by the *competent authority*."

2.7.3. Documentation

- Description of the licensing procedures, where applicable;
- Description of the requirements placed on an organization to whom a licence can be granted;
- Description of the general licensing approach of the competent authority, e.g. prescriptive or performance based;
- Copy of a licence granted to a facility and/or transport.

2.7.4. Review points/specimen questions

- What are the statutory responsibilities of licensees for physical protection?
- What documents regarding physical protection measures should be submitted as part of the licence application? Does this include a security plan?
- Which government organization is empowered to grant licences or authorizations and what are the principal prerequisites for granting such a licence or authorization?
- What are the main requirements regarding physical protection of a licence for each type of nuclear facility or activity?
- Is a licence specific to one facility or can it apply to a site with more than one facility?
- Do licences have restrictions, conditions or time limits for its validity and, if so, what are they? If not, explain the reasons for not having such limits.
- How does the competent authority control any proposed amendments to a licence? What system is in place to ensure that such an amendment receives appropriate consideration and assessment before being implemented?
- Does the competent authority initiate independent analysis, e.g. technical system testing, computer modelling? When is this analysis conducted?
- What physical protection review and assessment is carried out by the competent authority prior to the granting of a licence for the commencement of construction of a nuclear facility?
- Which programme of review and assessment of physical protection is carried out by the competent authority during construction and commissioning of a nuclear facility?
- What types and frequencies of performance testing and evaluations are required from the licensees?

- How does the competent authority review applications/submissions from licensees for modifications during the operational phase of the nuclear facility? Does the competent authority require periodic physical protection reviews during the operation of the nuclear facility? If so, what period of time is allowed between reviews?
- What procedures are in place for approval of modifications to a nuclear facility and/or nuclear material inventory that could affect physical protection systems?
- What are the requirements for the interface and integration of physical protection and nuclear safety?
- Is a comparable system of licensing required for transport? If not, what authorization is required prior to transport of nuclear material? What documentation regarding physical protection is required to be submitted as part of the authorization process?
- What physical protection responsibilities are placed on shippers and carriers?
- Does the transport licensing or authorizing process adequately address the requirements for international transport specified in the CPPNM?
- Are there any other special features that have a bearing on the licensing process?

2.8. COORDINATION WITH OTHER STATE ORGANIZATIONS THAT CONTRIBUTE TO NUCLEAR SECURITY

2.8.1. Objective

- Determine how all the entities involved in physical protection coordinate and cooperate and their awareness of their responsibilities.

2.8.2. Basis

- Nuclear Security Fundamentals, IAEA NSS No. 20: Essential Element 2: Identification and definition of nuclear security responsibilities:

"Nuclear security responsibilities of *competent authorities* designated by the State, as described in Essential Element 3, including *regulatory bodies* and those *competent authorities* related to border control and law enforcement, and responsibilities for all *authorized persons*, are clearly identified and defined. Provisions are identified and defined for appropriate integration and coordination of responsibilities within the *nuclear security regime*, as well as for the State's oversight to ensure the continued appropriateness of the nuclear security responsibilities."

- INFCIRC/225/Rev.5, para. 3.8:

"The State should clearly define and assign physical protection responsibilities within all levels of involved governmental entities including response forces and for *operators* and, if appropriate, carriers. Provision should be made for appropriate integration and coordination of responsibilities within the State's *physical protection regime*. Clear lines of responsibility should be established and recorded between the relevant entities especially where the entity responsible for the armed response is separate from the *operator*."

- INFCIRC/225/Rev.5, para. 3.13:

"The State should ensure that evaluations include exercises to test the *physical protection system*, including the training and readiness of *guards* and/or *response forces*."

- INFCIRC/225/Rev.5, para. 3.40:

"The State should give attention to providing protection measures against any airborne threat and against possible *stand-off attacks* specified in the State's *threat assessment* or *design basis threat*."

- INFCIRC/225/Rev.5, para. 3.58:

"The State should establish a *contingency plan*. The State's *competent authority* should ensure that the *operator* prepares *contingency plans* to effectively counter the *threat assessment* or *design basis threat* taking actions of the *response forces* into consideration."

- INFCIRC/225/Rev.5, para. 3.59:

"The *operator's contingency plan* should be approved by the State's *competent authority* as a part of the security plan."

- INFCIRC/225/Rev.5, para. 3.60:

"The coordination between the *guards* and *response forces* during a *nuclear security event* should be regularly exercised. In addition, other facility personnel should be trained and prepared to act in full coordination with the *guards*, *response forces* and other response teams for implementation of the plans."

- INFCIRC/225/Rev.5, para. 3.61:

"Arrangements should be made to ensure that during emergency conditions and exercises, the effectiveness of the *physical protection system* is maintained."

- INFCIRC/225/Rev.5, para. 3.62:

"The *operator* should initiate its *contingency plan* after detection and assessment of any *malicious act*."

- INFCIRC/225/Rev.5, para. 4.50:

"The State should ensure that its *physical protection* regime includes rapid response and comprehensive measures to locate and recover missing or stolen *nuclear material*. These location and recovery measures should include on-site and off-site operations."

- INFCIRC/225/Rev.5, para. 4.51:

"The State should define the roles and responsibilities of appropriate State response organizations and *operators* to locate and to recover any missing or stolen *nuclear material*."

- INFCIRC/225/Rev.5, para. 4.52:

"The State should ensure that *contingency plans* — including interfaces with safety, as appropriate — are established by *operators* to locate and to recover any missing or stolen *nuclear material*."

- INFCIRC/225/Rev.5, para. 4.53:

"The responsible State organizations should develop *contingency plans* for the rapid location and recovery of *nuclear material* which has been declared missing or stolen from facilities."

- INFCIRC/225/Rev.5, para. 4.54:

"For the coordination of location and recovery operations, the State should develop arrangements and protocols between appropriate State response organizations and *operators*. The arrangements should be clearly documented and this documentation should be made available to all relevant organizations."

- INFCIRC/225/Rev.5, para. 4.55:

"The State should ensure that *operators* and appropriate State response organizations conduct exercises to assess and validate the *contingency plans* and also to train the various participants in how to react in such a situation."

- INFCIRC/225/Rev.5, para. 4.56:

"The State should ensure that *contingency plans* for location and recovery are regularly reviewed and updated."

- INFCIRC/225/Rev.5, para. 5.45:

"The State should define the roles and responsibilities of appropriate State response organizations and *operators* to prevent further damage, secure the *nuclear facility* and protect emergency equipment and personnel."

- INFCIRC/225/Rev.5, para. 5.46:

"The State's *contingency plan* should complement the *contingency plan* prepared by the *operator*."

- INFCIRC/225/Rev.5, para. 5.47:

"The State should ensure that *contingency plans* are established by *operators*."

- INFCIRC/225/Rev.5, para. 5.48:

"The *contingency plans* of the State and of the *operators* should include a description of the objectives, policy and concept of operations for the response to *sabotage* or attempted *sabotage*, and of the structure, authorities and responsibilities for a systematic, coordinated and effective response."

- INFCIRC/225/Rev.5, para. 5.49:

"The State should develop arrangements and protocols among appropriate State response organizations and *operators*, for the coordination of measures for preventing further damage, securing the *nuclear facility* and protecting emergency equipment and personnel. The arrangements should be clearly documented and this documentation should be made available to all relevant organizations."

- INFCIRC/225/Rev.5, para. 5.50:

"The State should ensure that *operators* and appropriate State response organizations conduct exercises to assess and validate the *contingency plans* prepared by the *operators* and the State organizations, and also to train the various participants on how to react in such a situation."

- INFCIRC/225/Rev.5, para. 5.51:

"The State should ensure that *contingency plans* are regularly reviewed and updated."

- INFCIRC/225/Rev.5, para. 5.52:

"The State should ensure that joint exercises, which simultaneously test emergency and *contingency plans* and actions, are regularly carried out in order to assess and validate the adequacy of the interfaces and response coordination of emergency and security organizations involved in responding to various scenarios, and should have a method for incorporating lessons learned to improve both management systems."

- INFCIRC/225/Rev.5, para. 5.53:

"The State should ensure that *response forces* are familiarized with the site and *sabotage* targets and have adequate knowledge of radiation protection to ensure that they are fully prepared to conduct necessary response actions, considering their potential impact on safety."

- INFCIRC/225/Rev.5, para. 6.45:

"The State should ensure that its *physical protection regime* includes rapid response and comprehensive measures to locate and recover missing or stolen *nuclear material* during *transport*."

- INFCIRC/225/Rev.5, para. 6.46:

"The State should define the roles and responsibilities of appropriate State response organizations, carriers and/or other relevant entities to locate and to recover any missing or stolen *nuclear material* that occurs during *transport*."

- INFCIRC/225/Rev.5, para. 6.47:

"The State should ensure that *contingency plans* — including interfaces with safety, as appropriate — are established by carriers and/or other relevant entities to locate and to recover any missing or stolen *nuclear material* that occurs during *transport*."

- INFCIRC/225/Rev.5, para. 6.48:

"The responsible State organizations should develop *contingency plans* for the rapid location and recovery of *nuclear material* which has been declared missing or stolen during *transport*."

- INFCIRC/225/Rev.5, para. 6.49:

"For the coordination of location and recovery operations, the State should develop arrangements and protocols between appropriate State response organizations, carriers and/or other relevant entities. The arrangements should be clearly documented and this documentation should be made available to all relevant organizations."

- INFCIRC/225/Rev.5, para. 6.50:

"The State should ensure that appropriate State response organizations, carriers and/or other relevant entities conduct exercises to assess and validate the *contingency plans* and also to train the various participants on how to react in such a situation."

- INFCIRC/225/Rev.5, para. 6.51:

"The State should ensure that *contingency plans* for location and recovery operations are regularly reviewed and updated."

- INFCIRC/225/Rev.5, para. 6.61:

"The State should define the roles and responsibilities of appropriate State response organizations, carriers and/or other relevant entities to prevent further damage, secure the nuclear *transport* and protect emergency personnel."

- INFCIRC/225/Rev.5, para. 6.62:

"The State should establish a *contingency plan* for *transport* of *nuclear material*. This plan should complement the contingency plan prepared by the carrier and/or other relevant entities."

- INFCIRC/225/Rev.5, para. 6.63:

"The State should ensure that *contingency plans* — including interfaces with safety, as appropriate — are established by carriers and/or other relevant entities."

- INFCIRC/225/Rev.5, para. 6.64:

"The *contingency plans* for *transport* of *nuclear material* of the State, carriers and/or other relevant entities should include a description of the objectives, policy and concept of operations for the response to *sabotage* or attempted *sabotage*, and of the structure, authorities and responsibilities for a systematic, coordinated and effective response."

- INFCIRC/225/Rev.5, para. 6.65:

"The State should develop arrangements and protocols between appropriate State response organizations, carriers and/or other relevant entities for the coordination of measures for preventing further damage, securing the nuclear *transport* and protecting emergency personnel. The arrangements should be clearly documented and this documentation should be made available to all relevant organizations."

- INFCIRC/225/Rev.5, para. 6.66:

"The State should ensure that appropriate State response organizations, carriers and/or other relevant entities conduct exercises to assess and validate the *contingency plans* for *transport* of *nuclear material* and also to train the various participants on how to react in such a situation."

- INFCIRC/225/Rev.5, para. 6.67:

"The State should ensure that *contingency plans* for *transport* of *nuclear material* are regularly reviewed and updated."

- INFCIRC/225/Rev.5, para. 6.68:

"The State should ensure that joint exercises, which simultaneously test emergency and *contingency plans* and actions for *transport* of *nuclear material* are regularly carried out in order to assess and validate the adequacy of the interfaces and response coordination of emergency and security organizations involved in responding to various scenarios, and should have a method for incorporating lessons learned to improve both management systems."

- INFCIRC/225/Rev.5, para. 6.69:

"The State should ensure that *response forces* are familiarized with typical *transport* operations and *sabotage* targets and have adequate knowledge of radiation protection to ensure that they are fully prepared to conduct necessary response actions, considering their potential impact on safety."

2.8.3. Documentation

- A list and description of all organizations with physical protection responsibilities across all levels of governmental entities, including response forces;
- If applicable, instruments such as Memoranda of Agreement that specify requirements for coordination of all organizations with physical protection responsibilities, e.g. all organizations that respond to nuclear security events.

2.8.4. Review points/specimen questions

- How do competent authorities with responsibility for elements of physical protection (such as competent authorities responsible for the security of dangerous goods during transport, trustworthiness checks and licensing of guard forces) coordinate, liaise or consult with each other?
- Which organization coordinates these authorities?
- Which organization is responsible for the investigation of theft of nuclear material, sabotage or threats of sabotage or misuse of nuclear material?
- What is the role of the competent authority in national arrangements to detect and to recover nuclear material out of regulatory control?

- Describe the procedures in place for informing appropriate organizations of the loss/theft, sabotage or threats to sabotage or misuse of nuclear material?
- Describe the procedures that ensure that the competent authorities for physical protection and nuclear material accounting and control activities are coordinated?

2.9. THREAT ASSESSMENT AND DESIGN BASIS THREAT (DBT)

2.9.1. Objective

- Determine if the threats have been adequately assessed and defined in order to design and implement an appropriate physical protection regime and systems.

2.9.2. Basis

- Nuclear Security Fundamentals, IAEA NSS No. 20: Essential Element 7: Identification and Assessment of Nuclear Security Threats:

"A *nuclear security regime* ensures that:

(a) *Nuclear security threats*, both internal and external to the State, are identified and assessed, including their credibility, regardless of whether the *targets* of internal *nuclear security threats* are within or outside the jurisdiction of the State;
(b) The State's assessments of *nuclear security threats* are kept up to date;
(c) The State's assessments are used in implementing the State's *nuclear security regime*."

- CPPNM Amendment, Fundamental Principle G: Threat:

"The State's physical protection should be based on the State's current evaluation of the threat."

- INFCIRC/225/Rev.5, para. 3.10:

"The State should define requirements — based on the *threat assessment* or *design basis threat* — for the physical protection of *nuclear material* in use, in storage, and during *transport,* and for *nuclear facilities* depending on the associated consequences of either *unauthorized removal* or *sabotage*. The State should ensure that the more stringent requirements for physical protection — either those against *unauthorized removal* or those against *sabotage* — are applied."

- INFCIRC/225/Rev.5, para. 3.34:

"The appropriate State authorities, using various credible information sources, should define the *threat* and associated capabilities in the form of a *threat assessment* and, if appropriate, a *design basis threat*. A *design basis threat* is developed from an evaluation by the State of the threat of *unauthorized removal* and of *sabotage*."

- INFCIRC/225/Rev.5, para. 3.35:

"The State should ensure that the *competent authority* has access to information from other organizations in the State on present and foreseeable threats to nuclear activities."

- INFCIRC/225/Rev.5, para. 3.36:

"When considering the *threat*, due attention should be paid to *insiders*. They could take advantage of their access rights, complemented by their authority and knowledge, to bypass dedicated physical protection elements or other provisions, such as safety procedures. The *physical protection system* should be assisted by nuclear material accountancy and control measures to deter and detect the protracted theft of *nuclear material* by an *insider*."

- INFCIRC/225/Rev.5, para. 3.37:

"The State's physical protection requirements for *nuclear material* and *nuclear facilities* should be based on a *design basis threat*, specifically for:

- *Unauthorized removal* of Category I *nuclear material* (defined in Section 4),
- *Sabotage* of *nuclear material* and *nuclear facilities* that has potentially high radiological consequences.

The State should decide whether to use a *threat assessment* or *design basis threat* for other *nuclear material* and *nuclear facilities.*"

- INFCIRC/225/Rev.5, para. 3.38:

"The State's *competent authority* should require the use of a *threat assessment* and/or a *design basis threat* as a common basis for the design and implementation of the *physical protection system* by the *operator*, *shipper* and carrier. The State should consider whether or not the *threat assessment* and/or *design basis threat* are the same for *nuclear facilities* and for *transport*."

- INFCIRC/225/Rev.5, para. 3.39:

"The State should continuously review the *threat* and evaluate the implications of any changes in the *threat assessment* or *design basis threat*. The State's *competent authority* should take steps to ensure that any change is appropriately reflected in the regulations and by the *operator's*, *shipper's* and carrier's *physical protection measures*. Recognizing that a revision of the *design basis threat* may take additional time in this process, short term compensatory *physical protection measures* based on the current *threat assessment* should be implemented. The effectiveness of these measures against the current *threat* should be evaluated. The *design basis threat* should then be reviewed in the light of the revised *threat assessment*."

2.9.3. Documentation

- Relevant sections of the legislation requiring a threat assessment and/or DBT;
- Description of the State authorities responsible for, and that participate in, the State's current evaluation of the threat;
- Description of processes and procedures for defining the threat assessment and/or DBT.

2.9.4. Review points/specimen questions

- Does the State use a threat assessment during the complete life cycle of nuclear facilities, as well as for transports, in implementing the physical protection regime, including licensing?

- Does the State use the same or different threat assessments and/or DBT during different phases of the life cycle for nuclear facilities?
- Is a threat assessment used to develop a DBT? If a DBT is used, how is it developed and to what facilities/transports does it apply?
- Which authorities have responsibility for threat assessment and DBT and which organization coordinates their production?
- How does the competent authority coordinate, liaise or consult with the governmental or other bodies having responsibility for the State's current evaluation of the threat?
- Are there procedures in place for the relevant State authority or authorities to communicate information to the competent authority on the threat to nuclear material and nuclear facilities and transports?
- How is the threat related information disseminated to applicants/operators/carriers?
- What is the process to review or revise the threat assessment or the DBT? When and/or under what conditions is this undertaken?
- Does the DBT include information on adversary numbers, characteristics and capabilities? Does it consider potential insider, cyber, airborne and standoff threats?
- Is the threat assessment or DBT documentation classified? If yes, in which classification level?
- Are there procedures for advising those responsible for physical protection (including during transport) about the threat and significant changes to the threat? Is the transmittal system secure?

2.10. RISK INFORMED APPROACH

2.10.1. Risk management

2.10.1.1. Objective

- Determine how the State's physical protection regime uses a risk management approach to ensure adequate protection of nuclear material.

2.10.1.2. Basis

- Nuclear Security Fundamentals, IAEA NSS No. 20: Essential Element 9: Use of risk informed approaches:

"A *nuclear security regime* uses risk informed approaches, including in the allocation of resources for *nuclear security systems* and *nuclear security measures* and in the conduct of nuclear security related activities that are based on a *graded approach* and *defence in depth,* which take into account the following:

(a) The State's current assessment of the *nuclear security threats*, both internal and external;

(b) The relative attractiveness and vulnerability of identified *targets* to *nuclear security threats*;

(c) Characteristics of the *nuclear material*, *other radioactive material*, *associated facilities* and *associated activities*;

(d) Potential harmful consequences from criminal or intentional unauthorized acts involving or directed at *nuclear material*, *other radioactive material*, *associated facilities*, *associated activities*,

sensitive information or *sensitive information assets*, and other acts determined by the State to have an adverse impact on nuclear security."

- INFCIRC/225/Rev.5, para. 3.41:

"The State should ensure that the State's *physical protection regime* is capable of establishing and maintaining the risk of *unauthorized removal* and *sabotage* at acceptable levels through risk management. This requires assessing the *threat* and the potential consequences of *malicious acts*, and then developing a legislative, regulatory and programmatic framework which ensures appropriate effective *physical protection measures* are put in place."

- INFCIRC/225/Rev.5, para. 3.42:

"Risk can be managed by:

- Reducing the *threat*. The *threat* may be reduced, for example, by the deterrence of robust *physical protection measures*, or through the confidentiality of sensitive information;
- Improving the effectiveness of the *physical protection system*. The *physical protection system's* effectiveness may be increased, for example, by implementing *defence in depth* or establishing and maintaining *nuclear security culture*;
- Reducing the potential consequences of *malicious acts* by modifying specific contributing factors, for example, the amount and type of *nuclear material* and the design of the facility."

2.10.1.3. Documentation

- Examples of risk management strategies and plans by the State;
- Examples of how the State is assessing the threat and the potential consequences of malicious acts.

2.10.1.4. Review points/specimen questions

- Are risk management strategies implemented by the State?
- Are there policies or guidance on acceptable level of risk? If yes, who provides or is responsible for the guidance?
- Are the potential consequences of malicious acts evaluated and used as part of risk management by the State? If yes, which organization is responsible and what is the process?
- What relevant examples exist to illustrate how the State is:
    - Reducing the threat;
    - Improving the effectiveness of the physical protection system;
    - Reducing the potential consequences of malicious acts?

2.10.2. Graded approach

2.10.2.1. Objective

- Determine if the physical protection requirements are commensurate with the threat and the potential consequences of malicious acts.

2.10.2.2. Basis

- CPPNM Amendment, Fundamental Principle H: Graded Approach:

"Physical protection requirements should be based on a graded approach, taking into account the current evaluation of the threat, the relative attractiveness, the nature of the material and potential consequences associated with the unauthorized removal of nuclear material and with the sabotage against nuclear facilities or nuclear material."

- INFCIRC/225/Rev.5, para. 3.43:

"A *graded approach* is used to provide higher levels of protection against events that could result in higher consequences. The State should decide what level of risk is acceptable and what level of protection against the *threat* should be provided."

- INFCIRC/225/Rev.5, para. 3.44:

"For protection against *unauthorized removal*, the State should regulate the categorization of *nuclear material* in order to ensure an appropriate relationship between the *nuclear material* of concern and the *physical protection measures*. For protection against *sabotage*, the State should establish its threshold(s) of *unacceptable radiological consequences* in order to determine appropriate levels of physical protection taking into account existing nuclear safety and radiation protection."

2.10.2.3. Documentation

- Description of the State's decision on the unacceptable level of risk and on the level of protection to be provided:
- Description of the State's categorization of nuclear material and the corresponding physical protection measures:
- Description(s) of the State's threshold of unacceptable radiological consequences for sabotage and any additional grading of radiological consequences for sabotage, and the corresponding physical protection measures.

2.10.2.4. Review points/specimen questions

- Are the physical protection requirements based on a graded approach?

- Does the graded approach take into account the current evaluation of the threat, the relative attractiveness, the nature of the material and the potential consequences associated with the unauthorized removal of nuclear material and with sabotage against nuclear material or nuclear facilities?
- What categorization of nuclear material for unauthorized removal is used by the State?
- What are the graded sets of required protection measures that correspond to the nuclear material categories for unauthorized removal from facilities and during transport?
- What are the State's definition for:
    - Unacceptable radiological consequences;
    - Serious radiological consequences;
    - Other grades of radiological consequences; and
    - How are these determined?
- What are the sets of required protection measures that correspond to the grades of the radiological consequences?

2.10.3. Defence in depth

2.10.3.1. Objective

- Determine whether several layers and methods provide adequate robustness of physical protection systems.

2.10.3.2. Basis

- CPPNM Amendment, Fundamental Principle I: Defence in Depth:

"The State's requirements for physical protection should reflect a concept of several layers and methods of protection (structural or other technical, personnel and organizational) that have to be overcome or circumvented by an adversary in order to achieve his objectives."

- INFCIRC/225/Rev.5, para. 3.45:

"State requirements for physical protection should be based on the concept of *defence in depth*. The concept of physical protection is one which requires a designed mixture of hardware (security devices), procedures (including the organization of *guards* and the performance of their duties) and facility design (including layout)."

- INFCIRC/225/Rev.5, para. 3.46:

"The three physical protection functions of *detection*, delay, and response should each use *defence in depth* and apply a *graded approach* to provide appropriate effective protection."

- INFCIRC/225/Rev.5, para. 3.47:

"*Defence in depth* should take into account the capability of the *physical protection system* and the *system for nuclear material accountancy and control* to protect against *insiders* and external *threats*."

2.10.3.3. Documentation

- Examples of the implementation of defence in depth principle for physical protection, including during transport.

2.10.3.4. Review points/specimen questions

- How are the State's requirements for physical protection, including during transport, based on the concept of defence in depth?
- What do the regulations require regarding defence in depth for the three physical protection functions of detection, delay and response?
- How does the regulatory approach take into account the capability of the physical protection system and the system for nuclear material accountancy and control to protect against insiders and external threats?

2.11. SUSTAINING THE PHYSICAL PROTECTION REGIME

2.11.1. Security culture

2.11.1.1. Objective

- Determine how the State promotes security culture within all relevant organizations and what programme is available for maintaining and enhancing it.

2.11.1.2. Basis

- CPPNM Amendment, Fundamental Principle F: Security Culture:

"All organizations involved in implementing physical protection should give due priority to the security culture, to its development and maintenance necessary to ensure its effective implementation in the entire organization."

- INFCIRC/225/Rev.5, para. 3.48:

"The foundation of *nuclear security culture* should be the recognition that a credible *threat* exists, that preserving nuclear security is important, and that the role of the individual is important."

- INFCIRC/225/Rev.5, para. 3.49:

"The four component groups — the State, organizations, managers in organizations and individuals — should work together to establish and maintain an effective *nuclear security culture*."

- INFCIRC/225/Rev.5, para. 3.50:

"The State should promote a *nuclear security culture* and encourage all security organizations to establish and maintain one. A *nuclear security culture* should be pervasive in all elements of the *physical protection regime*."

- INFCIRC/225/Rev.5, para. 3.51:

"All organizations that have a role in physical protection should make their responsibilities known and understood in a statement of security policy issued by their executive management to demonstrate the management's commitment to provide guidelines to the staff and to set out the organization's security objectives. All personnel should be aware of and regularly educated about physical protection."

2.11.1.3. Documentation

- Copy of the State's statement of security policy as a commitment to security culture;
- Requirements for general security training of managers and employees.

2.11.1.4. Review points/specimen questions

- How do all organizations involved in implementing physical protection, including during transport, give due priority to the security culture, to its development and to the maintenance necessary to ensure its effective implementation in the entire organization?
- Do all personnel recognize that a credible threat exists, that nuclear security is important and that the role of the individual is important to nuclear security?
- How do the State, organizations, managers in organizations, and individuals work together to establish, promote and maintain a nuclear security culture?
- How does the competent authority promote and monitor a nuclear security culture and encourage/require all security organizations, operators and carriers to also establish, promote and maintain a security culture?
- Do all organizations that have a role in physical protection (including during transport) make their responsibilities known and understood in a statement of security policy issued by their executive management to demonstrate the management's commitment to provide guidelines to the staff and to set out the organization's security objectives?
- Are all personnel aware of, and regularly educated/trained in, physical protection?
- What indicators are used to monitor the status of nuclear security culture within the competent authority, operators and carriers?

2.11.2. Quality assurance

2.11.2.1. Objective

- Determine what the State requires regarding quality assurance policies and programmes to ensure physical protection is effective, reliable and sustainable.

2.11.2.2. Basis

- CPPNM Amendment, Fundamental Principle J: Quality Assurance:

"A quality assurance policy and quality assurance programmes should be established and implemented with a view to providing confidence that specified requirements for all activities important to physical protection are satisfied."

- INFCIRC/225/Rev.5, Para. 3.52:

"The quality assurance policy and programmes for physical protection should ensure that a *physical protection system* is designed, implemented, operated and maintained in a condition capable of effectively responding to the *threat assessment* or *design basis threat* and that it meets the State's regulations, including its prescriptive and/or performance based requirements."

2.11.2.3. Documentation

- Descriptions of the State's requirements for quality assurance programmes;
- Examples of quality assurance plans.

2.11.2.4. Review points/specimen questions

- What quality assurance policy and quality assurance programmes are established and implemented by the competent authority, operators and carriers for all important physical protection related activities?
- How do quality assurance policy and quality assurance programmes provide confidence that specified requirements for all activities important to physical protection are satisfied?
- What is the process used to report security events and deviations in procedures implementation and to report experience feedback?

2.11.3. Confidentiality

2.11.3.1. Objective

- Determine what requirements the State has established for the protection of sensitive information and systems containing sensitive information.

2.11.3.2. Basis

- CPPNM Amendment, Fundamental Principle L: Confidentiality:

"The State should establish requirements for protecting the confidentiality of information, the unauthorized disclosure of which could compromise the physical protection of nuclear material and nuclear facilities."

- INFCIRC/225/Rev.5, para. 3.53:

"The State should take steps to ensure appropriate protection of specific or detailed information the unauthorized disclosure of which could compromise the physical protection of *nuclear material* and *nuclear facilities*. It should specify what information needs to be protected and how it should be protected, using a *graded approach*."

- INFCIRC/225/Rev.5, para. 3.54:

"Management of a *physical protection system* should limit access to sensitive information to those whose trustworthiness has been established appropriate to the sensitivity of the information and who need to know it for the performance of their duties. Information addressing possible vulnerabilities in *physical protection systems* should be highly protected."

- INFCIRC/225/Rev.5, para. 3.55:

"Sanctions against persons violating confidentiality should be part of the State's legislative or regulatory system."

2.11.3.3. Documentation

- State requirements for protecting the confidentiality of information, the unauthorized disclosure of which could compromise the physical protection of nuclear material and nuclear facilities;
- State requirements for the determination of personnel trustworthiness.

2.11.3.4. Review points/specimen questions

- What measures are implemented to ensure appropriate protection of sensitive information against unauthorized disclosure, including information stored, used and communicated on computer systems?

- Which documents/regulations/guides detail the types of information that need to be protected and to what level it should be protected?
- What transport related information is identified as sensitive and are there specific requirements for its handling?
- How is the graded approach applied to protection of sensitive information? Does the system of trustworthiness support the graded approach with respect to who is allowed access to different levels of sensitive information?
- Are there protection requirements in place for each level of sensitive information? If so, what are they?
- How is access to sensitive information restricted to those whose trustworthiness has been established, appropriate to the sensitivity of the information, and who need to know it for the performance of their duties?
- To what level is information addressing possible vulnerabilities in physical protection systems required to be protected?
- What sanctions are available, as part of the State's legislative or regulatory regime, against persons violating confidentiality?

2.11.4. Sustainability programme

2.11.4.1. Objective

- Determine if an adequate sustainability programme exists to support the long term viability of the nuclear security regime.

2.11.4.2. Basis

- Nuclear Security Fundamentals, IAEA NSS No. 20: Essential Element 12: Sustaining a Nuclear Security Regime:

"A *nuclear security regime* ensures that each *competent authority* and *authorized person* and other organizations with nuclear security responsibilities contribute to the sustainability of the *regime* by:

(a) Developing, implementing, and maintaining appropriate and effective integrated management systems including quality management systems;

(b) Demonstrating leadership in nuclear security matters at the highest levels;

(c) Developing, fostering and maintaining a robust *nuclear security culture*;

(d) Allocating sufficient human, financial and technical resources to carry out the organization's nuclear security responsibilities on a continuing basis using a risk informed approach;

(e) Routinely conducting maintenance, training, and evaluation to ensure the effectiveness of the *nuclear security systems*;

(f) Having in place processes for using best practices and lessons learned from experience;

(g) Establishing and applying measures to minimize the possibility of *insiders* becoming *nuclear security threats*;

(h) Routinely performing assurance activities to identify and address issues and factors that may affect the capacity to provide adequate nuclear security, including cyber security, at all times."

- INFCIRC/225/Rev.5, para. 3.56:

"The State should establish a sustainability programme to ensure that its *physical protection regime* is sustained and effective in the long term by committing the necessary resources."

- INFCIRC/225/Rev.5, para. 3.57:

"*Operator*s, *shippers* and carriers should establish sustainability programmes for their *physical protection system*. Sustainability programmes should encompass:

- Operating procedures (instructions).
- Human resource management and training.
- Equipment updating, maintenance, repair and calibration.
- *Performance testing* and operational monitoring.
- Configuration management (the process of identifying and documenting the characteristics of a facility's *physical protection system* — including computer systems and software — and of ensuring that changes to these characteristics are properly developed, assessed, approved, issued, implemented, verified, recorded and incorporated into the facility documentation).
- Resource allocation and operational cost analysis."

2.11.4.3. Documentation

- State's sustainability programme to ensure its physical protection regime is effective in the long term by committing the necessary resources.

2.11.4.4. Review points/specimen questions

- Does the State have a sustainability programme for the national physical protection regime and what does it address?
- What are the State requirements for operators and carriers to establish and maintain a sustainability programme and how is this programme monitored?

2.12. PLANNING AND PREPAREDNESS FOR AND RESPONSE TO NUCLEAR SECURITY EVENTS

2.12.1. Objective

- Determine if contingency plans exist and if they are regularly reviewed, updated, exercised and interfaced with the emergency plans.

2.12.2. Basis

- Nuclear Security Fundamentals, IAEA NSS No. 20: Essential Element 11: Planning for, preparedness for, and response to, a nuclear security event

"A *nuclear security regime* ensures that relevant *competent authorities* and *authorized persons* are prepared to respond, and respond appropriately, at local, national, and international levels to *nuclear security events* by:

(a) Developing arrangements and response plans for ensuring:

(i) Rapid and effective mobilization of resources in response to a *nuclear security event*;

(ii) Effective coordination and cooperation during response to a *nuclear security event* among all those carrying out response functions (including intelligence, law enforcement, crime scene investigation, and nuclear forensics) and between the security and safety aspects of the response;

(iii) Effective use of relevant international emergency assistance and response systems;

(iv) Investigation of any nuclear security event and, as appropriate, prosecution or extradition of alleged offenders.

(b) Periodically exercising, testing, and evaluating the plans for effectiveness by relevant *competent authorities* and *authorized persons* with the aim of ensuring timely implementation of comprehensive measures to:

(i) Mitigate and minimize harmful consequences to persons, property, society, and the environment from *nuclear security events*;

(ii) Locate, recover, and secure *nuclear material* and *other radioactive material* that is out of *regulatory control*;

(iii) Feedback into the preparedness process, including into the response plans, the results of exercises and tests of the plans, and of experience."

- CPPNM Amendment, Fundamental Principle K: Contingency Plans:

"Contingency (emergency) plans to respond to unauthorized removal of nuclear material or sabotage of nuclear facilities or nuclear material, or attempts thereof, should be prepared and appropriately exercised by all licence holders and authorities concerned."

- INFCIRC/225/Rev.5, para. 3.58:

"The State should establish a *contingency plan*. The State's *competent authority* should ensure that the *operator* prepares *contingency plans* to effectively counter the *threat assessment* or *design basis threat* taking actions of the *response forces* into consideration."

- INFCIRC/225/Rev.5, para. 3.59:

"The *operator's contingency plan* should be approved by the State's *competent authority* as a part of the security plan."

- INFCIRC/225/Rev.5, para. 6.46:

"The State should define the roles and responsibilities of appropriate State response organizations, carriers and/or other relevant entities to locate and to recover any missing or stolen *nuclear material* that occurs during *transport*."

- INFCIRC/225/Rev.5, para. 6.47:

"The State should ensure that *contingency plans* — including interfaces with safety, as appropriate — are established by carriers and/or other relevant entities to locate and to recover any missing or stolen *nuclear material* that occurs during *transport*."

- INFCIRC/225/Rev.5, para. 6.49:

"For the coordination of location and recovery operations, the State should develop arrangements and protocols between appropriate State response organizations, carriers and/or other relevant entities. The arrangements should be clearly documented and this documentation should be made available to all relevant organizations."

- INFCIRC/225/Rev.5, para. 6.51:

"The State should ensure that *contingency plans* for location and recovery operations are regularly reviewed and updated."

- INFCIRC/225/Rev.5, para. 6.69:

"The State should ensure that *response forces* are familiarized with typical *transport* operations and *sabotage* targets and have adequate knowledge of radiation protection to ensure that they are fully prepared to conduct necessary response actions, considering their potential impact on safety."

2.12.3. Documentation

- List and table of contents of contingency plans.

2.12.4. Review points/specimen questions

- Which organizations are responsible for providing internal and external responses to a security event at facilities and during transport?
- Which organization is responsible for coordinating the above response?
- How do these response forces react to such events and how are they authorized?
- Are there different levels of security plans and how are they tested and maintained?
- How is testing carried out on the interfaces between the different organizations involved in the case of a security event and the roles/limits of them (how they work together and coordinate their efforts)?
- What topics are addressed in the contingency plans for response to security events?
- How are these plans interfaced/integrated with the emergency plans of other bodies and of operators/carriers?
- How is the effectiveness of physical protection systems maintained during emergency conditions and exercises?
- Are there different levels of exercises and what are their goals, what is the process for experience feedback and the associated corrective/improvement plan/actions?
- Describe a nuclear security event response exercise:
    - When was the last exercise conducted?
    - What was its scope?
    - Which organizations were involved?
    - What were the lessons learned?
- What is the process used to update/modify the contingency plans?

3. NUCLEAR FACILITY REVIEW (MODULE 2)

3.1. INTRODUCTION

The IPPAS nuclear facility review mission is a comprehensive review of a physical protection system, as it exists at a nuclear facility, e.g. a nuclear power plant or a nuclear research facility. The review provides the host country with an independent assessment of the status of physical protection at nuclear facilities selected by the State and provides advice to assist the State in the form of recommendations, suggestions and the recognition of good practices based on accepted international criteria and practice. This review, conducted by an IPPAS team, does not replace the regulatory compliance function of the State's competent authority.

The objectives of the nuclear facility review are to:

- Provide an independent assessment of a selected facility's physical protection system as agreed to by the IAEA and the host country;
- Provide advice to the host country (competent authority) in the form of recommendations, suggestions and the recognition of good practices;
- Share experience on the conduct of a detailed physical protection assessment;
- Provide a basis for assistance to the host country in implementing upgrades.

The facility review evaluates a facility's physical protection system and seeks to answer the following questions:

- Does the physical protection system correspond to international instruments and IAEA recommendations and guidance?
- Does the physical protection system function as designed?
- Does the physical protection system appear adequate to counter the State's DBT or current threat assessment, in accordance with information available to the IPPAS team?
- Is the facility's security organization sufficiently staffed, trained and equipped to carry out its assigned responsibilities?
- Is the system well maintained?

An IPPAS mission provides an expert qualitative judgement of the effectiveness of a facility's physical protection system. Conversely, an IPPAS mission does not have access to all necessary information or the time to conduct a quantitative evaluation of the effectiveness of the physical protection system or nuclear material accountancy and control system.

This module focuses on the facility but may involve meetings with representatives of the competent authority and other organizations that have related responsibilities in the physical protection of nuclear facilities and nuclear material. The IPPAS national review module is the recommended starting point for

host countries that wish to have their nuclear security regime reviewed against international instruments and guidance.

3.2. PURPOSE

The purpose of this module is to provide guidelines for IPPAS team members in the conduct of a facility review mission. The review points/specimen questions should not be used as a simple yes/no checklist but rather as questions which allow the interviewer to gain an appreciation of the subject and, as appropriate, to compare implementation with international instruments and IAEA recommendations and guidance. The guidance provided in this publication can be used by a host country to conduct a self-assessment of its own physical protection requirements implementation against accepted international criteria and good practice.

3.3. MISSION SCOPE

The scope of the mission should be tailored to accommodate the particular concerns of the host country. The mission can assess a facility's overall physical protection system or, at the direction of the host country, concentrate on those particular systems that have been identified by the host country.

A facility review may address the following areas:

- Security management programme:
    - Threat and target identification;
    - Security plan, including contingency plan;
    - Interfaces with nuclear material accountancy and control and nuclear safety;
    - Security organization;
    - Security staff training and qualifications;
    - Security culture;
    - Confidentiality;
    - Computer security;
    - Trustworthiness;
    - Security procedures;
    - Reporting of nuclear security events;
    - System evaluation, including performance testing;
    - Quality assurance;
    - Sustainability programme (including operating procedures, training, equipment maintenance, configuration management and resource allocation).

- Physical protection system:

    Detection:

    - Access control;
    - Intrusion detection;
    - Alarm assessment;
    - Central alarm station;
    - Emergency power.

Delay:

- Protected area barriers;
- Inner area barriers;
- Vital area barriers.

Response:

- Guards and response forces;
- Response communications system;
- Equipment, armament and transportation.

3.4. GENERAL GUIDANCE FOR IPPAS MISSION MEMBERS

3.4.1. Review of nuclear facility operations

Before commencing a review of the physical protection systems for either nuclear reactors or for fuel cycle facilities, IPPAS mission members are advised to acquire a good appreciation of the specific facilities to be reviewed during the mission. An IPPAS team needs to include some members familiar with the type of nuclear facility being reviewed, as the risks of theft and sabotage will vary from one part of the facility to another and across different facilities and hence the nature and level of physical protection will vary.

The following sections are intended to give a short summary of some of the security related characteristics of nuclear material, nuclear power plants, research reactors and fuel cycle facilities.

Nuclear material is widely used to produce radiation and energy. The safe use of nuclear material requires the control of criticality, the removal of produced energy (heat) and the containment of the irradiated nuclear material and fission products. If the loss of these functions will result in unacceptable radiological consequences, then physical protection measures against sabotage should be provided. The potential consequences of sabotage depend on the type of facility and the kind of nuclear fuel/material in use.

Some nuclear material can be used in a radiological dispersion device or as an improvised nuclear device. The vulnerability to theft depends very much on the type of facility, the type of nuclear material, its size, its weight and its radiation and should be evaluated for all nuclear activities.

The size and complexity of many nuclear facilities and the radiation protection measures required for access to these facilities means that time management is an important consideration when planning and conducting walk downs at nuclear facilities.

3.4.2. Nuclear power plants

Nuclear power plants, which are of varied types and design, are large complex facilities with a range of sizes depending on the number of reactor units at one location, e.g. from one to eight reactors at a site, where employee numbers can vary from several hundred to several thousand. A facility site generally comprises a main powerhouse (possibly a number of separate powerhouse buildings, depending on the number and design of the reactors), which contains, among many other things: the reactor(s); reactor containment; turbine hall containing turbines and electrical generators, which are cooled often by

hydrogen, and high energy steam lines; fresh fuel storage; spent (irradiated) fuel wet storage; and the facility's control room and secondary control room. Often located in separate buildings or at other locations within the facility's site are the reactor's intake water pumping facilities, administration and maintenance functions, emergency backup generators with fuel storage in either above ground or in-ground tanks, spent fuel dry storage, station transformers and electrical switchyard. One of the mitigating features is the many redundancies built-in for safety purposes.

The threat against a nuclear power plant includes theft of nuclear fuel and sabotage that could endanger the health and safety of personnel, the public and the environment by exposure to radiation or from the release of radioactive substances. The fresh (new) fuel, depending on the type of reactor, generally ranges from natural uranium to low enriched uranium (LEU) of up to 5% U-235 enrichment or mixed oxide (MOX) fuel containing a mixture of LEU and Pu. The spent (irradiated) fuel containing small quantities of plutonium and fission products is mostly highly irradiated.

3.4.3. Nuclear research facilities

There is a wide range of research reactors around the world. These reactors are designed primarily to supply neutrons or gamma radiation for experimental purposes. They may also be used for training, materials testing and production of radioactive isotopes.

Site location and size of research reactor facilities can vary significantly, e.g. from the university campus to an industrial park to a large research complex facility devoted exclusively to nuclear research and the production of radioactive isotopes. Often, because of the location of research reactors near population centres and on university campuses, nuclear research facilities, including separate but related laboratories, take on a campus-like appearance and atmosphere. Under such circumstances, security often comes into conflict with the openness that is desired for education and experimentation.

Some types of research reactor are:

- Training reactors, which are found typically at universities and other training centres. Often, these reactors are pool type and are cooled by natural convection of water through the reactor core. Power levels range up to 150 kW. An example of a test and training reactor is the TRIGA reactor.

- Medium flux test reactors include large, graphite moderated, LEU reactors, several heavy water moderated reactor designs, and pool or tank type designs with high enriched uranium (HEU) fuel in a compact core. Power levels in these reactors vary from a few tens of kilowatts to 10 MW.

- High flux reactors, usually a pool or tank type, are used to test reactor components and in other material science irradiation studies. These reactors are also used for transuranic isotope production.

- Pulsed reactors are utilized for testing that requires very high neutron flux. Fuel for these reactors is generally HEU.

Nuclear and other radioactive material at a research reactor are typically contained in seven different areas:

(i) Isotope target and product storage area;
(ii) Fresh (new) fuel storage areas;
(iii) Reactor cores;
(iv) Spent fuel storage pools/tanks;
(v) Spent fuel shipping casks;
(vi) Radioactive experiment areas (laboratories);
(vii) Radioactive waste storage areas.

Enrichment levels for research reactor fresh fuel vary from natural uranium to HEU. Fuel element configurations vary from flat plate designs to cylindrical rods in a multitude of matrices and claddings. Many research reactor fuel elements are relatively small and light.

Although acts of sabotage or theft could be directed against any of these types of radioactive material, their attractiveness as targets depends on the adversary's objective, technical ability and resources, as well as the accessibility, physical form, chemical composition, quantity, radiation level and toxicity of the material contained in each type of radioactive material.

The hazards to the public of being exposed to radioactive material at a research reactor can take two forms: (i) theft for purposes of extortion or creating a nuclear explosive device and (ii) internal or external radiation damage resulting from dispersed or hidden radioactive material. Dispersal of radioactive material could be accomplished either by theft of radioactive material from a reactor facility and release of the material at some other location or by sabotage of the facility in such a way that the material is released directly.

3.4.4. Fuel cycle facilities

Fuel cycle facilities are large and complex, with large quantities of nuclear material in different forms and locations. Effective management of nuclear material at such facilities is critical to ensuring that it is appropriately controlled, accounted for and protected at the various locations where it is held and during movement between these locations. Collection of information about material management procedures is therefore of equal importance during a review of these facilities as viewing the physical protection measures in place during a walk down.

3.4.5. Conversion facilities

These facilities may be co-located with an enrichment or fuel fabrication facility. They convert natural uranium into uranium hexafluoride and reconvert enriched/depleted uranium hexafluoride to uranium oxide. The material is of low radioactivity but may be chemotoxic.

3.4.6. Enrichment facilities

Nuclear material, normally in the form of natural uranium hexafluoride (sludge), is introduced into the facility, heated until gaseous and circulated through diffusers or centrifuges until the required enrichment level is achieved, i.e. typically 4% enriched for nuclear power plants, 19.5% for research reactors or HEU for research/naval reactors. The process also results in the separation of depleted uranium. Both forms of material are then packaged into separate transport flasks. The enriched uranium hexafluoride is then shipped to a conversion facility while the depleted uranium may remain at the facility.

3.4.7. Fuel fabrication facilities

Nuclear material in the form of oxide is manufactured into fuel pellets which are then inserted in fuel rods, a number of which are then used to make a complete fuel assembly for dispatch to reactors. Strict quality requirements often result in some fuel being discarded and stored as scrap. The nuclear material used can vary considerably depending upon the type of reactor, e.g. fast breeder, nuclear power plant using MOX, LEU or natural uranium and research/naval reactors using either HEU or LEU (typically 19.5%) fuel. The risk associated with such facilities is primarily one of theft (especially of fuel pellets because of their small size and low level of radioactivity), although the 'attractiveness' of the nuclear material differs considerably.

3.4.8. Interim spent fuel storage

The spent (irradiated) nuclear fuel is stored either in a water pond or in dry storage in casks while awaiting reprocessing or final disposal, depending of the national policy of the respective State. The storages contain large inventories of irradiated nuclear material and are potentially vulnerable to sabotage. Since the spent fuel is typically highly radioactive, it is less attractive to theft.

3.4.9. Reprocessing facilities

Nuclear material in the form of irradiated fuel is initially stored in ponds. During reprocessing, it is removed from the ponds and the fuel cladding removed, after which it is transferred to intermediate level waste (ILW) stores. It then moves through the heavily shielded chemical separation area, emerging in three separate material streams: plutonium nitrate, uranyl nitrate and fission products in the form of liquid high level waste (HLW). The nitrates are converted to oxides and dispatched to separate stores. The liquid HLW is vitrified and stored.

3.5. FACILITY PHYSICAL PROTECTION SYSTEM REVIEW PROCESS

For conducting a facility assessment, the IPPAS mission team should be familiar with the following information (taking into consideration sensitivity and availability of information):

- The host country's physical protection regime, including its physical protection regulations;
- Familiarity of the host country's assessment of the threat and/or DBT;
- The type and quantity of nuclear material held at the facility and, as necessary, information on its location(s);
- The facility's security plan or physical protection approach, which outlines how physical protection is achieved; and
- The facility's risk assessment.

Whereas the review of the facility management programme to a large degree will be based on documentation and interviews with appropriate facility staff, the review of areas of detection, delay and response requires more information on the practical implementation of physical protection measures. A facility walk down combined with an information session provided by the facility operator is invaluable in this regard. IPPAS members should not hesitate to ask questions of the host country's representatives to gain a clear understanding of the operation.

The following sections are intended to give a summary of the specific objectives and bases of the physical protection requirements for distinct fields of the physical protection system and examples of possible data to be collected from documents and interviews in the review process.

3.6. SECURITY MANAGEMENT PROGRAMME

3.6.1. Threat and target identification

3.6.1.1. Objective

- Determine if the threat and targets have been adequately defined and assessed to determine appropriate physical protection arrangements.
-

3.6.1.2. Basis

- CPPNM Amendment, Fundamental Principle G: Threat:

"The State's physical protection should be based on the State's current evaluation of the threat."

- CPPNM Amendment, Fundamental Principle H: Graded Approach:

"Physical protection requirements should be based on a graded approach, taking into account the current evaluation of the threat, the relative attractiveness, the nature of the material and potential consequences associated with the unauthorized removal of nuclear material and with the sabotage against nuclear facilities or nuclear material."

- INFCIRC/225/Rev.5, para. 3.38:

"The State's *competent authority* should require the use of a *threat assessment* and/or a *design basis threat* as a common basis for the design and implementation of the *physical protection system* by the *operator*, *shipper* and carrier. The State should consider whether or not the *threat assessment* and/or *design basis threat* are the same for *nuclear facilities* and for *transport*."

- INFCIRC/225/Rev.5, para. 4.5:

"The primary factor in determining the *physical protection measures* against *unauthorized removal* is the *nuclear material* itself. Table 1 of IAEA NSS No. 13 categorizes the different types of *nuclear material* in terms of element, isotope, quantity and irradiation. This categorization is the basis for a *graded approach* for protection against *unauthorized removal* of *nuclear material* that could be used in a nuclear explosive device, which itself depends on the type of *nuclear material* (e.g. plutonium and uranium), isotopic composition (i.e. content of fissile isotopes), physical and chemical form, degree of dilution, radiation level, and quantity."

- INFCIRC/225/Rev.5, para. 4.7:

"*Nuclear material*, which is in a form that is no longer usable for any nuclear activity, minimizes environmental dispersal and is practicably irrecoverable, may be protected against *unauthorized removal* in accordance with prudent management practice."

- INFCIRC/225/Rev.5, para. 4.8:

"In determining the levels of physical protection in a facility, which may consist of several buildings, the *operator* may identify, in agreement with the State's *competent authority*, part of the *nuclear facility* which contains *nuclear material* of a different category and which is therefore protected at a different level than the rest of the *nuclear facility*. Conversely, consideration may need to be given to adding together the total amount of *nuclear material* contained in a number of buildings to determine the appropriate protection arrangements for this group of buildings."

- INFCIRC/225/Rev.5, paras 4.9 and 5.17:

"The *physical protection system* of a *nuclear facility* should be integrated and effective against both *sabotage* and *unauthorized removal*."

- INFCIRC/225/Rev.5, para. 5.4:

"For each *nuclear facility*, an analysis, validated by the *competent authority*, should be performed to determine whether the radioactive inventory has the potential to result in *unacceptable radiological consequences* as determined by the State, assuming that the *sabotage* acts will be successfully completed while ignoring the impact of the physical protection or mitigation measures."

- INFCIRC/225/Rev.5, para. 5.7:

"If the potential radiological consequences of *sabotage* are less severe than the *unacceptable radiological consequences* defined by the State, then the *operator* should still protect safety related equipment and devices by controlling access to them and securing them."

- INFCIRC/225/Rev.5, para. 5.8:

"If the potential radiological consequences of *sabotage* exceed the State's *unacceptable radiological consequences*, then the *operator* should identify equipment, systems or devices, or *nuclear material*, the *sabotage* of which could directly or indirectly lead to this condition as potential sabotage targets and protect them in accordance with the following design process (INFCIRC/225/Rev.5, paras 5.9–5.19) and protection requirements (INFCIRC/225/Rev.5, paras 5.20–5.43). The results of safety analysis provide useful input, including target identification and potential radiological consequences, and should be considered during design of the *physical protection system*."

- INFCIRC/225/Rev.5, para. 5.9:

"Using the *threat assessment* or *design basis threat*, the *operator* — in cooperation with the State's *competent authority* — should define credible scenarios by which adversaries could carry out *sabotage* of *nuclear facilities* and *nuclear material*."

- INFCIRC/225/Rev.5, para. 5.10:

"When defining scenarios, the *operator* should consider the location of the *nuclear facility* and all *nuclear material* and *other radioactive material*, including radioactive waste, especially those at the same location inside a *nuclear facility*."

- INFCIRC/225/Rev.5, para. 5.11:

"*Sabotage* scenarios should consider external and/or *insider* adversaries who attempt to disperse *nuclear material* or *other radioactive material* or to damage or interfere with equipment, systems, structures, components or devices, including possible *stand-off attack*, consistent with the State's *threat assessment* or *design basis threat.*"

- INFCIRC/225/Rev.5, para. 5.12:

"The *operator* should design a *physical protection system* that is effective against the defined *sabotage* scenarios and complies with the required level of protection for the *nuclear facility* and *nuclear material*."

- INFCIRC/225/Rev.5, para. 5.15:

"The *operator* should evaluate and the *competent authority* should validate the design of *physical protection system* effectiveness to verify that it complies with the required level of protection for the *nuclear facility* and *nuclear material*."

3.6.1.3. Documentation/information

- Nuclear material categories and, as appropriate, locations;
- Sabotage approach to define targets and vital areas;
- Main assumptions taken into account for the threat assessment and/or DBT.

3.6.1.4. Review points/specimen questions

Determine if:

- The operator has been provided a nuclear material categorization table for protection against theft, thresholds of unacceptable radiological consequences and a threat assessment/DBT by the State.
- The facility has identified all theft targets, including Categories I, II and III nuclear material, their quantity, size and form, and their location within the facility.
- The operator has identified the radiological product inventory, equipment, systems or devices, or nuclear material, of which sabotage could directly or indirectly lead to potential radiological consequences exceeding the State's definition of unacceptable radiological consequences.
- The facility has identified high consequence targets that require protection in a vital area, taking into account safety studies.

- The operators have used the State's threat assessment and/or DBT in the design and implementation of the facility's physical protection system.
- Consideration was given to the various types of adversary, i.e. outsiders, insiders and outsiders in collusion with insiders, motivations, capabilities, scenarios and tactics that an adversary might use to conduct radiological sabotage and/or nuclear material theft.
- The facility has considered the possibility of a local threat in addition to the State defined DBT, recognizing the likelihood of the threat occurring at the facility.

3.6.2. Security plan, including contingency plan

3.6.2.1. Objectives

- To determine if an appropriate security plan exists, what it encompasses, and how it is implemented, maintained and kept up to date.
- To determine if a contingency plan exists and covers response actions to all foreseeable security events and whether it is regularly reviewed, updated, exercised and complements the emergency plan.

3.6.2.2. Basis

- CPPNM Amendment, Fundamental Principle K: Contingency Plans:

"Contingency (emergency) plans to respond to unauthorized removal of nuclear material or sabotage of nuclear facilities or nuclear material, or attempts thereof, should be prepared and appropriately exercised by all licence holders and authorities concerned."

- INFCIRC/225/Rev.5, para. 3.27:

"The *operator* should prepare a security plan as part of its application to obtain a licence. The security plan should be based on the *threat assessment* or the *design basis threat* and should include sections dealing with design, evaluation, implementation, and maintenance of the *physical protection system*, and *contingency plan*s. The *competent authority* should review and approve the security plan, the implementation of which should then be part of the licence conditions. The *operator* should implement the approved security plan. The *operator* should review the security plan regularly to ensure it remains up to date with the current operating conditions and the *physical protection system*. The *operator* should submit an amendment to the security plan for prior approval by the *competent authority* before making significant modifications, including temporary changes, to arrangements detailed in the approved security plan. The *competent authority* should verify the *operator*'*s* compliance with the security plan."

- INFCIRC/225/Rev.5, para. 3.58:

"The State should establish a *contingency plan*. The State's *competent authority* should ensure that the *operator* prepares *contingency plans* to effectively counter the *threat assessment* or *design basis threat* taking actions of the *response forces* into consideration."

- INFCIRC/225/Rev.5, para. 3.59:

"The *operator's contingency plan* should be approved by the State's *competent authority as* a part of the security plan."

- INFCIRC/225/Rev.5, para. 3.62:

"The *operator* should initiate its *contingency plan* after *detection* and assessment of any *malicious act*.

- INFCIRC/225/Rev.5, paras 4.19 and 5.42:

"*Contingency plans* should be prepared to counter *malicious acts* effectively and to provide for appropriate response by *guards* or *response forces*. Such plans should also provide for the training of facility personnel in their actions."

- INFCIRC/225/Rev.5, Para. 5.44:

"These plans *(the emergency plan and the contingency plan)* should be comprehensive and complementary."

- INFCIRC/225/Rev.5, para. 4.49 (for Category I nuclear material only):

"*Guards* and *response forces* should provide an effective and timely response to prevent an adversary from completing the *unauthorized removal*. At least annually, *performance testing* of the *physical protection system* should include appropriate exercises, for example *force-on-force exercises*, to determine if the *guards* and the *response forces* can reach this objective."

- INFCIRC/225/Rev.5, para. 4.60:

"The *operator's* measures to locate and recover missing or stolen *nuclear material* should be included in its contingency plan..."

3.6.2.3. Documentation

- Security plan, including contingency plan, or at least a table of contents of a security plan;
- Procedure on plant configuration management and documentation as regards physical protection system;
- Emergency plan;
- Chain of command procedures;
- Exercise outcome reports/records;
- Emergency/contingency records.

3.6.2.4. Review points/specimen questions

Determine if:

- A security plan approved by the competent authority exists.
- The security plan provides a comprehensive description of the physical protection system, including sections dealing with, for example, roles and responsibilities, design, evaluation, maintenance of the physical protection system and contingency plans.
- The security plan is implemented by the operator.
- The security plan is reviewed regularly to ensure it remains up to date with the current operating conditions and guidelines for the physical protection system.
- The operator submits changes to the security plan for prior approval by the competent authority before making significant modifications, including temporary changes, to arrangements detailed in the approved security plan.

Determine if:

- Contingency plan is developed to cover response to unauthorized removal of nuclear material or sabotage of nuclear facilities or nuclear material, including recovery and mitigation measures.
- Contingency plan is routinely reviewed and updated, as necessary.

3.6.3. Interfaces with nuclear material accountancy and control and nuclear safety

3.6.3.1. Objective

- To determine what the interface is between physical protection and other critical infrastructure of the operator's organization, specifically nuclear material accountancy and control and nuclear safety.

3.6.3.2. Basis

- INFCIRC/225/Rev.5, para. 3.26:

"The *operator* should ensure control of, and be able to account for, all *nuclear material* at a *nuclear facility* at all times. The *operator* should report any confirmed accounting discrepancy in a timely manner as stipulated by the *competent authority*."

- INFCIRC/225/Rev.5, paras 4.11 and 5.18:

"The *operator* should assess and manage the physical protection interface with safety and nuclear material accountancy and control activities in a manner to ensure that they do not adversely affect each other and that, to the degree possible, they are mutually supportive."

- INFCIRC/225/Rev.5, para. 5.13:

"The *physical protection system* against *sabotage* should be designed as an element of an integrated system to prevent the potential consequences of *sabotage* by taking into account the robustness of the

engineered safety and operational features, and the fire protection, radiation protection and emergency preparedness measures."

3.6.3.3. Documentation

- Security plan;
- Nuclear material accountancy and control plan;
- Nuclear safety programme plan;
- Facility configuration and control management plan;
- Relevant meeting records between security and safety organizations.

3.6.3.4. Review points/specimen questions

Determine if:

- The operator ensures control of, and is able to account for, all nuclear material at the nuclear facility at all times.
- The operator reports any confirmed accounting discrepancy in a timely manner, as stipulated by the competent authority.
- Nuclear material accountancy and control and security measures complement each other.
- Nuclear safety and security measures complement each other.
- Any safety–security issues have occurred and how they were resolved.

3.6.4. Security organization

3.6.4.1. Objective

- To determine if the security organization structure and management system are adequate to establish, operate and maintain a physical protection system.

3.6.4.2. Basis

- CPPNM Amendment, Fundamental Principle E: Responsibility of the Licence Holders:

"The responsibilities for implementing the various elements of physical protection within a State should be clearly identified. The State should ensure that the prime responsibility for the implementation of physical protection of nuclear material or of nuclear facilities rests with the holders of the relevant licences or of other authorizing documents (e.g. operators or shippers)."

- INFCIRC/225/Rev.5, para. 3.24:

"The *operator*, *shipper* and carrier should comply with all applicable regulations and requirements established by the State and the *competent authority*."

- INFCIRC/225/Rev.5, para. 3.25:

"The *operator*, *shipper* and carrier should cooperate and coordinate with all other State entities having physical protection responsibilities, such as off-site *response forces*."

- INFCIRC/225/Rev.5, para. 3.26:

"The *operator* should ensure control of, and be able to account for, all *nuclear material* at a *nuclear facility* at all times. The *operator* should report any confirmed accounting discrepancy in a timely manner as stipulated by the *competent authority*."

3.6.4.3 Documentation

- Organizational diagram/chart;
- Job descriptions;
- Staffing plan;
- Risk management plans, registers and policy/procedures;
- Management team meeting agenda and minutes.

3.6.4.4. Review points/specimen questions

Determine if:

- A single person has been assigned as the facility security manager.
- The facility security manager reports directly to, and has direct access to, the facility manager.
- The security manager has sufficient authority to manage the security programme effectively.
- The responsibilities of security management and staff are clearly defined and understood for both normal operations and during security events, including other emergency situations.
- All security staff are held accountable for assigned responsibilities.
- At least one full-time member of the security organization who has the authority to direct security activities of the organization is on-site at all times.
- The number of security staff on duty complies with staffing requirements, including minimum requirements for both normal operations and during security events and for other emergency situations identified in the security plan.

- All security activities are based on established procedures that include traceability and are part of the facility management system.
- Security staff are responsible for activities that conflict with their responsibility to protect the facility assets.
- Security event logs are maintained and are regularly reviewed by supervisors.

3.6.5. Security staff training and qualifications

3.6.5.1. Objective

- Determine if security staff have the knowledge, abilities and skills to protect the facility against radiological sabotage or unauthorized removal of nuclear material.

3.6.5.2. Basis

- INFCIRC 225/Rev.5, para. 3.57:

"*Operators*, *shippers* and carriers should establish sustainability programmes for their *physical protection system.* Sustainability programmes should encompass:

- Operating procedures (instructions).
- Human resource management and training.
- Equipment updating, maintenance, repair and calibration.
- *Performance testing* and operational monitoring.
- Configuration management (the process of identifying and documenting the characteristics of a facility's *physical protection system* — including computer systems and software — and of ensuring that changes to these characteristics are properly developed, assessed, approved, issued, implemented, verified, recorded and incorporated into the facility documentation).
- Resource allocation and operational cost analysis."

- INFCIRC 225/Rev.5, para. 4.33:

"A 24 hour guarding service and *response forces* should be provided to counter effectively any attempted *unauthorized removal*. The *central alarm station* personnel and off-site *response forces* should communicate at scheduled intervals. The *guards* and *response forces* should be trained and adequately equipped for their functions in accordance with national laws and regulations."

- INFCIRC 225/Rev.5, para. 5.39:

"A 24 hour guarding service and *response forces* should be provided to ensure an adequate and timely response to prevent an adversary from completing an act of *sabotage*. The *central alarm station* personnel and off-site

response forces should communicate at scheduled intervals. The *guards* and *response forces* should be trained and adequately equipped for their function in accordance with national laws and regulations."

3.6.5.3. Documentation

- Training programme;
- Training materials;
- Training records;
- Security staff performance review process.

3.6.5.4. Review points/specimen questions

Determine if and how:

- There is a fitness-for-duty programme.
- Security personnel meet the academic, physical and mental health fitness required for their assigned functions.
- There is an adequate defined training programme which is an on-going process for security personnel.
- Security personnel are trained and qualified to perform all their assigned physical protection related tasks and duties.
- Training and standards records exist, are current, and that personnel training and standards are maintained.

3.6.6. Security culture

3.6.6.1. Objective

- Determine what security culture exists within the organization and what programme is available for maintaining and enhancing it.

3.6.6.2. Basis

- CPPNM Amendment, Fundamental Principle F: Security Culture:

"All organizations involved in implementing physical protection should give due priority to the security culture, to its development and maintenance necessary to ensure its effective implementation in the entire organization."

- INFCIRC/225/Rev.5, para. 3.48:

"The foundation of *nuclear security culture* should be the recognition that a credible *threat* exists, that preserving nuclear security is important, and that the role of the individual is important."

- INFCIRC/225/Rev.5, para. 3.49:

"The four component groups — the State, organizations, managers in organizations and individuals — should work together to establish and maintain an effective *nuclear security culture*."

- INFCIRC/225/Rev.5, para. 3.50:

"The State should promote a *nuclear security culture* and encourage all security organizations to establish and maintain one. A *nuclear security culture* should be pervasive in all elements of the *physical protection regime*."

- INFCIRC/225/Rev.5, para. 3.51:

"All organizations that have a role in physical protection should make their responsibilities known and understood in a statement of security policy issued by their executive management to demonstrate the management's commitment to provide guidelines to the staff and to set out the organization's security objectives. All personnel should be aware of and regularly educated about physical protection."

3.6.6.3. Documentation

- Security policy statement.
- Security awareness programme
- Code of conduct for employees.
- Security training documentation.
- Self-assessment reports.
- Security culture survey results.

3.6.6.4. Review points/specimen questions

Determine if:

- Competent authority communicates with and/or evaluates facility management regarding security culture.
- There is a published security culture policy and programme.
- A statement of security policy has been issued by facility management to demonstrate the management's commitment to provide guidelines to the staff and to set out the organization's security objectives.

- Due priority is given to the security culture, to its development and maintenance, as necessary, to ensure its effective implementation in the entire organization.
- It is recognized that a credible threat exists, that preserving nuclear security is important, and that the role of the individual is important.
- Managers and staff work together to establish and maintain an effective nuclear security culture.
- Nuclear security culture is pervasive in all elements of the physical protection system.
- All security personnel are aware of, and regularly educated about, physical protection and their individual responsibilities to ensure its effectiveness.
- An employee security awareness programme is implemented.
- Contractors/employees are provided with an initial orientation and ongoing training related to their security related responsibilities.
- Employees are aware of their responsibilities during security events, including emergency evacuations, bomb threat incidents and facility exercises.

3.6.7. Confidentiality

3.6.7.1. Objective

- To determine if sensitive information and systems containing sensitive information are identified and how these are managed and protected.

3.6.7.2. Basis

- CPPNM Amendment, Fundamental Principle L: Confidentiality:

"The State should establish requirements for protecting the confidentiality of information, the unauthorized disclosure of which could compromise the physical protection of nuclear material and nuclear facilities."

- INFCIRC/225/Rev.5, para. 3.54:

"Management of a *physical protection system* should limit access to sensitive information to those whose trustworthiness has been established appropriate to the sensitivity of the information and who need to know it for the performance of their duties. Information addressing possible vulnerabilities in *physical protection systems* should be highly protected."

- INFCIRC/225/Rev.5, paras 4.10 and 5.19:

"Computer based systems used for physical protection, nuclear safety, and nuclear material accountancy and control should be protected against compromise (e.g. cyber attack, manipulation or falsification) consistent with the *threat assessment* or *design basis threat*."

3.6.7.3. Documentation

- Legislation and regulations on information protection;
- Information protection policy;
- National security information classification document.
- Classification process.
- Information protection training programme.
- Policy on reporting security infractions.

3.6.7.4. Review points/specimen questions

Determine if:

- Policies exist for determining what information requires protection and if the graded approach is adopted in this respect.
- Measures and procedures for protecting the confidentiality of information, the unauthorized disclosure of which could compromise the physical protection of nuclear material and nuclear facilities, have been established and are implemented.
- Sensitive information classifiers have access to, and are trained on, the use of classification guides.
- Personnel are trained on policy for confidentiality.
- Access to sensitive information is restricted to those whose trustworthiness has been established, appropriate to the sensitivity of the information, and who need to know it for the performance of their duties.
- Information addressing possible vulnerabilities in physical protection systems is highly protected.
- Secure storage containers, such as safes, cabinets, etc., are available.
- Computer based systems used for physical protection, nuclear safety and nuclear material accountancy and control are protected against compromise, using a graded approach.

3.6.8. Trustworthiness

3.6.8.1. Objective

- To determine what the trustworthiness programme is, how it is maintained and whether it applies the graded approach.

3.6.8.2. Basis

- INFCIRC/225/Rev.5, para. 3.54:

"Management of a *physical protection system* should limit access to sensitive information to those whose trustworthiness has been established appropriate to the sensitivity of the information and who need to know it for the performance of their duties. Information addressing possible vulnerabilities in *physical protection systems* should be highly protected."

- INFCIRC/225/Rev.5, paras 4.26 and 5.24:

"Only authorized persons should have access to the *protected area*. Effective access control measures should be taken to ensure the *detection* and prevention of unauthorized access. The number of authorized persons entering the *protected area* should be kept to the minimum necessary. Persons authorized unescorted access to the *protected area* should be limited to persons whose trustworthiness has been determined. Persons whose trustworthiness has not been determined such as temporary repair, service or construction workers and visitors should be escorted by persons authorized for unescorted access."

- INFCIRC/225/Rev.5, para. 4.42:

"Only authorized persons should have access to the *inner area*. Effective access control measures should be taken to ensure the *detection* and prevention of unauthorized access. The number of authorized persons entering the *inner area* should be kept to the minimum necessary. Persons with authorized access to the *inner area* should be limited to those whose trustworthiness has been determined. In exceptional circumstances and for a limited period, persons whose trustworthiness has not been determined should be provided access only when escorted by persons authorized for unescorted access."

- INFCIRC/225/Rev.5, para. 5.31:

"Only authorized persons should have access to the *vital area*. Effective access control measures should be taken to ensure the *detection* and prevention of unauthorized access. The number of authorized persons entering the *vital area* should be kept to the minimum necessary. Authorized access to the *vital area* should be limited to persons whose trustworthiness has been determined. In exceptional circumstances and for a limited period, persons whose trustworthiness has not been determined should be provided access only when escorted by persons authorized for unescorted access."

3.6.8.3. Documentation

- Procedure for determining trustworthiness;
- Employee code of conduct;
- Records of denied access.

3.6.8.4. Review points/specimen questions

Determine if:

- Trustworthiness determinations are carried out.
- How trustworthiness determinations are carried out.
- Which persons have to undergo trustworthiness checks.
- The trustworthiness of all security staff has been established.
- Process for access of temporary repair, service or construction workers and visitors.
- If different levels of trustworthiness require different trustworthiness checks.
- If a graded approach is implemented for different security areas.

3.6.9. Security procedures

3.6.9.1. Objective

- To determine if current physical protection procedures provide adequate and appropriate direction for security staff to perform their duties during normal conditions and nuclear security events.

3.6.9.2. Basis

- INFCIRC 225/Rev.5, para. 3.45:

"State requirements for physical protection should be based on the concept of *defence in depth*. The concept of physical protection is one which requires a designed mixture of hardware (security devices), procedures (including the organization of *guards* and the performance of their duties) and facility design (including layout)."

3.6.9.3. Documentation

- Security procedures.

3.6.9.4. Review points/specimen questions

Determine if and how:

- Physical protection procedures are developed, reviewed, revised, tested, implemented and enforced.
- All procedures and revisions that involve physical protection are approved by an appropriate level of management.

- Procedures are properly communicated to, and understood by, the appropriate staff.
- Physical protection measures are documented and applied for on-site movement of Category I or II nuclear material between two protected areas.
- Comprehensive written procedures cover the following:
    - Structure of the physical protection organization;
    - Duties of all physical protection staff;
    - Duties for all security posts;
    - Employee and visitor access and egress control;
    - Vehicle access and egress control;
    - Material access and egress control;
    - Vehicle, person, and package searches;
    - Limited access, protected, inner and vital area patrols;
    - Shift turnover;
    - Testing and maintenance of physical protection systems;
    - Incident response;
    - Initiating corrective action;
    - Event reporting;
    - Experience feedback.

3.6.10. Reporting of nuclear security events

3.6.10.1. Objective

- To determine what procedures are used for the reporting of nuclear security events to the State's competent authority.

3.6.10.2. Basis

- INFCIRC/225/Rev.5, para. 3.26:

"The *operator* should ensure control of, and be able to account for, all *nuclear material* at a *nuclear facility* at all times. The *operator* should report any confirmed accounting discrepancy in a timely manner as stipulated by the *competent authority*."

- INFCIRC/225/Rev.5, para. 3.30:

"Whenever the *physical protection system* is determined to be incapable of providing the required level of protection, the *operator*, *shipper* and/or carrier should immediately implement compensatory measures to provide adequate protection. The *operator* and/or *shipper* should then — within an agreed period — plan and implement corrective actions to be reviewed and approved by the *competent authority*."

- INFCIRC/225/Rev.5, para. 4.59:

"The *operator* should notify the *competent authority* and other relevant State organizations of missing or stolen *nuclear material* as specified by the State."

- INFCIRC/225/Rev.5, para. 5.57:

"The *operator* should notify, in a timely manner, the *competent authority*, *response forces* and other relevant State organizations of *sabotage* or attempted *sabotage* as specified in the *contingency plan*."

3.6.10.3. Documentation

- Procedure for reporting security events;
- Forms for reporting security events;
- Example records for reported security events.

3.6.10.4. Review points/specimen questions

Determine if:

- Procedures exist to guarantee timely reporting of nuclear security events and information to the State's competent authority.
- The operator reports any confirmed accounting discrepancy of nuclear material in a timely manner as stipulated by the competent authority.

3.6.11. System evaluation, including performance testing

3.6.11.1. Objective

- To determine how the effectiveness of procedures (including guards and response forces), equipment and physical protection system design is regularly verified.

3.6.11.2. Basis

- INFCIRC/225/Rev.5, para. 3.29:

"The *operator* should develop and implement means and procedures for evaluations, including *performance testing*, and maintenance of the *physical protection system*."

- INFCIRC/225/Rev.5, para. 3.30:

"Whenever the *physical protection system* is determined to be incapable of providing the required level of protection, the *operator*, *shipper* and/or carrier should immediately implement compensatory measures to provide adequate protection. The *operator* and/or *shipper* should then — within an agreed period — plan and implement corrective actions to be reviewed and approved by the *competent authority*."

For unauthorized removal, Category II:

- INFCIRC/225/Rev.5, para. 4.35:

"Evaluations, including *performance testing*, of the *physical protection measures* and of the *physical protection system*, including timely response of the *guards* and *response forces* should be conducted regularly to determine reliability and effectiveness against the *threat*. These should be carried out with full cooperation between the *operator* and *response forces*. Significant deficiencies and action taken should be reported as stipulated by the *competent authority*."

For unauthorized removal, Category I:

- INFCIRC/225/Rev.5, para. 4.49:

"*Guards* and *response forces* should provide an effective and timely response to prevent an adversary from completing the *unauthorized removal*. At least annually, *performance testing* of the *physical protection system* should include appropriate exercises, for example *force-on-force exercises*, to determine if the *guards* and the *response forces* can reach this objective."

For location and recovery of missing or stolen nuclear material:

- INFCIRC/225/Rev.5, para. 4.60:

"The *operator's* measures to locate and recover missing or stolen *nuclear material* should be included in its *contingency plan*, and should be regularly tested and evaluated. Appropriate joint exercises should be held with the *competent authority* and other State organizations."

For sabotage, unacceptable radiological consequences:

- INFCIRC/225/Rev.5, para. 5.15:

"The *operator* should evaluate and the *competent authority* should validate the design of *physical protection system* effectiveness to verify that it complies with the required level of protection for the *nuclear facility* and *nuclear material*."

For sabotage, high radiological consequences, vital area:

- INFCIRC/225/Rev.5, para. 5.41:

"Evaluations, including *performance testing*, of the *physical protection measures* and of the *physical protection system*, including timely response of the *guards* and *response forces*, should be conducted regularly to determine reliability and effectiveness against the *threat*. These should be carried out with full cooperation between the *operator* and *response forces*. *Performance testing* of the *physical protection system* should include appropriate exercises, for example *force-on-force exercises*, to determine if the *response forces* can provide an effective and timely response to prevent *sabotage*. Significant deficiencies and actions taken should be reported as stipulated by the *competent authority*."

3.6.11.3. Documentation

- Vulnerability assessment methods and tools.
- Computer modelling methods and tools.
- Equipment and procedure test plans.
- Security exercise plans: limited scope, table top, force-on-force.
- Contingency plans and procedures are routinely reviewed and performance tested, e.g. to verify the effectiveness of the security organization to respond to an intrusion.
- Exercise outcome reports/records.

3.6.11.4. Review points/specimen questions

Determine if and how:

- Vulnerability assessment has been conducted and the results used to address vulnerabilities that were revealed.
- Appropriate exercises, such as force-on-force, that include all response organizations have been conducted.
- Testing, maintenance and deficiency improvement programmes exist that ensure the integrity of security related systems.
- Physical protection and communication systems are tested and maintained, and deficiencies are reported and repaired.
- There are adequate testing budget, equipment and human resources available.
- Testing is carried out at an appropriate frequency, the different types of test and how they are conducted.
- Performance testing is conducted at the component, subsystem and system levels.
- All contingency plans are tested and revised as necessary.

- Capabilities specific to contingency plans (training, equipment, contact lists) are available and functional.
- Response force exercises (e.g. force-on-force exercise) are conducted regularly and include all guards and response forces, e.g. to verify the effectiveness of the security organization to respond to security events (date and scenario of recent exercises).
- The last exercise involving all security actors, as described in the contingency plan.
- Scenario(s) involving all actors are used.
- Exercise experience is used to enhance security.
- Emergency plans and contingency plans are exercised simultaneously.

3.6.12. Quality assurance

3.6.12.1. Objective

- To determine that adequate quality assurance policies and programmes for physical protection exist.

3.6.12.2. Basis

- CPPNM Amendment, Fundamental Principle J: Quality Assurance:

"A quality assurance policy and quality assurance programmes should be established and implemented with a view to providing confidence that specified requirements for all activities important to physical protection are satisfied."

- INFCIRC/225/Rev.5, para. 3.52:

"The quality assurance policy and programmes for physical protection should ensure that a *physical protection system* is designed, implemented, operated and maintained in a condition capable of effectively responding to the *threat assessment* or *design basis threat* and that it meets the State's regulations, including its prescriptive and/or performance based requirements."

3.6.12.3. Documentation

- Quality assurance plan;
- Quality manual;
- Quality metrics/measurements;
- Quality audit reports/review records;
- Incident reporting, including self-reports;
- Action tracking reports.

3.6.12.4. Review points/specimen questions

Determine if:

- Quality assurance policies and programmes for physical protection exist and how they ensure that a physical protection system is designed, evaluated, implemented, operated and maintained in a condition capable of effectively responding to the threat assessment or DBT.
- Any international standards are used as the basis of the programme, what they are and how they are used.

3.6.13. Sustainability programme

3.6.13.1. Objective

- To determine if there are adequate sustainability programme(s) which include human resources and equipment, including software.

3.6.13.2. Basis

- INFCIRC/225/Rev.5, para. 3.57:

"*Operator*s, *shippers* and carriers should establish sustainability programmes for their *physical protection system*. Sustainability programmes should encompass:

- Operating procedures (instructions).
- Human resource management and training.
- Equipment updating, maintenance, repair and calibration.
- *Performance testing* and operational monitoring.
- Configuration management (the process of identifying and documenting the characteristics of a facility's *physical protection system* — including computer systems and software — and of ensuring that changes to these characteristics are properly developed, assessed, approved, issued, implemented, verified, recorded and incorporated into the facility documentation).
- Resource allocation and operational cost analysis."

3.6.13.3. Documentation

- Maintenance programme and records, including spare parts inventory list;
- Security system configuration management and management system;
- Security budget records and expense records;
- Programme for security improvement actions (equipment, training, human resources);

- Management succession plan and staff hiring plan.

3.6.13.4. Review points/specimen questions

Determine if:

- A preventive maintenance programme is established, adhered to, and adequately supported.
- Testing, maintenance and deficiency improvement programmes exist that ensure the integrity of security related systems.
- Maintenance documentation is current and available only to authorized personnel.
- Maintenance personnel are qualified and effective, have adequate testing equipment and other necessary resources, and their training is current.
- The facility compensates for physical protection system maintenance outages and failures, and minimized the time within which repairs are effected and the system is returned to full operational status.
- Physical protection systems are tested and maintained, and deficiencies are reported and promptly repaired.
- Configuration management system addresses all security hardware, software and procedures.
- Programme to address hardware/software obsolescence exists.
- A succession plan exists for security personnel and what it is.
- There is an evaluation of training programmes and what it is.
- There is a development programme for staff and what it is.
- There is a process to identify and evaluate new security equipment and what it is.
- There is a budget for capital improvement.
- Essential spares have been identified and are available and how they were determined.
- Testing is carried out, e.g. testing at an appropriate frequency, the different types of test and how these tests are conducted.

3.7. PHYSICAL PROTECTION SYSTEM

3.7.1. Graded protection and defence in depth

3.7.1.1. Objective

- To determine if the physical protection is based on a graded approach and whether it incorporates appropriate levels of defence in depth.

3.7.1.2. Basis

- INFCIRC/225/Rev.5, para. 3.46:

"The three physical protection functions of *detection*, delay, and response should each use *defence in depth* and apply a *graded approach* to provide appropriate effective protection."

3.7.1.3. Documentation

- List and locations of nuclear material and sabotage targets;
- Physical protection system design overview, including facility layout.

3.7.1.4. Review points/specimen questions

Determine if and how:

- The three physical protection functions of detection, delay and response each use defence in depth and apply a graded approach to provide appropriate effective protection.
- Nuclear material is categorized and its location has been assigned the appropriate level of graded protection.
- Each potential sabotage target is identified and its location has been assigned the appropriate level of graded protection.
- Defence in depth has been applied for nuclear material and sabotage targets.
- The physical protection system relies on defence in depth for increased effectiveness and reliability, and takes into account the capability of the system for nuclear material accountancy and control.
- The physical protection system benefits from relevant safety features.

3.7.2. Detection

3.7.2.1. Access control

(a) Objectives

- To determine if appropriate access control is in place for people, vehicles and packages.
- To determine how locks, keys and combination are managed.

(b) Basis

For unauthorized removal, Category III, limited access area:

- INFCIRC/225/Rev.5, para. 4.17:

"Technical means and procedures for access control, such as keys and computerized access lists, should be protected against compromise, e.g. manipulation or falsification."

For unauthorized removal, Category II, protected area:

- INFCIRC/225/Rev.5, para. 4.24:

"The number of access points into the *protected area* should be kept to the minimum necessary. All points of potential access should be appropriately secured and fitted with alarms."

- INFCIRC/225/Rev.5, para. 4.25:

"Vehicles, persons and packages entering and leaving the *protected area* should be subject to search for *detection* and prevention of unauthorized access and of introduction of prohibited items or removal of *nuclear material*, as appropriate. Entry of vehicles into the *protected area* should be strictly minimized and limited to designated parking areas."

- INFCIRC/225/Rev.5, para. 4.26:

"Only authorized persons should have access to the *protected area*. Effective access control measures should be taken to ensure the *detection* and prevention of unauthorized access. The number of authorized persons entering the *protected area* should be kept to the minimum necessary. Persons authorized unescorted access to the *protected area* should be limited to persons whose trustworthiness has been determined. Persons whose trustworthiness has not been determined such as temporary repair, service or construction workers and visitors should be escorted by persons authorized for unescorted access."

- INFCIRC/225/Rev.5, para. 4.27:

"The identity of authorized persons entering the *protected area* should be verified. Passes or badges should be issued and visibly displayed inside the *protected area*."

- INFCIRC/225/Rev.5, para. 4.28:

"A record should be kept 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*."

- INFCIRC/225/Rev.5, para. 4.34:

"The *guards* should conduct random patrols of the *protected area*. The main functions of the patrols should be to:

- Deter an adversary;
- Detect intrusion;
- Inspect visually the physical protection components;
- Supplement the existing *physical protection measures*;
- Provide an initial response."

For unauthorized removal, Category I, inner area:

- INFCIRC/225/Rev.5, para. 4.40:

"The number of access points to the *inner areas* should be kept to the minimum necessary (ideally only one). All points of potential access should be appropriately secured and fitted with alarms."

- INFCIRC/225/Rev.5, para. 4.42:

"Only authorized persons should have access to the *inner area*. Effective access control measures should be taken to ensure the *detection* and prevention of unauthorized access. The number of authorized persons entering the *inner area* should be kept to the minimum necessary. Persons with authorized access to the *inner area* should be limited to those whose trustworthiness has been determined. In exceptional circumstances and for a limited period, persons whose trustworthiness has not been determined should be provided access only when escorted by persons authorized for unescorted access."

- INFCIRC/225/Rev.5, para. 4.43:

"Vehicles, persons and packages should be subject to search on entering both the *protected* and *inner areas* for *detection* and prevention of unauthorized access and of introduction of prohibited items. Vehicles, persons and packages leaving the *inner area* should be subject to search for *detection* and prevention of *unauthorized removal*. Instruments for the *detection* of *nuclear material*, metals, and explosives could be used for such searches."

- INFCIRC/225/Rev.5, para. 4.44:

"Private vehicles should be prohibited access to *inner areas*."

- INFCIRC/225/Rev.5, para. 4.45:

"Records should be kept of all persons who access *inner areas* and of all persons who have access to or possession of keys, keycards and/or other systems, including computer systems, that control access to *inner areas*."

- INFCIRC/225/Rev.5, para. 4.46:

"Inside the *inner area*, *nuclear material* should be stored in a hardened room ('strong room') or hardened enclosure that provides an additional layer of *detection* and delay against removing the material. This storage area should be locked and alarms activated except during authorized access to the material. When *nuclear material* is kept in an unoccupied work area outside this storage area, e.g. overnight, equivalent compensatory *physical protection measures* should be established."

For sabotage, unacceptable radiological consequences:

- INFCIRC/225/Rev.5, para. 5.14:

"The *physical protection system* should be designed to deny unauthorized access of persons or equipment to the targets, minimize opportunity of *insiders*, and to protect the targets against possible *stand-off*

attacks consistent with the State's *threat assessment* or *design basis threat*. The response strategy should include denial of adversary access to the *sabotage* targets or denial of adversary task completion at the *sabotage* targets. Denying access to the targets or denial of adversary task completion is accomplished by the primary physical protection functions of *detection*, delay and response, whereas protecting against *stand-off attacks* involves facility design considerations, barrier design considerations to implement stand-off distance, and other disruption measures."

For sabotage, high radiological consequences, vital area:

- INFCIRC/225/Rev.5, para. 5.22:

"The number of access points into the *protected area* should be kept to the minimum necessary. All points of potential access should be appropriately secured and fitted with alarms."

- INFCIRC/225/Rev.5, para. 5.23:

"Vehicles, persons and packages entering the *protected area* should be subject to search for *detection* and prevention of unauthorized access and of introduction of prohibited items. Instruments for the *detection* of *nuclear material*, metal, and explosives can be used for such searches. Entry of vehicles into the *protected area* should be strictly minimized and limited to designated parking areas."

- INFCIRC/225/Rev.5, para. 5.24:

"Only authorized persons should have access to the *protected area*. Effective access control measures should be taken to ensure the *detection* and prevention of unauthorized access. The number of authorized persons entering the *protected area* should be kept to the minimum necessary. Authorized unescorted access to the *protected area* should be limited to persons whose trustworthiness has been determined. Persons, whose trustworthiness has not been determined, such as temporary repair, service or construction workers and visitors, should be escorted by persons authorized for unescorted access."

- INFCIRC/225/Rev.5, para. 5.25:

"The identity of authorized persons entering the *protected area* should be verified. Passes or badges should be issued and visibly displayed inside the *protected area*."

- INFCIRC/225/Rev.5, para. 5.28:

"The number of access points to the *vital areas* should be kept to the minimum necessary (ideally only one). All points of potential access should be appropriately secured and fitted with alarms."

- INFCIRC/225/Rev.5, para. 5.31:

"Only authorized persons should have access to the *vital area*. Effective access control measures should be taken to ensure the *detection* and prevention of unauthorized access. The number of authorized persons entering the *vital area* should be kept to the minimum necessary. Authorized access to the *vital area* should be limited to persons whose trustworthiness has been determined. In exceptional circumstances and for a limited period, persons whose trustworthiness has not been determined should be provided access only when escorted by persons authorized for unescorted access."

- INFCIRC/225/Rev.5, para. 5.32:

"Private vehicles should be prohibited from accessing *vital areas*."

- INFCIRC/225/Rev.5, para. 5.34:

"During a shutdown/maintenance period, strict access control to *vital areas* should be maintained. Prior to reactor start-up, searches and testing should be conducted to detect any tampering that may have been committed during shutdown/maintenance."

- INFCIRC/225/Rev.5, para. 5.35:

"Records should be kept of all persons who access *vital areas* or have access to or possession of keys, keycards and/or other systems, including computer systems that control access to *vital areas*."

(c) Documentation

- Facility layout showing access points and including detailed layout of personnel and vehicles portals;
- User manuals;
- Training records of operators;
- Policy/procedures for key management;
- Key records/log book.

(d) Review points/specimen questions

Determine:

- How procedures for personnel, vehicle, and package/material access to and from the limited access, protected, inner and vital areas are implemented.
- How personnel, vehicles, packages and bags are searched, including type of search and frequency of search
- If there reference materials are used for calibration.
- If personnel are informed and understand what is being searched for.
- How deliveries are effected, including how freight packages are handled and stored.
- If access authorization lists or databases are updated in a timely manner to reflect removal of authorization for transferred or terminated employees.
- If a current access authorization list or database is maintained at every access point for the guards to reference.
- If a credential system is implemented for all personnel who are authorized for unescorted access to the protected area (include all areas) and what it is.
- If all personnel who are authorized only for escorted access are registered and 'badged' to indicate that an escort is required.

- If badges are clearly displayed by all persons.
- If the badging process system and materials are maintained in a secure manner.
- If all badges are accounted for and all un-issued badges are controlled and secured.
- If all authorized escorted persons are escorted at all times while in the protected area.
- If all escorts understand their responsibilities and duties and are authorized to perform the escort function.
- If access to an inner area is subject to the two person rule.
- If performance tests are implemented.
- If there is a secure backup power supply for the access control server.
- If access control software is verified and validated.
- If there is a procedure for a lost or forgotten badge.
- If the number of access points for each area is minimized.
- If the number of private vehicles in each area is minimized.
- If there are any exceptions to the screening/searching of personnel, vehicles and packages.
- If there are records of personnel access (who and when) to each area.
- If emergency response personnel/vehicles are screened/searched during a nuclear security event or emergency situation.
- During nuclear power plant scheduled maintenance outage how access control procedures are implemented.
- If technical means and procedures for access control, such as keys and computerized access lists, are protected against compromise, e.g. manipulation or falsification.
- If all required key/lock activities are defined in procedures.
- If authorization is based on a need to access principle.
- If a current list of authorized key users is maintained.
- If keys and combinations are issued by authorized personnel to authorized users only.
- If a lock and key control register is maintained to identify the number of keys issued for each lock, their location and a history of each lock/keying change.
- If key logs are reviewed and signed by appropriate staff.
- If keys have not been out or unaccounted for over extended periods of time without justification.
- If the quality of locks is appropriate for the intended use.
- If, as appropriate, keys and combinations are changed on a routine basis or upon discovery of compromise, loss, or termination of employment.
- If all keys, locks, combinations, key cards, key codes and keying records are the responsibility of designated personnel.

- If keys, combinations and key cards not in use are adequately protected from theft, alteration or duplication.
- If reports are prepared documenting incidents involving lost, misplaced keys, and/or compromised keys and locks.
- If the issue of master keys is minimized, controlled and accounted for.
- If separation of two person keys and combinations is maintained (they are to be stored and controlled separately).
- If keys are allowed to be taken off-site.
- If copying/duplicating of keys is controlled and how.

3.7.2.2. Intrusion detection

(a) Objective

- To determine how attempts of unauthorized access and intrusion are detected.

(b) Basis

For unauthorized removal, Category III, limited access area:

- INFCIRC/225/Rev.5, para. 4.15:

"Provision should be made for detecting unauthorized intrusion and for appropriate action by sufficient *guards* and/or *response forces* to address a *nuclear security event*."

For unauthorized removal, Category II, protected area:

- INFCIRC/225/Rev.5, para. 4.23:

"A *protected area* should be located inside a *limited access area*. The *protected area* perimeter should be equipped with a *physical barrier*, intrusion *detection* and assessment to *detect* unauthorized access. These protection measures should be configured to provide time for assessment of the cause of alarms, and provide adequate delay for an appropriate response, under all operational conditions. Alarms generated by intrusion detection sensors should be promptly and accurately assessed and appropriate action taken."

For unauthorized removal, Category I, inner area:

- INFCIRC/225/Rev.5, para. 4.38:

"An *inner area* should provide an additional layer to the *protected area* for *detection*, access control and delay against *unauthorized removal*. *Inner areas* should be appropriately secured and fitted with alarms when unattended."

- INFCIRC/225/Rev.5, para. 4.48:

"To counter the *insider* threat, whenever an *inner area* is occupied, *detection* of unauthorized action should be achieved by constant surveillance (e.g. the *two person rule*)."

For sabotage, unacceptable radiological consequences:

- INFCIRC/225/Rev.5, para. 5.14:

"The *physical protection system* should be designed to deny unauthorized access of persons or equipment to the targets, minimize opportunity of *insiders*, and to protect the targets against possible *stand-off attacks* consistent with the State's *threat assessment* or *design basis threat*. The response strategy should include denial of adversary access to the *sabotage targets* or denial of adversary task completion at the *sabotage targets*. Denying access to the targets or denial of adversary task completion is accomplished by the primary physical protection functions of *detection*, delay and response, whereas protecting against *stand-off attacks* involves facility design considerations, barrier design considerations to implement a stand-off distance, and other disruption measures."

For sabotage, high radiological consequences, vital area:

- INFCIRC/225/Rev.5, para. 5.21:

"A *protected area* should be located inside a *limited access area*. The *protected area* perimeter should be equipped with a *physical barrier*, intrusion *detection* and assessment to *detect* unauthorized access. These protection measures should be configured to provide time for assessment of the cause of alarms, and provide adequate delay for an appropriate response, under all operational conditions. Alarms generated by intrusion detection sensors should be promptly and accurately assessed and appropriate action taken."

- INFCIRC/225/Rev.5, para. 5.29:

"To counter the *insider* threat, whenever persons are present in *vital areas*, provision should be made for timely *detection* of unauthorized action."

- INFCIRC/225/Rev.5, para. 5.40:

"The *guards* should conduct random patrols of the *protected area*. The main functions of the patrols should be to:

- Deter an adversary;
- Detect intrusion;
- Inspect visually the physical protection components;
- Supplement the existing *physical protection measures*;
- Provide an initial response."

(c) Documentation

- Physical protection system design package, including physical layout;

- Nuisance alarm rates and sources;
- Performance testing procedure and schedule;
- Maintenance records, including preventive and unscheduled.

(d) Review points/specimen questions

Determine:

- If intrusion detection equipment is appropriate and adequate for the facility and the threat environment and if it performs as designed.
- If the detection systems are segmented into sufficient numbers of overlapping alarm zones to provide adequate coverage of the areas under surveillance.
- If the maximum length of the detection zone is appropriate to the sensor and assessment system capability.
- If and how the system detects any openings in the protected areas, inner areas and vital areas.
- If and how the detection systems, including transmission lines to their respective annunciators, are tamper resistant, tamper indicating and self-checking.
- If the controls and switches that affect sensitivity of the detection systems are located in a tamper alarmed container or housing.
- If and how compensatory measures are taken when activities that could interfere with the intrusion detection system are present, for example, a guard being posted.
- If access to detection and alarm control and annunciating equipment areas is limited only to authorized persons.
- If nuisance alarms are at an acceptable level.
- If false alarms are at an acceptable level.
- If there is a procedure in place to discern between actual, nuisance and false alarms.
- If all areas are periodically checked by guards for unauthorized activities, conditions, personnel, vehicles and nuclear material.
- If intrusion detection sensors cover all avenues of approach to the target.
- How intrusion detection is accomplished at water boundaries.
- What aerial detection is provided.
- How insider adversaries are detected.
- What operability tests are conducted, by whom, and how frequently.
- What detection volume tests are conducted, by whom, and how frequently.

3.7.2.3. Alarm assessment

(a) Objective

- To determine how alarm assessment is made.

(b) Basis

For unauthorized removal, Category II, protected area:

- INFCIRC/225/Rev.5, para. 4.23:

"A *protected area* should be located inside a *limited access area*. The *protected area* perimeter should be equipped with a *physical barrier*, intrusion *detection* and assessment to *detect* unauthorized access. These protection measures should be configured to provide time for assessment of the cause of alarms, and provide adequate delay for an appropriate response, under all operational conditions. Alarms generated by intrusion detection sensors should be promptly and accurately assessed and appropriate action taken."

- INFCIRC/225/Rev.5, para. 4.30:

"A permanently staffed *central alarm station* should be provided for monitoring and assessment of alarms, initiation of response, and communication with the *guards*, *response forces*, and facility management. Information acquired at the *central alarm station* should be stored in a secure manner. The *central alarm station* should normally be located in a *protected area* and protected so that its functions can continue in the presence of a *threat*, e.g. hardened. Access to the *central alarm station* should be strictly minimized and controlled."

For unauthorized removal, Category I, inner area:

- INFCIRC/225/Rev.5, para. 4.47:

"Provisions, including redundancy measures, should be in place to ensure that the functions of the *central alarm station* in monitoring and assessment of alarms, initiation of response and communication can continue during an emergency (e.g. a backup alarm station)."

For sabotage, high radiological consequences, vital area:

- INFCIRC/225/Rev.5, para. 5.21:

"A *protected area* should be located inside a *limited access area*. The *protected area* perimeter should be equipped with a *physical barrier*, intrusion *detection* and assessment to *detect* unauthorized access. These protection measures should be configured to provide time for assessment of the cause of alarms, and provide adequate delay for an appropriate response, under all operational conditions. Alarms generated by intrusion detection sensors should be promptly and accurately assessed, and appropriate action taken."

- INFCIRC/225/Rev.5, para. 5.36:

"A permanently staffed *central alarm station* should be provided for monitoring and assessment of alarms, initiation of response, and communication with the *guards*, *response forces*, and facility management. Information acquired at the *central alarm station* should be stored in a secure manner. The *central alarm station* should normally be located in a *protected area* and protected so that its functions can continue in the presence of a *threat*, e.g. hardened. Access to the *central alarm statio*n should be strictly minimized and controlled. Provisions, including redundancy measures, should be in place to ensure that the functions of the *central alarm station* in monitoring and assessment of alarms, initiation of response and communication can continue during an emergency (e.g. backup alarm station)."

(c) Documentation

- Camera coverage layout;
- Lighting plan;
- Assessment procedures;
- Alarm assessment records.

(d) Review points/specimen questions

Determine:

- If and how the cause of an intrusion alarm is assessed.
- If the assessment equipment (e.g. video) is adequate and appropriate for the facility and the equipment performs as designed.
- If, when video is used, the alarm zone covered can be viewed effectively during both daylight and night-time hours.
- For outdoor night-time assessment lighting, what are the minimum lighting levels and maximum dark-to-light ratio.
- If there is no glare or blooming effect that impedes assessment on the video monitors.
- If there any clutter, such as vegetation or construction materials, in the field of view that impedes assessment.
- If the picture quality of video system is appropriate to monitor persons or activities anywhere within the field of view.
- If outdoor video cameras are appropriately protected from the environment.
- If video lenses are maintained, e.g. free from dust and cobwebs.
- If a system is in place to prevent tampering with cameras.
- If procedures are in place to handle situations where assessment is not achieved, for example, guards promptly responding to the suspect area to check for physical evidence of entry, attempted entry, and/or damage to the barriers.
- If criteria are in place to manually assess an alarm event.

- If video is not used for assessment, how assessment is performed in a timely manner.
- If protected area access points and other key posts (e.g. central alarm station (CAS) and reactor control room) are equipped with duress alarms.
- If duress alarms annunciate in the CAS.
- If guards are equipped with duress alarms.
- If duress alarms are tested regularly and documented.
- How the insider threat is taken into account.
- How the insider threat is addressed by specific physical protection measures.
- What specific training is in place to cope with the insider threat.
- What exercises are performed to counter the insider threat.
- How the security awareness programme addresses the insider threat.

3.7.2.4. Central alarm station

(a) Objective

- To determine where CAS is located, how it is protected and what functions it performs.

(b) Basis

For unauthorized removal, Category II, protected area:

- INFCIRC/225/Rev.5, para. 4.30:

"A permanently staffed *central alarm station* should be provided for monitoring and assessment of alarms, initiation of response, and communication with the *guards*, *response forces*, and facility management. Information acquired at the *central alarm station* should be stored in a secure manner. The *central alarm station* should normally be located in a *protected area* and protected so that its functions can continue in the presence of a *threat*, e.g. hardened. Access to the *central alarm station* should be strictly minimized and controlled."

- INFCIRC/225/Rev.5, para. 4.31:

"Alarm equipment, alarm communication paths, and the *central alarm station* should be provided with an uninterruptible power supply and be tamper protected against unauthorized monitoring, manipulation and falsification."

- INFCIRC/225/Rev.5, para. 4.32:

"Dedicated, redundant, secure and diverse transmission systems for two way voice communication between the *central alarm station* and the *response forces* should be provided for activities involving *detection*, assessment and response. Dedicated two way secure voice communication should be provided between *guards* and the *central alarm station*."

- INFCIRC/225/Rev.5, para. 4.33:

"A 24 hour guarding service and *response forces* should be provided to counter effectively any attempted *unauthorized removal*. The *central alarm station* personnel and off-site *response forces* should communicate at scheduled intervals. The *guards* and *response forces* should be trained and adequately equipped for their functions in accordance with national laws and regulations."

For unauthorized removal, Category I, inner area:

- INFCIRC/225/Rev.5, para. 4.47:

"Provisions, including redundancy measures, should be in place to ensure that the functions of the *central alarm station* in monitoring and assessment of alarms, initiation of response and communication can continue during an emergency (e.g. a backup alarm station)."

For sabotage, high radiological consequences, vital area:

- INFCIRC/225/Rev.5, para. 5.36:

"A permanently staffed *central alarm station* should be provided for monitoring and assessment of alarms, initiation of response, and communication with the *guards*, *response forces*, and facility management. Information acquired at the *central alarm station* should be stored in a secure manner. The *central alarm station* should normally be located in a *protected area* and protected so that its functions can continue in the presence of a *threat,* e.g. hardened. Access to the *central alarm station* should be strictly minimized and controlled. Provisions, including redundancy measures, should be in place to ensure that the functions of the *central alarm station* in monitoring and assessment of alarms, initiation of response and communication can continue during an emergency (e.g. backup alarm station)."

- INFCIRC/225/Rev.5, para. 5.37:

"Alarm equipment, alarm communication paths and the *central alarm station* should be provided with an uninterruptible power supply and be tamper protected against unauthorized monitoring, manipulation and falsification."

- INFCIRC/225/Rev.5, para. 5.38:

"Dedicated, redundant, secure and diverse transmission systems for two way voice communication between the *central alarm station* and the *response forces* should be provided for activities involving *detection*, assessment and response. Dedicated two way secure voice communication should be provided between *guards* and the *central alarm station*."

- INFCIRC/225/Rev.5, Para. 5.39:

"A 24 hour guarding service and *response forces* should be provided to ensure an adequate and timely response to prevent an adversary from completing an act of *sabotage*. The *central alarm station* personnel and off-site *response forces* should communicate at scheduled intervals. The *guards* and *response forces* should be trained and adequately equipped for their function in accordance with national laws and regulations."

(c) Documentation

- CAS design document;
- CAS operator procedures;
- Alarm and access control records;
- Communication records.

(d) Review points/specimen questions

Determine:

- If the CAS is located in the protected area; if not, is it in a suitably secured location or hardened against the threat.
- If the CAS is a hardened facility so that its functions can continue in the presence of the DBT or during an emergency (e.g. backup station).
- If entry to the CAS is limited to authorized individuals.
- If the CAS is continuously staffed by a sufficient number of trained security guard(s) who can initiate response and communicate with other security guards, facility management and the off-site response force.
- If the CAS is adequately equipped with alarm, surveillance and communications capabilities.
- If the CAS equipment performs as designed.
- If security systems alarm annunciators indicate the type and locations of alarms.
- If the status of all alarms and alarm zones is indicated.
- If alarm annunciator systems are self-checking and annunciate equipment or component failure and indicate the location of the alarm source.
- If the video alarm assessment system is equipped with automatic video recording and capture capability that can be quickly retrieved and displayed.
- If a backup CAS exists or if there is provision for CAS functions to be continued in the event that the primary CAS is not available for one reason or another.
- If all intrusion detection alarm events, including alarm assessment, are automatically recorded.
- How the operator copes with an alarm event if a video system is not available or if it fails, and what actions are taken to assess the alarm.
- How many video monitors the CAS operator continuously monitors.
- How the CAS/operator copes with multiple simultaneous alarms.

3.7.2.5. Emergency power supply

(a) Objective

- Determine if emergency power supply for the physical protection system exists and if it is adequate.

(b) Basis

- INFCIRC/225/Rev.5, paras 4.31 and 5.37:

"Alarm equipment, alarm communication paths, and the *central alarm station* should be provided with an uninterruptible power supply and be tamper protected against unauthorized monitoring, manipulation and falsification."

(c) Documentation

- Power supply drawing/schematic for UPS, including location(s);
- Procedures for switching to UPS.

(d) Review points/specimen questions

Determine:

- What equipment/load is connected to the emergency power system.
- If the security emergency power supply is separate from other facility equipment and emergency power supplies.
- How long the security emergency power supply will continue to operate.
- If the emergency power supply or other emergency power source maintains the operation of the physical protection system and its equipment in the event of loss of normal power.
- If all alarm and assessment systems remain operable from uninterruptible power sources.
- If an adequate lighting system remains operable from emergency power sources.
- If telephone and any non-portable communication equipment is supported by an uninterruptible power supply.
- If transfer from normal to emergency power does not result in false alarms, and provides loss of power indication.
- If duration of uninterruptible power supply is sufficient for transfer from normal to emergency power.
- If there are procedures in place for immediate deployment or other compensation in the absence or failure of an emergency power supply.
- If the emergency power supply is protected, maintained and regularly tested.
- Detect availability of the emergency power supply to physical protection system.

3.7.3. Delay

3.7.3.1. Protected area barriers

(a) Objective

- Determine how the protected area is defined and what barriers to intrusion are implemented.

(b) Basis

- INFCIRC/225/Rev.5, paras 4.23 and 5.21:

"A *protected area* should be located inside a *limited access area*. The *protected area* perimeter should be equipped with a *physical barrier*, intrusion *detection* and assessment to *detect* unauthorized access. These protection measures should be configured to provide time for assessment of the cause of alarms, and provide adequate delay for an appropriate response, under all operational conditions. Alarms generated by intrusion detection sensors should be promptly and accurately assessed and appropriate action taken."

(c) Documentation

- Site plans/map which shows delay/barrier locations and materials/construction;
- Barrier inspection/test/maintenance procedures and records.

(d) Review points/specimen questions

Determine:

- If protected areas have been established.
- If the protected area perimeter fence fabric (or other material) is intact, taut and free from significant corrosion (does it fulfil its function).
- How openings in the protected area perimeter fence are controlled to prevent an individual from penetrating the barrier undetected.
- If fence posts, brackets, fasteners, hardware, guy wire or cables and electric grounding (earth ground) cables are intact and in good condition.
- If and how all junctions between physical barrier fences and corner posts, gate posts, turnstiles, buildings or walls retain barrier integrity.
- If the protected area perimeter barrier walls of structures and gates offer the same level of resistance to penetration and climbing as the perimeter fence.
- If piping, ducting, culverts, tunnels and other penetrations through protection layers are equipped with barriers (such as grills or other obstacles) and the level to which they delay the DBT (is adequate detection and assessment provided at these penetrations?).
- If and how doors are equipped to prevent or delay unauthorized access, e.g. door construction, locking mechanism, door strike and hinge protection.
- If fences, walls and doors offer comparable delays for balanced protection.
- If and how performance tests are performed on barriers and what expected level of delay is estimated.
- If and how forcible vehicle access is prevented.
- How damage to the protected area barrier is detected.

3.7.3.2. Inner area barriers

(a) Objective

- Determine how the inner area is defined and barriers to intrusion are implemented.

(b) Basis

- INFCIRC/225/Rev.5, Para. 4.38:

"An *inner area* should provide an additional layer to the *protected area* for *detection*, access control and delay against *unauthorized removal*. *Inner areas* should be appropriately secured and fitted with alarms when unattended."

- INFCIRC/225/Rev.5, para. 4.39:

"*Inner areas* should provide delay against unauthorized access to allow for a timely and appropriate response to an *unauthorized removal*. Delay measures should be designed considering both *insiders*' and external adversaries' capabilities, and should take into account and be balanced for all potential points of intrusion."

- INFCIRC/225/Rev.5, para. 4.41:

"Vehicle barriers should be installed at an appropriate distance from the *inner area* to prevent the penetration of unauthorized land and waterborne vehicles specified in the *design basis threat* that could be used by an adversary for committing a *malicious act*. Attention should also be given to providing protection measures against any airborne threat specified in the *design basis threat* for the *operator*."

- INFCIRC/225/Rev.5, para. 4.46:

"Inside the *inner area, nuclear material* should be stored in a hardened room ('strong room') or hardened enclosure that provides an additional layer of *detection* and delay against removing the material. This storage area should be locked and alarms activated except during authorized access to the material. When *nuclear material* is kept in an unoccupied work area outside this storage area, e.g. overnight, equivalent compensatory *physical protection measures* should be established."

(c) Documentation

- Site plans/map which shows delay/barrier locations and materials/construction;
- Barrier inspection/test/maintenance procedures and records.

(d) Review points/specimen questions

Determine:

- If inner areas have been established.

- If inner areas are located within protected areas.
- If the inner areas provide an additional layer to the protected area for delay against unauthorized removal.
- If inner areas provide delay against unauthorized access to allow for a timely and appropriate response to an unauthorized removal.
- If delay measures are designed with consideration of both insiders' and external adversaries' capabilities.
- If inner area barriers such as walls, doors and windows offer the same level of resistance to penetration.
- If piping, ducting, culverts and other penetrations through protection layers are equipped with barriers (such as grills or other obstacles) which offer the same level of resistance to penetration.
- If and how doors and windows are equipped to prevent or delay unauthorized access, e.g. door construction, locking mechanism, door strike and hinge protection.
- If walls, ceilings, floors and doors offer comparable delays for balanced protection.
- If performance tests are performed on barriers to verify that delay requirements are met. If forcible vehicle access is prevented.
- If inside the inner area, nuclear material is stored in a hardened room ('strong room') or hardened enclosure that provides an additional layer of detection and delay against removing the material.
- How damage to the inner area barriers is detected.

3.7.3.3. Vital area barriers

(a) Objective

- Determine how the vital area is defined and what barriers to intrusion are implemented.

(b) Basis

- INFCIRC/225/Rev.5, para. 5.26:

"A *vital area* should provide an additional layer to the *protected area* for *detection*, access control and delay. *Vital areas* should be appropriately secured and alarmed when unattended."

- INFCIRC/225/Rev.5, para. 5.27:

"*Vital areas* should provide delay against unauthorized access to allow for a timely and appropriate response to an act of *sabotage* consistent with the *design basis threat.* Delay measures should be designed considering both the *insiders'* and external adversaries' capabilities, and should take into account and be balanced for all potential points of intrusion."

- INFCIRC/225/Rev.5, para. 5.30:

"Vehicle barriers should be installed at an appropriate distance from the *vital area* to prevent the penetration of unauthorized land and waterborne vehicles specified in the *design basis threat* that could be used by an adversary for committing a *malicious act*. Attention should be given to providing protection measures against any airborne threat specified in the *design basis threat* for the *operator*."

(c) Documentation

- Site plans/map which shows delay/barrier locations;
- Barrier inspection/test/maintenance procedures and records.

(d) Review points/specimen questions

Determine:

- If vital areas have been established.
- If vital areas are located within protected areas.
- If the vital area provides an additional layer to the protected area for delay against unauthorized removal.
- If vital areas provide delay against unauthorized access to allow for a timely and appropriate response to attempts of sabotage.
- If delay measures are designed with consideration of both insiders' and external adversaries' capabilities.
- If vital area barriers such as walls, doors and windows offer the same level of resistance to penetration.
- If piping, ducting, culverts and other penetrations through protection layers are equipped with barriers (such as grills or other obstacles) which offer the same level of resistance to penetration.
- If and how doors and windows are equipped to prevent or delay unauthorized access, e.g. door construction, locking mechanism, door strike and hinge protection.
- If walls, ceilings, floors and doors offer comparable delays for balanced protection.
- If performance tests are performed on barriers to verify that delay requirements are met.
- If forcible vehicle access is prevented.
- How damage to the vital area barriers is detected.

3.7.4 Response

3.7.4.1. Guards and response forces

(a) Objective

- To determine if there is a timely and effective response to nuclear security events.

(b) Basis

- INFCIRC/225/ Rev.5, para. 3.25:

"The *operator*, *shipper* and carrier should cooperate and coordinate with all other State entities having physical protection responsibilities, such as off-site *response forces.*"

- INFCIRC/225/Rev.5, para. 3.60:

"The coordination between the *guards* and *response forces* during a *nuclear security event* should be regularly exercised. In addition, other facility personnel should be trained and prepared to act in full coordination with the *guards*, *response forces* and other response teams for implementation of the plans."

For unauthorized removal, Category III, limited access area:

- INFCIRC/225/ Rev.5, para. 4.20:

"The State should ensure that *response forces* are familiarized with the site and *nuclear material* locations and have adequate knowledge of radiation protection to ensure that they are fully prepared to conduct necessary response actions, considering their potential impact on safety."

For unauthorized removal, Category II, protected area:

- INFCIRC/225/ Rev.5, para. 4.30:

"A permanently staffed *central alarm station* should be provided for monitoring and assessment of alarms, initiation of response, and communication with the *guards*, *response forces*, and facility management. Information acquired at the *central alarm station* should be stored in a secure manner. The *central alarm station* should normally be located in a *protected area* and protected so that its functions can continue in the presence of a *threat*, e.g. hardened. Access to the *central alarm station* should be strictly minimized and controlled."

- INFCIRC/225/ Rev.5, para. 4.33:

"A 24 hour guarding service and *response forces* should be provided to counter effectively any attempted *unauthorized removal*. The *central alarm station* personnel and off-site *response forces* should communicate at scheduled intervals. The *guard*s and *response forces* should be trained and adequately equipped for their functions in accordance with national laws and regulations."

- INFCIRC/225/ Rev.5, para. 4.34:

"The *guards* should conduct random patrols of the *protected area*. The main functions of the patrols should be to:

- Deter an adversary;
- Detect intrusion;
- Inspect visually the physical protection components;
- Supplement the existing *physical protection measures*;
- Provide an initial response."

For unauthorized removal, Category I, inner area:

- INFCIRC/225/ Rev.5, para. 4.49:

"*Guards* and *response forces* should provide an effective and timely response to prevent an adversary from completing the *unauthorized removal*. At least annually, *performance testing* of the *physical protection system* should include appropriate exercises, for example *force-on-force exercises*, to determine if the *guards* and the *response forces* can reach this objective."

For sabotage, unacceptable radiological consequences:

- INFCIRC/225/ Rev.5, para. 5.14:

"The *physical protection system* should be designed to deny unauthorized access of persons or equipment to the targets, minimize opportunity of *insiders*, and to protect the targets against possible *stand-off attacks* consistent with the State's *threat assessment* or *design basis threat*. The response strategy should include denial of adversary access to the *sabotage* targets or denial of adversary task completion at the *sabotage* targets. Denying access to the targets or denial of adversary task completion is accomplished by the primary physical protection functions of *detection*, delay and response, whereas protecting against *stand-off attacks* involves facility design considerations, barrier design considerations to implement a stand-off distance, and other disruption measures."

For sabotage, high radiological consequences, vital area:

- INFCIRC/225/ Rev.5, para. 5.36:

"A permanently staffed *central alarm station* should be provided for monitoring and assessment of alarms, initiation of response, and communication with the *guards*, *response forces*, and facility management. Information acquired at the *central alarm station* should be stored in a secure manner. The *central alarm station* should normally be located in a *protected area* and protected so that its functions can continue in the presence of a *threat*, e.g. hardened. Access to the *central alarm station* should be strictly minimized and controlled. Provisions, including redundancy measures, should be in place to ensure that the functions of the *central alarm station* in monitoring and assessment of alarms, initiation of response and communication can continue during an emergency (e.g. backup alarm station)."

- INFCIRC/225/ Rev.5, para. 5.39:

"A 24 hour guarding service and *response forces* should be provided to ensure an adequate and timely response to prevent an adversary from completing an act of *sabotage*. The *central alarm station* personnel and off-site *response forces* should communicate at scheduled intervals. The *guards* and *response forces* should be trained and adequately equipped for their function in accordance with national laws and regulations."

- INFCIRC/225/ Rev.5, para. 5.40:

"The *guards* should conduct random patrols of the *protected area*. The main functions of the patrols should be to:

- Deter an adversary;
- Detect intrusion;
- Inspect visually the physical protection components;
- Supplement the existing *physical protection measures*;
- Provide an initial response."

(c) Documentation

- Guard post functions, locations, staffing and scheduling;
- Procedures;
- Rosters;
- Exercise data;
- Training reports;
- Shift plans;
- Example shift reports.
- Memorandum of Understanding between facility and off-site response force and other entities.

(d) Review points/specimen questions

Determine:

- If 24 hour guarding service and response forces availability is provided.
- If other facility personnel are trained and prepared to act in full coordination with the guards, response forces and other response teams for implementation of the plans.
- If the central alarm station personnel and off-site response forces communicate at scheduled intervals.
- If the guards and response forces are trained and adequately equipped for their function in accordance with national laws and regulations.
- If the guards conduct random patrols of the protected area.

- If guards and response forces provide an effective and timely response to prevent an adversary from completing the unauthorized removal or sabotage.
- The level of education and training of the guards. Is it planned and correctly implemented (more generally sustainable)?
- If the different roles of the guards are clearly identified.
- If they know the procedures well. How are they tested? Feedback of interventions?
- What knowledge the guards have about the facilities. Do they often go there? Do they know the operators well and do they interact with them?
- What the different equipment of the guards is during an intervention, especially their communication equipment.
- Which organization(s) provides armed response.
- If there is a Memorandum of Understanding with each external response organization, and does it address response time, number of responders and their categories/capabilities.
- What site familiarization has been provided to guards and response forces, including off-site responders.
- What the response strategies are for theft and sabotage.
- If guards and response forces are allowed access to the inner areas and vital areas.
- How a potential insider in the guards or response forces could be detected.
- If the internal response forces building is the same as the CAS building. What protection has this building?
- Commitments from the off-site response force are adequate and timely.
- If the on- and off-site response forces are sufficient in numbers and are adequately trained and equipped to deal with the DBT.
- If the on-site security force participates in exercises (the date and scenario of recent exercises, exercise outcomes).
- If the off-site response force and the on-site security force participate in joint exercises (the date and scenario of recent exercises, exercise outcomes).
- If the on-site and off-site response forces are familiar with the facility.
- If procedures facilitate the off-site response force's immediate access to, and deployment within, the nuclear facility.
- If the response measures are conducted taking account of facility hazards.
- If guards know the law and policy for the use of deadly force.
- If security personnel are knowledgeable and functionally capable with respect to their emergency (contingency?) response roles and responsibilities.

3.7.4.2. Guard and response communications

(a) Objective

- Determine what communication systems are available in order to provide situational awareness to all bodies involved in guarding and responding to a nuclear security event and during routine operations.

(b) Basis

For unauthorized removal, Category II, protected area:

- INFCIRC/225/Rev.5, para. 4.30:

"A permanently staffed *central alarm station* should be provided for monitoring and assessment of alarms, initiation of response, and communication with the *guards*, *response forces*, and facility management. Information acquired at the *central alarm station* should be stored in a secure manner. The *central alarm station* should normally be located in a *protected area* and protected so that its functions can continue in the presence of a *threat*, e.g. hardened. Access to the *central alarm station* should be strictly minimized and controlled."

- INFCIRC/225/Rev.5, para. 4.31:

"Alarm equipment, alarm communication paths, and the *central alarm station* should be provided with an uninterruptible power supply and be tamper protected against unauthorized monitoring, manipulation and falsification."

- INFCIRC/225/Rev.5, para. 4.32:

"Dedicated, redundant, secure and diverse transmission systems for two way voice communication between the *central alarm station* and the *response forces* should be provided for activities involving *detection*, assessment and response. Dedicated two way secure voice communication should be provided between *guards* and the *central alarm station*."

- INFCIRC/225/Rev.5, para. 4.33:

"A 24 hour guarding service and *response forces* should be provided to counter effectively any attempted *unauthorized removal*. The *central alarm station* personnel and off-site *response forces* should communicate at scheduled intervals. The *guard*s and *response forces* should be trained and adequately equipped for their functions in accordance with national laws and regulations."

For unauthorized removal, Category I, inner area:

- INFCIRC/225/Rev.5, para. 4.47:

"Provisions, including redundancy measures, should be in place to ensure that the functions of the *central alarm station* in monitoring and assessment of alarms, initiation of response and communication can continue during an emergency (e.g. a backup alarm station)."

For sabotage, high radiological consequences, vital area:

- INFCIRC/225/Rev.5, para. 5.36:

"A permanently staffed *central alarm station* should be provided for monitoring and assessment of alarms, initiation of response, and communication with the *guards*, *response forces*, and facility management. Information acquired at the *central alarm station* should be stored in a secure manner. The *central alarm station* should normally be located in a *protected area* and protected so that its functions can continue in the presence of a *threat*, e.g. hardened. Access to the *central alarm station* should be strictly minimized and controlled. Provisions, including redundancy measures, should be in place to ensure that the functions of the *central alarm station* in monitoring and assessment of alarms, initiation of response and communication can continue during an emergency (e.g. backup alarm station)."

- INFCIRC/225/Rev.5, para. 5.37:

"Alarm equipment, alarm communication paths, and the *central alarm station* should be provided with an uninterruptible power supply and be tamper-protected against unauthorized monitoring, manipulation and falsification."

- INFCIRC/225/Rev.5, para. 5.38:

"Dedicated, redundant, secure and diverse transmission systems for two way voice communication between the *central alarm station* and the *response forces* should be provided for activities involving *detection*, assessment and response. Dedicated two way secure voice communication should be provided between *guards* and the *central alarm station*."

- INFCIRC/225/Rev.5, para. 5.39:

"A 24 hour guarding service and *response forces* should be provided to ensure an adequate and timely response to prevent an adversary from completing an act of *sabotage*. The *central alarm station* personnel and off-site *response forces* should communicate at scheduled intervals. The *guard*s and *response forces* should be trained and adequately equipped for their function in accordance with national laws and regulations."

(c) Documentation

- Communication plan/design;
- Communications protocol/procedure;

- Contingency plan.

(d) Review points/specimen questions

Determine if and how:

- The CAS and members of the security staff initiate and receive communications (i.e. radio or telephone) that are clear and intelligible, with other members of the security staff during the performance of any assigned duty.
- The CAS has dedicated, redundant and diverse means of communication, e.g. radio or direct telephone line, for contact with a response force.
- The CAS is equipped with a duress alarm (or similar device) that can be used at any time to alert a response force.
- The CAS is equipped with recording equipment to record all communications traffic.
- All transmission lines are supervised, i.e. tamper indicating.
- The CAS protects sensitive communication, i.e. radio communication during emergency situations between the CAS and the emergency services.
- Failures of the communication systems are handled.
- Communications are protected against listening in and jamming.
- Records of communications surveillance checks with various security emergency coordinating agencies are being maintained.
- There is a secondary alarm station.
- All guards and response forces are able to communicate with each other during a nuclear security event, as needed.
- Contact lists are available and updated regularly.

3.7.4.3. Equipment, armament and transportation

(a) Objective

- Determine if security staff are adequately equipped and trained (list of documents referring to training) to perform their duties.

(b) Basis

- INFCIRC/225/Rev.5, para. 4.33:

"A 24 hour guarding service and *response forces* should be provided to counter effectively any attempted *unauthorized removal*. The *central alarm station* personnel and off-site *response forces* should communicate at scheduled intervals. The *guard*s and *response forces* should be trained and adequately equipped for their functions in accordance with national laws and regulations."

- INFCIRC/225/Rev.5, para. 5.39:

"A 24 hour guarding service and *response forces* should be provided to ensure an adequate and timely response to prevent an adversary from completing an act of *sabotage*. The *central alarm station* personnel and off-site *response forces* should communicate at scheduled intervals. The *guard*s and *response forces* should be trained and adequately equipped for their function in accordance with national laws and regulations."

(c) Documentation

- List of equipment, weapons and transport vehicles held by guard and response force organizations and position;
- Memorandum of Understanding between guards and response forces;
- Training plan, schedule and records.

(d) Review points/specimen questions

Determine:

- If security staff have sufficient resources, e.g. vehicles, communications equipment, appropriate clothing, computers and firearms to perform their duties properly, including incident response.
- If guard and response forces equipment, weapons and vehicles are adequate to counter the capabilities of the threat/DBT.
- If compensatory measures exist what they are.
- If performance standards exist with off-site response and what they are.

4. TRANSPORT REVIEW (MODULE 3)

4.1. INTRODUCTION

The IPPAS transport review module provides guidelines for the comprehensive review of physical protection as it exists during the transport of nuclear material. The review provides the Member State with an independent assessment of the status of physical protection during a transport selected by the State. The IPPAS mission provides advice to assist the State in the form of recommendations and suggestions. The mission recognizes good practices by shippers, carriers and receivers, which could be incorporated into international guidance. The mission involves meetings with representatives of the competent authority and with other organizations that have responsibilities for the physical protection of nuclear material during transport. This review, conducted by an IPPAS team, does not replace the regulatory function of the State's competent authority.

The review is based on obligations imposed by the CPPNM (INFCIRC/274) and its Amendment (GOV/INF/2005/10-GC(49)/INF/6), and recommendations and guidance provided by the IAEA's IAEA NSS publications, rather than on State regulatory requirements.

An IPPAS national review is the recommended starting point for host countries wishing to have their nuclear security regime reviewed against international instruments, recommendations and guidance. Module 1 of the IPPAS Guidelines includes State responsibilities related to transport security and should be completed as a prelude to the transport security review covered in this module.

The objectives of the transport review are to:

- Provide an independent assessment of a selected physical protection system for transport as agreed to by the IAEA and the host country;
- Provide advice to a Member State (competent authority) in the form of recommendations, suggestions and the recognition of good practices;
- Share experience in the conduct of a detailed transport physical protection assessment;
- Provide a basis for assistance to the requesting Member State in implementing upgrades.

The transport review evaluates the physical protection system of nuclear material during transport in order to answer the following questions:

- Does the physical protection system correspond to international instruments, IAEA recommendations and guidance?
- Does the physical protection system function as designed?
- Does the physical protection system appear adequate to counter the threat with regard to transport of nuclear material, in accordance with information available to the IPPAS team?
- Is the system effective and well maintained?

- Is the transport security organization sufficiently staffed, trained and equipped to carry out its assigned responsibilities?

4.2. PURPOSE

The purpose of this publication is to provide guidelines for IPPAS team members in the conduct of a transport security review. The review points/specimen questions should not be used as a simple yes/no checklist but rather as questions which allow the interviewer to gain an appreciation of the subject and, as appropriate, to compare implementation with international instruments, IAEA recommendations and guidance, and accepted international best practice. The guidance provided in this publication can be used by a State to conduct a self-assessment of its own transport physical protection requirements and implementation against accepted international criteria and practice.

4.3. MISSION SCOPE

The mission can fully assess the entire physical protection system for all modes of transport (including trans-shipment/transit) or, at the direction of the host country, be tailored to concentrate on particular aspects.

A transport review may address the following areas:

- Transport security management programme:
    - Threat and target identification;
    - Allocation of responsibilities;
    - Transport security plan, including contingency plan;
    - Interfaces with safety and nuclear material accountancy and control;
    - Security staff training and qualifications;
    - Security culture;
    - Confidentiality;
    - Trustworthiness;
    - Reporting;
    - System evaluation, including performance testing;
    - Quality assurance;
    - Sustainability programme.
- Transport physical protection system:

    Detection:

    - Access control;
    - Surveillance;
    - Transport control centre.

    Delay:

    - Resistance to forcible attack;
    - Disabling devices.

Response:

- Guards and response forces;
- Communications;
- Equipment.

4.4. TRANSPORT SPECIFIC PHYSICAL PROTECTION REVIEW PROCESS

Before conducting an assessment of security during transport of nuclear material, the IPPAS mission team should be familiar with the following documentation, as made available by the host country (also see Module 1 for State level transport security information):

- The relevant aspects of the Member State's legislative and regulatory infrastructure, including establishment of the transport security competent authority, its legislative mandate, licensing regime and powers regarding physical protection regulation;
- The Member State's transport physical protection regulations, including assignment of physical protection responsibilities to shippers, carriers and receivers;
- The Member State's approach to threat assessment and DBT;
- General information on the number and types of shipment occurring within the host country.

Whereas the review of the transport organization and management programme to a large degree will be based on documentation and interviews with the relevant staff, the review of areas such as detection, delay and response requires more information on the practical implementation of physical protection measures during transport. Observing an actual transport or a transport exercise by the IPPAS members combined with an information session provided by the licence holders and relevant staff is invaluable in this regard. IPPAS members should not hesitate to ask questions of the host country's representatives to gain a clear understanding of the operation.

When reviewing transport security programmes and operations, it is imperative to keep the 'graded approach' in mind (as referred in INFCIRC/225/Rev.5, para. 6.6). There are numerous requirements that apply to all categories of nuclear material that must be applied in an increasingly stringent manner, as the nuclear material category dictates. The reviewer should always evaluate the transport security system with this in mind.

Some requirements only apply to specified categories of nuclear material. Requirements in the following paragraphs of INFCIRC/225/Rev.5 only apply to the specified nuclear material category:

- All nuclear material: Paras 6.6–6.10;
- Categories I, II and III: Paras 6.11–6.18;
- Categories I and II: Paras 6.19–6.31;
- Category I: Paras 6.32–6.43.

The following sections are intended to provide a summary of the specific objectives of the physical protection requirements for distinct fields of the physical protection regime and examples of possible questions to be asked and data to be collected in the review process.

4.5. TRANSPORT SECURITY MANAGEMENT PROGRAMME

4.5.1. Threat and target identification

4.5.1.1. Objectives

- To determine if transport security threats have been identified and taken into account in the design of the transport physical protection system.
- To determine if potential targets have been identified on the basis of:
    - Nuclear material category;
    - Radioactive material properties;
    - Potential radiological consequences due to an act of sabotage.

4.5.1.2. Basis

- Nuclear Security Fundamentals, IAEA NSS No. 20: Essential Element 9: Use of Risk Informed Approaches:

"A *nuclear security regime* uses risk informed approaches, including in the allocation of resources for *nuclear security systems* and *nuclear security measures* and in the conduct of nuclear security related activities that are based on a *graded approach* and *defence in depth*, which take into account the following:

(a) The State's current assessment of the *nuclear security threats*, both internal and external;

(b) The relative attractiveness and vulnerability of identified *targets* to *nuclear security threats*;

(c) Characteristics of the *nuclear material*, *other radioactive material*, *associated facilities* and *associated activities*;

(d) Potential harmful consequences from criminal or intentional unauthorized acts involving or directed at *nuclear material*, *other radioactive material*, *associated facilities*, *associated activities*, *sensitive information* or *sensitive information assets*, and other acts determined by the State to have an adverse impact on nuclear security."

- CPPNM Amendment, Fundamental Principle G: Threat:

"The State's physical protection should be based on the State's current evaluation of the threat."

- CPPNM Amendment, Fundamental Principle H: Graded Approach:

"Physical protection requirements should be based on a graded approach, taking into account the current evaluation of the threat, the relative attractiveness, the nature of the material and potential consequences associated with the unauthorized removal of nuclear material and with the sabotage against nuclear facilities or nuclear material."

- INFCIRC/225/Rev.5, para. 6.1:

"Levels of protection defined in this section are based on categorization of *nuclear material* for use in the construction of a nuclear explosive device. However, *nuclear material* is radioactive material, which has also to be protected against *unauthorized removal* since it could have significant consequences if dispersed or used otherwise for a malicious purpose. Protection requirements against *unauthorized removal* of *nuclear material* for potential subsequent off-site radiological dispersal are provided in IAEA Nuclear Security Series No. 14, Nuclear Security Recommendations on Radioactive Material and Associated Facilities."

- INFCIRC/225/Rev.5, para. 6.2:

"These two sets of requirements for protection against *unauthorized removal* should be considered and implemented in a manner that the more stringent requirements for physical protection are applied."

- INFCIRC/225/Rev.5, para. 6.3:

"When implementing requirements for protection against *unauthorized removal*, the requirements for the protection against *sabotage* addressed in paras 6.56–6.59 should also be taken into account. Appropriate *physical protection measures* should then be designed based on the more stringent applicable requirements and implemented for both in an integrated manner."

- INFCIRC/225/Rev.5, para. 6.4:

"Table 1 in Section 4 is the basis for a *graded approach* to protection against *unauthorized removal* during *transport* of *nuclear material* that could be used in a nuclear explosive device."

- INFCIRC/225/Rev.5, para. 6.5:

"The total amount of *nuclear material* on or in a single *conveyance* should be aggregated to determine a categorization and identify the appropriate protection requirements for the *conveyance*. When different types of *nuclear material* are transported on the same *conveyance*, an appropriate aggregation formula should be used to determine the category of the consignment."

4.5.1.3. Documentation

- Process for conducting transport threat assessment and defining the DBT and assumptions regarding current/recent threat information;
- Examples of nuclear material shipment inventory, including categories and consequences.

4.5.1.4. Data to be collected/specimen questions

Determine if and how:

- The threat is taken into account in design of the transport physical protection system.
- The possibility of a local threat has been considered in addition to the State defined DBT, recognizing the likelihood of the threat occurring during the transport.
- The shipper and/or carrier know and understand the transport specific threat.
- The shipper has identified all theft targets, including Category I, II and III nuclear material, their quantity, size and form.
- The graded approach used for protection against unauthorized removal during transport is based on the categorization table in Chapter 5 of INFCIRC/225/Rev.5.
- The total quantity of nuclear material on or in a single conveyance is aggregated to determine a categorization and identify the appropriate protection requirements for the conveyance.
- The shipper has identified and evaluated any nuclear material, the sabotage of which could directly or indirectly lead to potential radiological consequences exceeding the State's definition of unacceptable radiological consequences.
- The results of the nuclear material evaluations (nuclear material category, radiological nature and potential consequences of sabotage) have been considered during design of the physical protection system.
- Consideration is given to the various types of adversary, i.e. outsiders, insiders, and outsiders in collusion with insiders, their scenario tactics, motivations, capabilities and any other threat information.
- There is a description of the scenarios used to effect an unauthorized removal during transport or a radiological release as a result of sabotage.

4.5.2. Allocation of responsibilities

4.5.2.1. Objective

- To determine if the transport security allocation of responsibilities is adequate and addressed in the management system.

4.5.2.2. Basis

- CPPNM Amendment, Fundamental Principle B: Responsibilities during International Transport:

"The responsibility of a State for ensuring that nuclear material is adequately protected extends to the international transport thereof, until that responsibility is properly transferred to another State, as appropriate."

- CPPNM Amendment, Fundamental Principle E: Responsibility of the Licence Holders:

"The responsibilities for implementing the various elements of physical protection within a State should be clearly identified. The State should ensure that the prime responsibility for the implementation of physical protection of nuclear material or of nuclear facilities rests with the holders of the relevant licences or of other authorizing documents (e.g. operators or shippers)."

- INFCIRC/225/Rev.5, para. 3.24:

"The *operator*, *shipper* and carrier should comply with all applicable regulations and requirements established by the State and the *competent authority*."

- INFCIRC/225/Rev.5, para. 3.25:

"The *operator*, *shipper* and carrier should cooperate and coordinate with all other State entities having physical protection responsibilities, such as off-site *response forces*."

For Categories I and II:

- INFCIRC/225/Rev.5, para. 6.27:

"Personnel with physical protection responsibilities should be given written instructions that, when appropriate, have been approved by the *competent authority*, detailing their responsibilities during the *transport*."

4.5.2.3. Documentation

- Transport security organization chart;
- Information on specific responsibilities assigned to organizations and individuals;
- Written instructions for individuals with physical protection responsibilities;
- Licences or other authorizations for performing functions (e.g. carrier, shipper).

4.5.2.4. Data to be collected/specimen questions

Determine if and how:

- The shipper and/or carrier ensure proper handover of physical protection responsibilities during international transport.
- A clear transport security organization scheme exists, including the transport control centre.
- Responsibilities of security management and staff are clearly defined and understood for normal operating conditions and for nuclear security events (including shippers, carriers and receivers).
- All security activities are covered by documented procedures.
- All security staff are held accountable for assigned responsibilities.
- At least one full-time senior member of the security organization, who has the authority to direct the security activities of the organization, is available at all times.
- Personnel with physical protection responsibilities are given written instructions detailing their responsibilities during the transport.
- Physical protection responsibilities are clearly defined when multiple carriers, intermodal transfers and international shipments are involved.

4.5.3. Transport security plan, including contingency plan

4.5.3.1. Objectives

- To determine if an adequate transport security plan exists and is implemented for each shipment of nuclear material.
- To determine if a transport security contingency plan exists and if it is regularly reviewed, updated and exercised and complements the emergency plan.

4.5.3.2. Basis

- CPPNM Amendment, Fundamental Principle K: Contingency Plans:

"Contingency (emergency) plans to respond to unauthorized removal of nuclear material or sabotage of nuclear facilities or nuclear material, or attempts thereof, should be prepared and appropriately exercised by all licence holders and authorities concerned."

- INFCIRC/225/Rev.5 para. 3.45:

"State requirements for physical protection should be based on the concept of *defence in depth*. The concept of physical protection is one which requires a designed mixture of hardware (security devices), procedures (including the organization of *guards* and the performance of their duties) and facility design (including layout)."

- INFCIRC/225/Rev.5, para. 3.46:

"The three physical protection functions of *detection*, delay, and response should each use *defence in depth* and apply a graded approach to provide appropriate effective protection."

- INFCIRC/225/Rev.5, para. 3.47:

"*Defence in depth* should take into account the capability of the *physical protection system* and the *system for nuclear material accountancy and control* to protect against *insiders* and external threats."

- INFCIRC/225/Rev.5, para. 6.6:

"Physical protection against *unauthorized removal* during *transport* should encompass, as far as operationally practicable in accordance with the *graded approach*:

(a) Minimizing the total time during which the *nuclear material* remains in *transport*;
(b) Minimizing the number and duration of *nuclear material* transfers, i.e. transfer from one *conveyance* to another, transfer to and from temporary storage and temporary storage while awaiting the arrival of a *conveyance*, etc.;
(c) Protecting *nuclear material* during *transport* and in temporary storage in a manner consistent with the category of that *nuclear material*;
(d) Avoiding the use of predictable movement schedules by varying times and routes;
(e) Requiring predetermination of the trustworthiness of individuals involved during *transport* of *nuclear material*;
(f) Limiting advance knowledge of transport information to the minimum number of persons necessary;
(g) Using a material transport system with passive and/or active *physical protection measures* appropriate for the *threat assessment* or *design basis threat*;
(h) Using routes which avoid areas of natural disaster, civil disorder or with a known threat; and,
(i) Ensuring that packages and/or *conveyances* are not left unattended for any longer than is absolutely necessary."

- INFCIRC/225/Rev.5, para. 6.8:

"Before commencing an international shipment, the *shipper* should ensure that the arrangements are in accordance with the physical protection regulations of the receiving State and of other States which are transited."

- INFCIRC/225/Rev.5, para. 6.10:

"If the *conveyance* makes an unexpected extended stop, the *physical protection measures* appropriate for that category of material in storage should be applied to the extent possible and practicable. Physical protection of *nuclear material* in storage incidental to *transport* should be at a level appropriate for the

category of the *nuclear material* and provide a level of protection consistent with that required in Section 4 for use and storage."

For Categories I, II and III:

- INFCIRC/225/Rev.5, para. 6.12:

"The carrier should give the receiver advance notification of the planned shipment specifying the mode of *transport* (road/rail/water/air), the estimated time of arrival of the shipment and the exact point of handover if this is to be done at some intermediate point before the ultimate destination. This advance notification should be supplied in time to enable the receiver to make adequate physical protection arrangements."

- INFCIRC/225/Rev.5, para. 6.13:

"Physical protection during *transport* should include prior agreement among *shipper*, receiver, and carrier, specifying time, place and procedures for transferring physical protection responsibilities."

- INFCIRC/225/Rev.5, para. 6.16:

"There should be a detailed search of the *conveyance* to ensure that nothing has been tampered with and that nothing has been affixed to the package or *conveyance* that might compromise the security of the consignment."

For Categories I and II:

- INFCIRC/225/Rev.5, para. 6.21:

"The receiver should confirm readiness to accept delivery (and handover, if applicable) at the expected time, prior to the commencement of the shipment."

- INFCIRC/225/Rev.5, para. 6.22:

"A transport security plan should be submitted by the *shipper* and/or carrier as appropriate to the *competent authority* for approval. A plan may cover a series of similar movements. This plan should address routing of the shipment, stopping places, destination handover arrangements, identification of persons authorized to take delivery, accident procedures, reporting procedures, both routine and emergency, and, as appropriate, *contingency plans*. In choosing the route, the capabilities of the *response forces* should be taken into account. Exercises should be conducted to assess and validate the transport security plan and to train the participants on how to respond to *nuclear security events*."

- INFCIRC/225/Rev.5, para. 6.23:

"Prior to commencing *transport*, the carrier should verify that all *physical protection measures* are in place in accordance with the transport security plan."

- INFCIRC/225/Rev.5, para. 6.31:

"Depending on the mode of *transport*, the consignment should be shipped by:

- Road, under exclusive use conditions; or
- Rail, where operationally practicable, in a freight train in an exclusive use fully enclosed and locked *conveyance*; or
- Water, in a secure compartment or container which is locked and sealed; or
- Air, in an aircraft designated for cargo only and in a secure compartment or container which is locked and sealed.

While *nuclear material* is on board pending departure, provisions should be made for sufficient *access delay* or compensating measures to meet the *threat assessment* or *design basis threat*."

For Category I:

- INFCIRC/225/Rev.5, para. 6.33:

"The approval by the *competent authority* of the transport security plan should be based on a detailed examination of proposed *physical protection measures*, which should provide sufficient delay so that *guards* and/or *response forces* have time to intervene to prevent *unauthorized removal*. The transport security plan should include the route and arrangements for making changes, such as alteration of the route during the shipment, in response to unexpected changes in the physical environment, *threat assessment* and operating conditions."

- INFCIRC/225/Rev.5, para. 6.34:

"A further authorization by the *competent authority* of the shipment should be required just prior to commencing *transport* and should be conditional on a current *threat assessment* and intelligence information and, where appropriate, on a detailed route surveillance to observe the current environment. The consent to a *transport* operation can include specific limitations and conditions related to the particular circumstances."

- INFCIRC/225/Rev.5, para. 6.42:

"Shipment by water should be carried out on a dedicated transport vessel."

- INFCIRC/225/Rev.5, para. 6.43:

"Shipment by air should be by aircraft designated for cargo only and on which the *nuclear material* is its sole cargo."

For location and recovery of missing or stolen material:

- INFCIRC/225/Rev.5, para. 6.47:

"The State should ensure that *contingency plans* — including interfaces with safety, as appropriate — are established by carriers and/or other relevant entities to locate and recover any missing or stolen *nuclear material* that occurs during *transport*."

- INFCIRC/225/Rev.5, para. 6.49:

"For the coordination of location and recovery operations, the State should develop arrangements and protocols between appropriate State response organizations, carriers and/or other relevant entities. The arrangements should be clearly documented and this documentation should be made available to all relevant organizations."

- INFCIRC/225/Rev.5, para. 6.50:

"The State should ensure that appropriate State response organizations, carriers and/or other relevant entities conduct exercises to assess and validate the *contingency plans* and also to train the various participants on how to react in such a situation."

- INFCIRC/225/Rev.5, para. 6.52:

"The carrier should be alert during *transport* for any indications that packages have been removed from the *conveyance* or tampered with and should verify during delivery that no packages are missing or have been tampered with."

- INFCIRC/225/Rev.5, para. 6.53:

"The carrier should take immediate action to determine if missing packages are misplaced but still under its control."

- INFCIRC/225/Rev.5, para. 6.54:

"If packages are determined to be missing or have been tampered with, the carrier should immediately report this to relevant authorities and the *shipper*."

- INFCIRC/225/Rev.5, para. 6.55:

"The carrier should provide any requested assistance to the appropriate State organizations to locate and recover *nuclear material* and should cooperate during subsequent investigations and prosecution."

For protection against sabotage:

- INFCIRC/225/Rev.5 para. 6.57:

"When implementing requirements for protection against *sabotage*, the requirements for the protection against *unauthorized removal* addressed in paras 6.1–6.43 should also be taken into account. Appropriate *physical protection measures* should then be designed based on the more stringent applicable requirements and implemented for both in an integrated manner."

- INFCIRC/225/Rev.5, para. 6.59:

"If the current or potential *threat* warrants additional *physical protection measures* to protect against *sabotage*, consideration should be given to:

- Postponing the shipment;
- Rerouting the shipment to avoid high *threat* areas;
- Enhancing the robustness of the package or the *conveyance*;
- Detailed route surveillance to observe the current environment;
- Providing (additional) *guards*."

For mitigation or minimization of radiological consequences of sabotage:

- INFCIRC/225/Rev.5, para. 6.63:

"The State should ensure that *contingency plans* — including interfaces with safety, as appropriate — are established by carriers and/or other relevant entities."

- INFCIRC/225/Rev.5, para. 6.70:

"The carrier should prepare transport personnel to act in full coordination with *guards*, *response forces* and law enforcement agencies for implementing the *contingency plan*."

- INFCIRC/225/Rev.5, para. 6.73:

"Immediately following an act of *sabotage*, the carrier and/or *guards* should take measures to secure the *transport* and minimize the consequences of the act."

4.5.3.3. Documentation

- Transport security plan(s);
- Shipment authorization documentation;
- Contingency plan(s), including chain of command;
- Emergency plan.

4.5.3.4. Data to be collected/specimen questions

Determine if and how:

- The transport plan addresses both unauthorized removal and sabotage.
- The physical protection system includes a designed mixture of hardware (security devices and features) and procedures (including the organization of guards and the performance of their duties).
- The three physical protection functions of detection, delay and response each use defence in depth and apply a graded approach to provide appropriate effective protection.
- Defence in depth takes into account the capability of the physical protection system and the system for nuclear material accountancy and control to protect against insiders and external threats.
- The number of security staff on duty complies with staffing requirements.
- Sufficient personnel and appropriate structures are available to enable the security functions to be performed, including incident response.
- Physical protection during transport includes prior agreement among shipper, receiver and carrier, specifying time, place and procedures for transferring physical protection responsibilities.
- Physical protection against unauthorized removal during transport encompasses, as far as operationally practicable and in accordance with the graded approach:
    - Minimizing the total time during which the nuclear material remains in transport;
    - Minimizing the number and duration of nuclear material transfers, i.e. transfer from one conveyance to another, transfer to and from temporary storage and temporary storage while awaiting the arrival of a conveyance, etc.;
    - Protecting nuclear material during transport and in temporary storage in a manner consistent with the category of that nuclear material;
    - Avoiding the use of predictable movement schedules by varying times and routes;
    - Using routes which avoid areas of natural disaster, civil disorder or with a known threat;
    - Ensuring that packages and/or conveyances are not left unattended for any longer than is absolutely necessary.

- Before commencing an international shipment, the shipper ensures that the arrangements are in accordance with the physical protection regulations of the receiving State and of other States which are transited.
- Arrangements are in place so that if the conveyance makes an unexpected extended stop, physical protection measures appropriate for that category of material in storage are applied to the extent possible and practicable.
- Physical protection of nuclear material in storage incidental to transport is at a level appropriate for the category of the nuclear material and provides a level of protection consistent with that required for use and storage.
- The carrier gives the receiver advance notification of the planned shipment, specifying the mode of transport (road/rail/water/air), the estimated time of arrival of the shipment and the exact point of handover, if this is to be done at some intermediate point before the ultimate destination.
- This advance notification is supplied in time to enable the receiver to make adequate physical protection arrangements.
- The receiver checks the integrity of the packages, and locks and seals when used, and accepts the shipment immediately upon arrival.
- The receiver notifies the shipper of the arrival of the shipment immediately or, for non-arrival, within a reasonable interval after the estimated time of arrival at the destination.
- The carrier has suitable procedures to detect any indications that packages have been removed from the conveyance or tampered with and to verify upon delivery that no packages are missing or have been tampered with.
- The carrier is prepared to take immediate action to determine if missing packages are misplaced but still under its control.
- There are arrangements for the carrier to provide any requested assistance to the appropriate State organizations to locate and recover nuclear material and during subsequent investigations and prosecution.
- The current or potential threat is taken into account to determine if additional physical protection measures to protect against sabotage are required.
- The carrier prepares transport personnel to act in full coordination with guards, response forces and law enforcement agencies for implementing the contingency plan.
- Contingency plans address attempts at the unauthorized removal of nuclear material, loss of nuclear material and sabotage of nuclear material.
- All appropriate organizations are involved in contingency planning and that their roles are clearly defined.
- Capabilities specific to contingency plans (training, equipment, contact lists) are available and functional.
- For Categories I and II material, the contingency plans are appropriately reflected in the transport security plan.

- The response forces are familiar with typical transport operations and threats, including radiation protection considerations.
- Transport personnel are aware of their responsibilities during security events and emergency situations.

For Categories I and II material, determine if and how:

- A transport security plan is submitted by the shipper and/or carrier as appropriate to the competent authority for approval.
- The transport security plan addresses:
    - Routing of the shipment;
    - Stopping places;
    - Destination handover arrangements;
    - Identification of persons authorized to take delivery;
    - Accident procedures;
    - Reporting procedures, both routine and emergency;
    - Contingency plans, as appropriate.
- The transport security plan is periodically reviewed and updated as necessary.
- After each shipment, or as appropriate at regular periodicity, there is an operational review to identify potential improvements and that any such improvements are incorporated into the subsequent transport security plans.
- What criteria are used to select the route.
- In choosing the route, the capabilities of the response forces are taken into account.
- Exercises are conducted to assess and validate the transport security plan and to train the participants on how to respond to nuclear security events.
- The receiver confirms readiness to accept delivery (and handover, if applicable) at the expected time, prior to the commencement of the shipment.
- Prior to commencing transport, the carrier verifies that all physical protection measures are in place in accordance with the transport security plan.
- Dependent on the mode of transport, the consignment is shipped by:
    - Road, under exclusive use conditions; or
    - Rail, where operationally practicable, in a freight train in an exclusive use fully enclosed and locked conveyance; or
    - Water, in a secure compartment or container which is locked and sealed; or
    - Air, in an aircraft designated for cargo only and in a secure compartment or container which is locked and sealed.

For Category I material, determine if and how:

- The approval by the competent authority of the transport security plan is based on a detailed examination of proposed physical protection measures.
- The physical protection measures provide sufficient delay so that guards and/or response forces have time to intervene to prevent unauthorized removal.
- The transport security plan includes the route and arrangements for making changes, such as alteration of the route during the shipment, in response to unexpected changes in the physical environment, threat assessment and operating conditions.
- A further authorization by the competent authority is required just prior to commencing transport and is conditional on a current threat assessment and intelligence information and, where appropriate, on a detailed route surveillance to observe the current environment.
- The carrier receives current threat information.
- Route surveillance is conducted prior to transport.
- Consent to a transport operation includes specific limitations and conditions related to the particular circumstances.
- Shipment by water is carried out by a dedicated transport vessel.
- Shipment by air is by aircraft designated for cargo only and for which the nuclear material is its sole cargo.

4.5.4. Interfaces with safety and nuclear material accountancy and control

4.5.4.1. Objective

- To identify how the licence holder assesses and manages the physical protection interface with safety and nuclear material accountancy and control activities in a manner that ensures they are mutually supportive and complement each other and that they do not adversely affect each other.

4.5.4.2. Basis

- INFCIRC/225/Rev.5 para. 3.26:

"The *operator* should ensure control of, and be able to account for, all *nuclear material* at a *nuclear facility* at all times. The *operator* should report any confirmed accounting discrepancy in a timely manner as stipulated by the *competent authority*."

- INFCIRC/225/Rev.5, para. 6.18:

"The receiver should check the integrity of the packages, and locks and seals when used, and accept the shipment immediately upon arrival. The receiver should notify the *shipper* of the arrival of the shipment immediately or of non-arrival within a reasonable interval after the estimated time of arrival at the destination."

- INFCIRC/225/Rev.5, para. 6.58:

"In accordance with the fundamental principle of the *graded approach* to physical protection, the State should define protection requirements that correspond to the level of potential radiological consequences. The safety features of the design of the *transport* package, container and *conveyance* should be taken into account when deciding what additional *physical protection measures* are needed to protect the material against *sabotage*."

4.5.4.3. Documentation

- Shipper's procedure for preparing and dispatching packages;
- Receiver's procedure for accepting packages;
- Information on how package, container and conveyance design is taken into account in design of physical protection system against sabotage.

4.5.4.4. Data to be collected/specimen questions

Determine if and how:

- Material is prepared for transport, including accountancy and control, and verification measures (e.g. temporary storage, seals).
- Material is accepted after transport, including nuclear material accountancy and control.
- Contingency plans to locate and recover nuclear material include consideration of radiation and criticality.
- Safety features of the transport packaging (such as materials of construction, size, shape, etc.), container and/or conveyance are taken into account when determining physical protection measures against sabotage.
- Procedures for dealing with emergency situations are consistent for safety and security purposes.

4.5.5. Security staff training and qualifications

4.5.5.1. Objective

- To determine if security staff have the skills, knowledge, and abilities to protect the transport against sabotage and unauthorized removal of nuclear material.

4.5.5.2. Basis

- INFCIRC/225, Rev.5, para. 3.57:

"*Operators*, *shippers* and carriers should establish sustainability programmes for their *physical protection system*. Sustainability programmes should encompass:

- Operating procedures (instructions);
- Human resource management and training
- Equipment updating, maintenance, repair and calibration;
- *Performance testing* and operational monitoring;
- Configuration management (the process of identifying and documenting the characteristics of a facility's *physical protection system* — including computer systems and software — and of ensuring that changes to these characteristics are properly developed, assessed, approved, issued, implemented, verified, recorded and incorporated into the facility documentation);
- Resource allocation and operational cost analysis."

For Categories I and II:

- INFCIRC/225, Rev.5, para. 6.22:

"A transport security plan should be submitted by the *shipper* and/or carrier as appropriate to the *competent authority* for approval. A plan may cover a series of similar movements. This plan should address routing of the shipment, stopping places, destination handover arrangements, identification of persons authorized to take delivery, accident procedures, reporting procedures, both routine and emergency, and, as appropriate, *contingency plans*. In choosing the route, the capabilities of the *response forces* should be taken into account. Exercises should be conducted to assess and validate the transport security plan and to train the participants on how to respond to *nuclear security events*."

For Category I:

- INFCIRC/225, Rev.5, para. 6.35:

"*Guards*, appropriately equipped and trained, should accompany each shipment to protect the *nuclear material*, including before and during loading and unloading operations, to conduct surveillance of the route and to initiate an appropriate response. Continuous, effective surveillance of the packages or locked cargo hold or compartment holding the packages should be maintained by the *guard* at all times, especially when the *conveyance* is not in motion. States are encouraged to use armed *guards* to the extent that laws and regulations permit. When *guards* are not armed, compensating measures should be applied, such as adding delay barriers to the *conveyance* exterior structure and/or interior cargo area."

4.5.5.3. Documentation

- Training plan;
- Training materials;
- Training records;
- Personnel qualification requirements.

4.5.5.4. Data to be collected/specimen questions

Determine if and how:

- Security personnel meet the academic, physical and mental health qualifications required for their assigned functions.
- There is a defined training programme for security personnel, including response to nuclear security events as specified in the transport security plan.
- Security personnel are trained and qualified to perform all assigned physical protection related tasks and duties, including during emergency situations.
- The training is relevant and sound.
- The training includes integration of lessons learned.
- Training and standards records exist, are current, and that personnel training and standards are maintained.

4.5.6. Security culture

4.5.6.1. Objective

- To determine how and the extent to which a transport security culture is established in all organizations involved in a transport (shippers, carriers and receivers).

4.5.6.2. Basis

- CPPNM Amendment, Fundamental Principle F: Security Culture:

"All organizations involved in implementing physical protection should give due priority to the security culture, to its development and maintenance necessary to ensure its effective implementation in the entire organization."

- INFCIRC/225/Rev.5, para. 3.48:

"The foundation of *nuclear security culture* should be the recognition that a credible *threat* exists, that preserving nuclear security is important, and that the role of the individual is important."

- INFCIRC/225/Rev.5, para. 3.49:

"The four component groups — the State, organizations, managers in organizations and individuals — should work together to establish and maintain an effective *nuclear security culture*."

- INFCIRC/225/Rev.5, para. 3.50:

"The State should promote a *nuclear security culture* and encourage all security organizations to establish and maintain one. A *nuclear security culture* should be pervasive in all elements of the *physical protection regime*."

- INFCIRC/225/Rev.5, para. 3.51:

"All organizations that have a role in physical protection should make their responsibilities known and understood in a statement of security policy issued by their executive management to demonstrate the management's commitment to provide guidelines to the staff and to set out the organization's security objectives. All personnel should be aware of and regularly educated about physical protection."

4.5.6.3. Documentation

- Security policy;
- Transport manager handbook;
- Security awareness training programme and records;
- Self-assessment process (plan, records, etc.).

4.5.6.4. Data to be collected/specimen questions

Determine if and how:

- There is a formal security culture policy and programme. Due priority is given to the security culture, to its development and to the maintenance necessary to ensure its effective implementation in the entire organization.
- It is recognized that a credible threat exists, that preserving nuclear security is important, and that the role of the individual is important.

- Managers in organizations and individuals work together to establish, maintain and improve an effective nuclear security culture.
- Nuclear security culture is pervasive in all elements of the physical protection system.
- Organizations make their responsibilities known and understood in a statement of security policy issued by their executive management to demonstrate the management's commitment to providing guidelines to the staff and to setting out the organization's security objectives.
- An employee security awareness programme is implemented and effective.
- Employees are provided with an initial orientation and ongoing training related to their security related responsibilities.

4.5.7. Confidentiality

4.5.7.1. Objective

- To determine what transport security information is deemed sensitive and how it is protected from unauthorized disclosure.

4.5.7.2. Basis

- CPPNM Amendment, Fundamental Principle L: Confidentiality:

"The State should establish requirements for protecting the confidentiality of information, the unauthorized disclosure of which could compromise the physical protection of nuclear material and nuclear facilities."

- INFCIRC/225/Rev.5, para. 3.54:

"Management of a *physical protection system* should limit access to sensitive information to those whose trustworthiness has been established appropriate to the sensitivity of the information and who need to know it for the performance of their duties. Information addressing possible vulnerabilities in *physical protection systems* should be highly protected."

- INFCIRC/225/Rev.5, para. 6.6(f):

"Physical protection against *unauthorized removal* during *transport* should encompass, as far as operationally practicable in accordance with the *graded approach*:

  - Limiting advance knowledge of transport information to the minimum number of persons necessary."

- INFCIRC/225/Rev.5, para. 6.7:

"Appropriate measures, consistent with national requirements and using a *graded approach*, should be taken to protect the confidentiality of information relating to *transport* operations, based on a need to know, including detailed information on the schedule and route. Great restraint should be applied in the use of any special markings on *conveyances*, and also in the use of open channels for transmission of messages concerning shipments of *nuclear material*. When a security related message is transmitted, measures such as coding and appropriate routing should be taken to the extent practicable, and care should be exercised in the handling of such information."

For Categories I and II:

- INFCIRC/225/Rev.5, para. 6.28:

"Particular consideration should be given to ensuring confidentiality of information relating to transport operations, including dissemination only to persons with a need to know this information."

4.5.7.3. Documentation

- Information protection policy;
- Information protection requirements (regulations, orders, etc.);
- Information protection plan and procedures;
- Classification process (company procedures);
- Communications security plan and procedures.

4.5.7.4. Data to be collected/specimen questions

Determine if and how:

- The shipper and carrier have an information security policy and have implemented procedures for the protection and confidentiality of sensitive information.
- Appropriate measures, using a graded approach, are taken to protect the confidentiality of information relating to the design of the physical protection system and to transport operations, based on a need to know, including detailed information on the schedule and route.
- Access to sensitive information is limited to those whose trustworthiness has been established appropriate to the sensitivity of the information.

- Access to sensitive information is limited to personnel who need to know it for the performance of their duties.
- Information addressing possible vulnerabilities in physical protection systems is highly protected.
- Computer based systems are protected against compromise consistent with the threat assessment or DBT, for example, communications systems, and monitoring and tracking systems, and those containing sensitive information pertaining to transport operations.
- Appropriate storage containers, such as safes, cabinets, etc., are available.
- Measures are taken to ensure the confidentiality of communications, for example, if security related messages are transmitted using measures such as encryption or coding.
- Restraint is applied in the use of any special markings on conveyances.

4.5.8. Trustworthiness

4.5.8.1. Objective

- To determine if trustworthiness considerations are an integral part of the transport security programme.

4.5.8.2. Basis

- INFCIRC/225/Rev.5, para. 6.6(e):

"Physical protection against *unauthorized removal* during *transport* should encompass, as far as operationally practicable in accordance with the *graded approach*:

> (e) Requiring predetermination of the trustworthiness of individuals involved during *transport* of *nuclear material*."

For Category I:

- INFCIRC/225/Rev.5, para. 6.37:

"There should be a *transport control centre* for the purpose of keeping track of the current position and security status of the shipment of *nuclear material*, alerting *response forces* in case of an attack and maintaining continuous secure two way voice communication with the shipment and the *response forces*. The *transport control centre* should be protected so that its function can continue in the presence of the *threat*. While the shipment is in progress, the *transport control centre* should be staffed by qualified *shipper* or State designees whose trustworthiness has been predetermined."

4.5.8.3. Documentation

- Trustworthiness requirements and procedures;
- Employee code of conduct;
- Trustworthiness records.

4.5.8.4. Data to be collected/specimen questions

Determine if and how:

- Trustworthiness determinations are carried out.
- Specific persons or positions involved with transport operations are identified that require trustworthiness checks.
- The trustworthiness of all security staff has been established.

4.5.9. Reporting

4.5.9.1. Objective

- To determine that reporting procedures and capabilities are in place for both routine reports and nuclear security events.

4.5.9.2. Basis

For Categories I, II and III:

- INFCIRC/225/Rev.5, para. 6.12:

"The carrier should give the receiver advance notification of the planned shipment specifying the mode of *transport* (road/rail/water/air), the estimated time of arrival of the shipment and the exact point of handover if this is to be done at some intermediate point before the ultimate destination. This advance notification should be supplied in time to enable the receiver to make adequate physical protection arrangements."

- INFCIRC/225/Rev.5, para. 6.18:

"The receiver should check the integrity of the packages, and locks and seals when used, and accept the shipment immediately upon arrival. The receiver should notify the *shipper* of the arrival of the shipment immediately or of non-arrival within a reasonable interval after the estimated time of arrival at the destination."

For Categories I and II:

- INFCIRC/225/Rev.5, para. 6.21:

"The receiver should confirm readiness to accept delivery (and handover, if applicable) at the expected time, prior to the commencement of the shipment."

For Category I:

- INFCIRC/225/Rev.5, para. 6.39:

"The *guards* or *conveyance* crew should be instructed to report frequently and upon arrival at the destination, each overnight stopping place and place of handover of the shipment by secure two way voice communications to the *transport control centre*."

For location and recovery of missing or stolen nuclear material:

- INFCIRC/225/Rev.5, para. 6.54:

"If packages are determined to be missing or have been tampered with, the carrier should immediately report this to relevant authorities and the *shipper*."

For mitigation or minimization of the radiological consequences of sabotage:

- INFCIRC/225/Rev.5, para. 6.71:

"The *transport control centre* or carrier's management should be informed as soon as an attempt or an act of *sabotage* is detected."

- INFCIRC/225/Rev.5, para. 6.72:

"The carrier should notify, in a timely manner, the *shipper*, the *competent authority*, *response forces* and other relevant State organizations of *sabotage* or attempted *sabotage* as specified in the *contingency plan*."

4.5.9.3. Documentation

- Reporting procedures and forms for shipment and receipt of material;
- Reporting procedures and forms for nuclear material discrepancies and nuclear security events.

4.5.9.4. Data to be collected/specimen questions

Determine if and how:

- Arrangements and procedures are in place for the timely reporting of nuclear security events.
- Arrangements are in place that enable the State's competent authority to be informed of any changes relating to transport of nuclear material which may affect physical protection measures.
- The carrier ensures control of the packages and is able to account for the integrity of the packages at all times during transport.
- The carrier reports to relevant authorities and the shipper when packages are suspected to be missing or having been tampered with.
- The transport control centre or carrier's management is informed when an attempt or an act of sabotage is detected.
- The carrier notifies, in a timely manner, the shipper, the competent authority, response forces and other relevant State organizations of sabotage or attempted sabotage as specified in the contingency plan.

4.5.10. System evaluation, including performance testing

4.5.10.1. Objective

- To determine if a systematic approach is in place and used to test and evaluate the performance capabilities of the physical protection system.

4.5.10.2. Basis

- INFCIRC/225/Rev.5, para. 3.21:

"To ensure that *physical protection measures* are maintained in a condition capable of meeting the State's regulations and of effectively responding to the State's requirements for physical protection, the State's *competent authority* should ensure that evaluations based on *performance testing* are conducted by *operators* at *nuclear facilities* and, as appropriate, by *shippers* and/or carriers for *transport*. Evaluations should be reviewed by the State's *competent authority*, and should include administrative and technical measures, such as testing of *detection*, assessment, delay and communications systems, and reviews of the implementation of physical protection procedures. When deficiencies are identified, the *competent authority* should ensure that corrective action is taken by the *operator*, *shipper* and/or carrier."

- INFCIRC/225/Rev.5, para. 3.29:

"The *operator* should develop and implement means and procedures for evaluations, including *performance testing*, and maintenance of the *physical protection system.*"

- INFCIRC/225/Rev.5, para. 3.30:

"Whenever the *physical protection system* is determined to be incapable of providing the required level of protection, the *operator*, *shipper* and/or carrier should immediately implement compensatory measures to provide adequate protection. The *operator* and/or *shipper* should then — within an agreed period — plan and implement corrective actions to be reviewed and approved by the *competent authority*."

- INFCIRC/225/Rev.5, para. 6.50:

"The State should ensure that appropriate State response organizations, carriers and/or other relevant entities conduct exercises to assess and validate the *contingency plans* and also to train the various participants on how to react in such a situation."

4.5.10.3. Documentation

- System evaluation and performance testing programme plan and records;
- Vulnerability assessments;
- Training and exercise requirements and records;
- Exercise results;
- Procedures for responding to discovered deficiencies in the physical protection system.

4.5.10.4. Data to be collected/specimen questions

Determine:

- If the effectiveness of the physical protection system is evaluated.
- When and by whom such evaluations are performed.
- How the results are evaluated and how any identified deficiencies in the transport physical protection system are addressed.
- If any deficiencies in the physical protection system discovered during transport are compensated for and if any follow-up corrective actions are taken.
- If contingency plans and procedures are routinely reviewed and performance tested, e.g. to verify the effectiveness of the security organization to respond to a security event.
- If transport personnel are trained and exercised in their responsibilities during security events and emergency situations.
- If contingency plans and emergency plans are jointly exercised and complement each other.

4.5.11. Quality assurance

4.5.11.1. Objective

- To verify that comprehensive quality assurance programmes are in place to ensure the quality and reliability of all aspects of the physical protection system.

4.5.11.2. Basis

- CPPNM Amendment, Fundamental Principle J: Quality Assurance:

"A quality assurance policy and quality assurance programmes should be established and implemented with a view to providing confidence that specified requirements for all activities important to physical protection are satisfied."

- INFCIRC/225/Rev.5, para. 3.52:

"The quality assurance policy and programmes for physical protection should ensure that a *physical protection system* is designed, implemented, operated and maintained in a condition capable of effectively responding to the *threat assessment* or *design basis threat* and that it meets the State's regulations, including its prescriptive and/or performance based requirements."

4.5.11.3. Documentation

- Quality assurance plan and standards used;
- Quality manual;
- Quality assurance records;
- Qualifications of quality assurance personnel;
- Lessons learned programme;
- Audit reports.

4.5.11.4. Data to be collected/specimen questions

Determine if and how:

- Quality assurance policies and programmes for physical protection exist and ensure that a physical protection system is designed, implemented, operated and maintained in a condition capable of effectively responding to the threat assessment or DBT.

- A lessons learned programme exists to identify and correct quality issues identified within the physical protection system.

4.5.12. Sustainability programme

4.5.12.1. Objective

- To determine if there is a systematic approach to ensure the continuous reliability and long term availability of personnel, systems and equipment including operating procedures, training, equipment maintenance (including conveyances and escort vehicles), configuration management and resource allocation.

4.5.12.2. Basis

- INFCIRC/225/Rev.5, para. 3.57:

"*Operator*s, *shippers* and carriers should establish sustainability programmes for their *physical protection system*. Sustainability programmes should encompass:

- Operating procedures (instructions).
- Human resource management and training.
- Equipment updating, maintenance, repair and calibration.
- *Performance testing* and operational monitoring.
- Configuration management (the process of identifying and documenting the characteristics of a facility's *physical protection system* — including computer systems and software — and of ensuring that changes to these characteristics are properly developed, assessed, approved, issued, implemented, verified, recorded and incorporated into the facility documentation).
- Resource allocation and operational cost analysis."

4.5.12.3. Documentation

- Human resource management plan;
- Personnel reliability programme;
- Operating procedures;
- Maintenance plans and records;
- Configuration management plans;
- Cost projections and budget requests.

4.5.12.4. Data to be collected/specimen questions

Determine if and how:

- Configuration management is implemented to ensure that any changes to the physical protection system are assessed and approved before those changes are made.
- A preventive maintenance programme is established and adhered to, including maintenance of conveyances, escort and other support vehicles.
- Testing, maintenance and deficiency improvement programmes exist that ensure the integrity of security related systems (communications, detection, etc.).
- Maintenance documentation is current and available only to authorized personnel.
- Confirmation is made that people involved in transport are qualified for transport and fit for duty, and their training current.
- There are procedures to address any vulnerability posed by insiders performing maintenance.
- Last check of compliance with transport security plan is applied before transport commences.

4.6. TRANSPORT PHYSICAL PROTECTION SYSTEM

4.6.1. Detection

4.6.1.1. Access control

(a) Objective

- To determine that appropriate searches of conveyances are performed and that access control is provided during and after the searches.
- To assess how locks, keys and seals are applied and managed in the transport security system.

(b) Basis

- INFCIRC/225/Rev.5, para. 6.6(i):

"Physical protection against *unauthorized removal* during *transport* should encompass, as far as operationally practicable in accordance with the *graded approach*:

(j) Ensuring that packages and/or *conveyances* are not left unattended for any longer than is absolutely necessary."

- INFCIRC/225/Rev.5, para. 6.9:

"Procedures should be established to ensure the security of keys to *conveyances* and security locks commensurate with the categorization of the *nuclear material* being transported."

For Categories I, II and III:

- INFCIRC/225/Rev.5, para. 6.14:

"Packages containing *nuclear material* should be carried in closed, locked *conveyances*, compartments or freight containers. However, carriage of packages weighing more than 2000 kg that are locked or sealed may be allowed in open vehicles. Packages should be tied down or attached to the vehicle or freight container and should be secured as appropriate."

- INFCIRC/225/Rev.5, para. 6.15:

"Where practicable, locks and seals should be applied to *conveyance*s, compartments or freightcontainers. If locks and/or seals are used, checks should be made before dispatch and during any intermodal transfer of each *nuclear material* consignment to confirm the integrity of the locks and seals on the package, vehicle, compartment or freight container."

- INFCIRC/225/Rev.5, para. 6.16:

"There should be a detailed search of the *conveyance* to ensure that nothing has been tampered with and that nothing has been affixed to the package or *conveyance* that might compromise the security of the consignment."

- INFCIRC/225/Rev.5, para. 6.18:

"The receiver should check the integrity of the packages, and locks and seals when used, and accept the shipment immediately upon arrival. The receiver should notify the *shipper* of the arrival of the shipment immediately or of non-arrival within a reasonable interval after the estimated time of arrival at the destination."

For Categories I and II:

- INFCIRC/225/Rev.5, para. 6.26:

"The *conveyance* should be searched immediately prior to loading and shipment. Immediately following completion of the search, the *conveyance* should be placed in a secure area or kept under *guard* surveillance pending its loading and shipment for *transport* and unloading."

- INFCIRC/225/Rev.5, para. 6.31

"Depending on the mode of *transport*, the consignment should be shipped by:

- Road, under exclusive use conditions; or
- Rail, where operationally practicable, in a freight train in an exclusive use fully enclosed and locked *conveyance*; or
- Water, in a secure compartment or container which is locked and sealed; or
- Air, in an aircraft designated for cargo only and in a secure compartment or container which is locked and sealed.

While *nuclear material* is on board pending departure, provisions should be made for sufficient *access delay* or compensating measures to meet the *threat assessment* or *design basis threat*."

For Category I:

- INFCIRC/225/Rev.5, para. 6.36:

"When locked or sealed packages weighing more than 2000 kg are transported in open vehicles, enhanced *physical protection measures* should be applied, such as additional *guards*. The package should be tied down or attached to the *conveyance* or freight container with multiple locking mechanisms that require to be unlocked by two different keys held by two different authorized persons."

(c) Documentation

- Access control and search procedures;
- Key control policy, procedures and records;
- Lock and seal inspection procedures.

(d) Data to be collected/specimen questions

Determine if and how:

- Access control is implemented to deny unauthorized access of persons or the introduction of prohibited items into the vicinity of the packages and conveyance.
- There is a detailed search of the conveyance, including crew compartments, to ensure that nothing has been tampered with, that nothing has been affixed to the package or conveyance that might compromise the security of the consignment and that nothing has been brought on-board that might compromise security.
- Personnel are trained and equipped to conduct searches of the conveyance.
- Technical means for access control are protected against compromise (e.g. manipulation or falsification).
- Procedures have been established to ensure the security of keys to conveyances and security locks.
- Locks and seals are applied to conveyances, compartments or freight containers.
- Locks and/or seals are checked before dispatch and during any intermodal transfer of each nuclear material consignment.

- The receiver checks the integrity of the packages, and locks and seals upon delivery.
- For Category I material, when locked or sealed packages are transported in open vehicles, the enhanced physical protection measures that are applied.
- Appropriate training is given to personnel who conduct integrity checks of locks/seals.

4.6.1.2. Surveillance

(a) Objective

- To determine how intrusion into the conveyance or cargo area is detected and assessed in a timely manner.

(b) Basis

- CPPNM Amendment, Fundamental Principle I: Defence in Depth:

"The State's requirements for physical protection should reflect a concept of several layers and methods of protection (structural or other technical, personnel and organizational) that have to be overcome or circumvented by an adversary in order to achieve his objectives."

- INFCIRC/225/Rev.5, para. 3.46:

"The three physical protection functions of *detection*, delay, and response should each use *defence in depth* and apply a *graded approach* to provide appropriate effective protection."

For Categories I and II:

- INFCIRC/225/Rev.5, para. 6.20:

"*Physical protection measures* should include surveillance of the cargo, load compartment or *conveyance*. States are encouraged to use *guards* for such surveillance."

- INFCIRC/225/Rev.5, para. 6.26:

"The *conveyance* should be searched immediately prior to loading and shipment. Immediately following completion of the search, the *conveyance* should be placed in a secure area or kept under *guard* surveillance pending its loading and shipment for *transport* and unloading."

For Category I:

- INFCIRC/225/Rev.5, para. 6.34:

"A further authorization by the *competent authority* of the shipment should be required just prior to commencing *transport* and should be conditional on a current *threat assessment* and intelligence information and, where appropriate, on a detailed route surveillance to observe the current environment. The consent to a transport operation can include specific limitations and conditions related to the particular circumstances."

- INFCIRC/225/Rev.5, para. 6.35:

"*Guards*, appropriately equipped and trained, should accompany each shipment to protect the *nuclear material*, including before and during loading and unloading operations, to conduct surveillance of the route and to initiate an appropriate response. Continuous, effective surveillance of the packages or locked cargo hold or compartment holding the packages should be maintained by the *guard* at all times, especially when the *conveyance* is not in motion. States are encouraged to use armed *guards* to the extent that laws and regulations permit. When *guards* are not armed, compensating measures should be applied, such as adding delay barriers to the *conveyance* exterior structure and/or interior cargo area."

- INFCIRC/225/Rev.5, para. 6.40:

"For shipment by road, designated *conveyance(s)* should be used exclusively for each consignment and should preferably be specially designed to resist attack and equipped with a *conveyance* disabling device. Each *conveyance* should carry a *guard* or crew member in addition to the driver. Each *conveyance* should be accompanied by at least one vehicle with *guards* to conduct a surveillance of the route for any threat indicators and to protect the *conveyance* and initiate an appropriate response."

- INFCIRC/225/Rev.5, para. 6.41:

"During shipment by rail, accompanying *guards* should travel close to the *conveyance* to have proper effective surveillance."

(c) Documentation

- Cargo and conveyance surveillance methods and procedures.
- Equipment (vehicle, sensor and alarm station) design information and certifications.
- Test and maintenance records.

(d) Data to be collected/specimen questions

Determine if and how:

- Cargo/conveyance surveillance provides continuous detection.

- Intrusion detection equipment is appropriate and adequate for the transport system and if it performs as designed.
- The detection systems are tamper indicating and self-checking.
- Controls and switches that affect sensitivity of the detection systems are located in a tamper alarmed housing.
- The cause of an intrusion alarm is assessed.
- Assessment equipment is adequate and appropriate for the transport and the equipment performs as designed.
- A system is in place to prevent tampering of the alarm equipment.
- Duress alarms, if present in the cargo carry vehicle and/or guard vehicles, are tested and capable of initiating response.

4.6.1.3. Transport control centre

(a) Objective

- To determine that for any shipment of Category I nuclear material a Transport Control Centre is in place and capable of performing all necessary functions

(b) Basis

For Category I:

- INFCIRC/225/Rev.5, para. 6.37:

"There should be a *transport control centre* for the purpose of keeping track of the current position and security status of the shipment of *nuclear material*, alerting *response forces* in case of an attack and maintaining continuous secure two way voice communication with the shipment and the *response forces*. The *transport control centre* should be protected so that its function can continue in the presence of the *threat*. While the shipment is in progress, the *transport control centre* should be staffed by qualified *shipper* or State designees whose trustworthiness has been predetermined."

- INFCIRC/225/Rev.5, para. 6.39:

"The *guards* or *conveyance* crew should be instructed to report frequently and upon arrival at the destination, each overnight stopping place and place of handover of the shipment by secure two way voice communications to the *transport control centre*."

(c) Documentation

- Transport control centre design information and protection requirements;
- Operating procedures (communications, notifications, etc.);

- Incident log.

(d) Data to be collected/specimen questions

Determine:

- If there is a transport control centre for the purpose of keeping track of the current position and security status of the shipment of nuclear material, alerting response forces in case of an attack and maintaining continuous secure two way voice communication with the shipment and the response forces.
- Where it is located;
- Its functions and equipment;
- Who works in the transport control centre and how are they deemed qualified and trustworthy.
- If the transport control centre is protected, commensurate with the threat/DBT.

4.6.2. Delay

4.6.2.1. Resistance to forcible attack

(a) Objective

- To assess the transport security system in its ability to provide sufficient delay to enable an appropriate response.

(b) Basis

- CPPNM Amendment, Fundamental Principle I: Defence in Depth:

"The State's requirements for physical protection should reflect a concept of several layers and methods of protection (structural or other technical, personnel and organizational) that have to be overcome or circumvented by an adversary in order to achieve his objectives."

- INFCIRC/225/Rev.5, para. 3.46:

"The three physical protection functions of *detection*, delay, and response should each use *defence in depth* and apply a *graded approach* to provide appropriate effective protection."

- INFCIRC/225/Rev.5, para. 6.6(g):

"Physical protection against *unauthorized removal* during *transport* should encompass, as far as operationally practicable in accordance with the *graded approach*:

(g) Using a material transport system with passive and/or active *physical protection measures* appropriate for the *threat assessment* or *design basis threat*."

For Categories I, II and III:

- INFCIRC/225/Rev.5, para. 6.14:

"Packages containing *nuclear material* should be carried in closed, locked *conveyances*, compartments or freight containers. However, carriage of packages weighing more than 2000 kg that are locked or sealed may be allowed in open vehicles. Packages should be tied down or attached to the vehicle or freight container and should be secured as appropriate."

For Categories I and II:

- INFCIRC/225/Rev.5, para. 6.25:

"*Physical protection measures* should provide sufficient delay in the c*onveyance*, freight container and/or package so that *guards* and/or *response forces* have time for an appropriate response."

- INFCIRC/225/Rev.5, para. 6.31:

"Depending on the mode of *transport*, the consignment should be shipped by:

- Road, under exclusive use conditions; or
- Rail, where operationally practicable, in a freight train in an exclusive use fully enclosed and locked *conveyance*; or
- Water, in a secure compartment or container which is locked and sealed; or
- Air, in an aircraft designated for cargo only and in a secure compartment or container which is locked and sealed.

While *nuclear material* is on board pending departure, provisions should be made for sufficient *access delay* or compensating measures to meet the *threat assessment* or *design basis threat*."

For Category I:

- INFCIRC/225/Rev.5, para. 6.33:

"The approval by the *competent authority* of the transport security plan should be based on a detailed examination of proposed *physical protection measures*, which should provide sufficient delay so that *guards* and/or *response forces* have time to intervene to prevent *unauthorized removal*. The transport security plan should include the route and arrangements for making changes, such as alteration of the route during the shipment, in response to unexpected changes in the physical environment, *threat assessment* and operating conditions."

- INFCIRC/225/Rev.5, para. 6.35:

"*Guards*, appropriately equipped and trained, should accompany each shipment to protect the *nuclear material*, including before and during loading and unloading operations, to conduct surveillance of the route and to initiate an appropriate response. Continuous, effective surveillance of the packages or locked cargo hold or compartment holding the packages should be maintained by the *guard* at all times, especially when the *conveyance* is not in motion. States are encouraged to use armed *guards* to the extent that laws and regulations permit. When *guards* are not armed, compensating measures should be applied, such as adding delay barriers to the *conveyance* exterior structure and/or interior cargo area."

(c) Documentation

- Design information on delay features.

(d) Data to be collected/specimen questions

Determine if, and how, for Categories I and II material:

- Physical protection measures are in place to provide sufficient delay in the conveyance, freight container and/or package to enable guards and/or response forces time for an appropriate response.
- The transport security system has been designed and evaluated in terms of offering sufficient delay against forceful attack and minimizing opportunities for insiders.
- The material transport system takes into account passive and/or active physical protection measures appropriate for the threat assessment or DBT.

4.6.2.2. Disabling devices

(a) Objective

- To determine if appropriate devices and features are present to resist attack and to delay or stop the conveyance.

(b) Basis

For Category I:

- INFCIRC/225/Rev.5, para. 6.40:

"For shipment by road, designated *conveyance(s)* should be used exclusively for each consignment and should preferably be specially designed to resist attack and equipped with a *conveyance* disabling device. Each *conveyance* should carry a *guard* or crew member in addition to the driver. Each *conveyance* should be accompanied by at least one vehicle with *guards* to conduct a surveillance of the route for any threat indicators and to protect the *conveyance* and initiate an appropriate response."

(c) Documentation

- Design information and testing procedures for disabling devices.

(d) Data to be collected/specimen questions

Determine if, and how, for Category I material transported by road:

- A designated conveyance(s) is used exclusively for each consignment.
- Each road conveyance is specially designed to resist attack and equipped with a conveyance disabling device.
- The disabling device is activated either automatically or by person. If automatically, then what triggers it; if by person, then by whom, including person's location.

4.6.3. Response

4.6.3.1. Guards and response forces

(a) Objectives

- To determine that there is an adequate and timely response capability for nuclear security events.
- To determine that arrangements are made to provide sufficient guards and/or response forces to deal with nuclear security events consistent with the category of nuclear material being transported or the potential consequences of radiological releases.

(b) Basis

- CPPNM Amendment, Fundamental Principle I: Defence in Depth:

"The State's requirements for physical protection should reflect a concept of several layers and methods of protection (structural or other technical, personnel and organizational) that have to be overcome or circumvented by an adversary in order to achieve his objectives."

- INFCIRC/225/Rev.5, para. 3.46:

"The three physical protection functions of *detection*, delay, and response should each use *defence in depth* and apply a *graded approach* to provide appropriate effective protection."

For Categories I, II and III:

- INFCIRC/225/Rev.5, para. 6.17:

"Arrangements should be made to provide sufficient *guards* and/or *response forces* to deal with *nuclear security events* consistent with the category of *nuclear material* being transported and *physical protection measures* should include communication from the *conveyance* capable of summoning appropriate responders."

For Categories I and II:

- INFCIRC/225/Rev.5, para. 6.20:

"*Physical protection measures* should include surveillance of the cargo, load compartment or *conveyance*. States are encouraged to use *guards* for such surveillance."

- INFCIRC/225/Rev.5, para. 6.24:

"When justified by the State's *threat assessment*, States are encouraged to use armed *guards* for shipments of Category II *nuclear material* to the extent that laws and regulations permit. In those circumstances when *guards* are not armed, compensating measures should be applied."

- INFCIRC/225/Rev.5, para. 6.30:

"Arrangements should be made to provide adequately sized *response forces* to deal with *nuclear security events*. The objective should be the arrival of the *response forces* in time to prevent *unauthorized removal*."

For Category I:

- INFCIRC/225/Rev.5, para. 6.35:

"*Guards*, appropriately equipped and trained, should accompany each shipment to protect the *nuclear material*, including before and during loading and unloading operations, to conduct surveillance of the route and to initiate an appropriate response. Continuous, effective surveillance of the packages or locked cargo hold or compartment holding the packages should be maintained by the *guard* at all times, especially when the *conveyance* is not in motion. States are encouraged to use armed *guards* to the extent that laws and regulations permit. When *guards* are not armed, compensating measures should be applied, such as adding delay barriers to the *conveyance* exterior structure and/or interior cargo area."

- INFCIRC/225/Rev.5, para. 6.36:

"When locked or sealed packages weighing more than 2000 kg are transported in open vehicles, enhanced *physical protection measures* should be applied, such as additional *guards*. The package should be tied

down or attached to the *conveyance* or freight container with multiple locking mechanisms that require to be unlocked by two different keys held by two different authorized persons."

- INFCIRC/225/Rev.5, para. 6.39:

"The *guards* or *conveyance* crew should be instructed to report frequently and upon arrival at the destination, each overnight stopping place and place of handover of the shipment by secure two way voice communications to the *transport control centre*."

- INFCIRC/225/Rev.5, para. 6.40:

"For shipment by road, designated *conveyance(s)* should be used exclusively for each consignment and should preferably be specially designed to resist attack and equipped with a *conveyance* disabling device. Each *conveyance* should carry a *guard* or crew member in addition to the driver. Each *conveyance* should be accompanied by at least one vehicle with *guards* to conduct a surveillance of the route for any threat indicators and to protect the *conveyance* and initiate an appropriate response."

- INFCIRC/225/Rev.5, para. 6.41:

"During shipment by rail, accompanying *guards* should travel close to the *conveyance* to have proper effective surveillance."

(c) Documentation

- Contingency plan and procedures;
- Guard staffing plan;
- Guard training plan and records;
- Memorandum of Understanding with local response forces.

(d) Data to be collected/specimen questions

Determine if and how:

- Guards, appropriately equipped and trained, accompany each shipment to conduct surveillance of the route.
- Detailed route surveillance is carried out just prior to commencing transport to observe the current environment.
- Routes are selected to avoid areas of natural disaster, civil disorder or with a known threat.
- Guards and response forces are sufficient in numbers and adequately trained and equipped to deal with the DBT.
- Guards are not used, then who escorts the shipment, how is their trustworthiness determined and what training do they receive.

For Categories I and II material, determine:

- If physical protection measures include surveillance of the cargo, load compartment or conveyance.
- If the guard vehicles/enclosures are protected/hardened against the threat/DBT.
- If guards are used for such surveillance.
- If armed guards are used for shipments of Category II nuclear material.
- If, when guards are not armed, compensating measures are applied.
- If arrangements are made to provide adequately sized response forces to deal with nuclear security events.
- If there is a Memorandums of Understanding with the local/enroute response forces, and what the content is.
- If arrival of the response forces will be in time to prevent the unauthorized removal and/or other appropriate response according to the category or sensitivity of the nuclear material.

For Category I material, determine if and how:

- Guards, appropriately equipped and trained, accompany each shipment to protect the nuclear material, including before and during loading and unloading operations, to conduct surveillance of the route and to initiate an appropriate response.
- Guards know the law and policy for the use of force and are trained accordingly.
- Continuous, effective surveillance of the packages or locked cargo hold or compartment holding the packages is maintained by the guards at all times, especially when the conveyance is not in motion.
- Armed guards are used.
- When guards are not armed, compensating measures are applied, such as adding delay barriers to the conveyance exterior structure and/or interior cargo area.
- Guards or conveyance crew is instructed to report frequently and upon arrival at the destination, each overnight stopping place and place of handover of the shipment by secure two way voice communications to the transport control centre.
- During shipment by rail, accompanying guards travel close to the conveyance to ensure effective surveillance.
- Each conveyance carries a guard or crew member in addition to the driver.
- Each conveyance is accompanied by at least one vehicle with guards to conduct a surveillance of the route for any threat indicators and to protect the conveyance and initiate an appropriate response.

4.6.3.2. Communications during transport

(a) Objective

- To evaluate the provisions for continuous two way voice communication between the conveyance, any guards accompanying the shipment, the designated response forces and, where appropriate, the shipper and/or receiver.

(b) Basis

For Categories I, II and III:

- INFCIRC/225/Rev.5, para. 6.17:

"Arrangements should be made to provide sufficient *guards* and/or *response forces* to deal with *nuclear security events* consistent with the category of *nuclear material* being transported and *physical protection measures* should include communication from the *conveyance* capable of summoning appropriate responders."

For Categories I and II:

- INFCIRC/225/Rev.5, para. 6.29:

"*Physical protection measures* should include provision of continuous two way voice communication between the *conveyance*, any *guards* accompanying the shipment, the designated *response forces* and, where appropriate, the *shipper* and/or receiver."

For Category I:

- INFCIRC/225/Rev.5, para. 6.37:

"There should be a *transport control centre* for the purpose of keeping track of the current position and security status of the shipment of *nuclear material*, alerting *response forces* in case of an attack and maintaining continuous secure two way voice communication with the shipment and the *response forces*. The *transport control centre* should be protected so that its function can continue in the presence of the *threat*. While the shipment is in progress, the *transport control centre* should be staffed by qualified *shipper* or State designees whose trustworthiness has been predetermined."

- INFCIRC/225/Rev.5, para. 6.38:

"Continuous two way communication systems between the *conveyance, transport control centre*, *guards* accompanying the shipment, the designated *response forces*, and where appropriate, the *shipper* and/or receiver should be redundant, diverse and secure."

(c) Documentation

- Communications plan (system design, maintenance, testing, etc.) and records;
- Communications procedures.

(d) Data to be collected/specimen questions

Determine if and how:

- Physical protection measures include provision of continuous two way voice communication between the conveyance, any guards accompanying the shipment, the designated response forces and, where appropriate, the shipper and/or receiver.

Determine if, and how, for Category I material:

- There is a communications system and applicable procedures during transport.
- Redundant communication capabilities are provided.
- The communications are determined to be diverse and secure.
- A reporting protocol exists between the guards, conveyance crew and the transport control centre.
-

4.6.3.3. Equipment

(a) Objective

- To determine if guards and response personnel have adequate equipment, including weapons.

(b) Basis

For Category I:

- INFCIRC/225/Rev.5, para. 6.35:

"*Guards*, appropriately equipped and trained, should accompany each shipment to protect the *nuclear material*, including before and during loading and unloading operations, to conduct surveillance of the route and to initiate an appropriate response."

(c) Documentation

- Equipment requirements, including training requirements;
- Weapons requirements, including training requirements.

(d) Data to be collected/specimen questions

Determine:

- What equipment is available for the guard and response personnel (e.g. vehicles, communications equipment, appropriate clothing, computers, firearms, night vision devices).
- If this equipment is sufficient for guards and response personnel to perform their duties properly, including incident response.

5. SECURITY OF RADIOACTIVE MATERIAL, ASSOCIATED FACILITIES AND ASSOCIATED ACTIVITIES (MODULE 4)

5.1. INTRODUCTION

Radioactive material is widely used in the world's health care, manufacturing, research and quality control industries. The IAEA provides a set of recommendations to ensure a consistent level of security of *radioactive material* and to ensure that there is a balance between managing *radioactive material* securely while still enabling it to be used safely by *authorized persons* for societal benefits.

The possibility that nuclear or other radioactive material could be used for malicious purposes cannot be ruled out in the current global situation. States have responded to this risk by engaging in a collective commitment to strengthen the protection and control of such material and to respond effectively to nuclear security events. States have agreed to strengthen existing nuclear security and have established new international legal instruments to enhance nuclear security worldwide. Nuclear security is fundamental to the management of nuclear technologies and in applications where nuclear or other radioactive material is used, stored or transported.

The IAEA has adopted a comprehensive approach to nuclear security. This recognizes that an effective national nuclear security regime builds on the: implementation of relevant international legal instruments; information protection; physical protection; material accounting and control; detection of, and response to, trafficking in such material; and national response plans and contingency measures.

Each State carries full responsibility for nuclear security, specifically to provide for the security of nuclear and other radioactive material and associated facilities and activities; to ensure the security of such material in use, storage or in transport; to combat illicit trafficking and the inadvertent movement of such material; and to be prepared to respond to a nuclear security event.

The potential consequences resulting from an improvised nuclear device or the potential economic and social disruption resulting from a radiological dispersal device could be enormous. Since 11 September 2001, a new realization has emerged regarding the potential for malicious acts involving nuclear material. Recent evaluations of the potential consequences of the use of a radiological dispersal device have identified the need to improve the security of radioactive material.

The primary security concern associated with radioactive material such as radioactive sources lies in deliberately exposing individuals to radiation or the dispersal of the radioactive material, with consequent detrimental effects on people, property and the environment. The threat of a direct act of sabotage or theft of radioactive material to be released at another location as a malicious act is a valid concern. Since transport occurs in the public domain and frequently involves intermodal transfers, it is a potentially vulnerable phase of domestic and international commerce.

While considerable attention and resources have been directed towards improving the security of sources in facilities, there has been a less focused effort directed at the security of radioactive material, other than nuclear material, during transport. Radioactive material is most vulnerable during transport. Transport of large radioactive sources is often an international activity involving movement through the public domain with minimal physical protection. Historically, the emphasis has been on safety in transport, but now there is a recognized need to address security as a priority. The current concern about transport security

may be due to the fact that the safety record for the transport of radioactive material has been very good but the threat of malicious acts, including sabotage, is now more widely recognized.

The importance of fostering a security culture in all organizations and among all individuals engaged in the regulatory control or the use, storage and transport of radioactive sources is now widely recognized.

5.2. PURPOSE

The IPPAS mission, initially created for nuclear material and nuclear facilities, has been extended to provide advice to a State regarding the security of radioactive material, associated facilities and associated activities, including radioactive material during transport.

This module can be used as the basis of a standalone IPPAS mission for the security of radioactive material, associated facilities, and associated activities, or within a broader IPPAS mission on the full scope of a State's nuclear security regime. This module provides practical advice and bases on how to perform an IPPAS mission dedicated to the review of the security of radioactive material. This module is addressed principally to the team members of IPPAS missions; although it also provides guidance to the State that may be considering hosting an IPPAS mission, or information to a host country on preparing for and receiving a mission.

The review points should not be used as a simple yes/no checklist but rather as questions which allow the interviewer to gain an appreciation of the subject and, as appropriate, to compare implementation with international instruments, IAEA recommendations and guidance and accepted international best practice. The terms 'recommendation' and 'suggestion' are used to differentiate two types of advice based upon the mission findings. Recommendations are based upon international instruments and IAEA nuclear security recommendations whereas suggestions may be based upon IAEA lower level security guidance, best practices or the experiences of team members.

The objectives of IPPAS missions for the security of radioactive material, associated facilities and associated activities are:

- To provide an independent assessment of a State's nuclear security regime for radioactive material, associated facilities and associated activities;
- To provide advice to a State (competent authority) in the form of recommendations and suggestions, and to recognize good practices;
- To share experience in the design and implementation of a State's nuclear security regime for radioactive material, associated facilities and associated activities;
- To provide a basis for assistance to the requesting State in implementing security improvements;
- To provide advice to operators, shippers and carriers.

5.3. IPPAS MISSION SCOPE

The scope of the mission covers the security of radioactive material, associated facilities and associated activities for the prevention of malicious acts intended or likely to have harmful radiological

consequences. Such radioactive material may include *nuclear material*[1], sealed sources, unsealed radioactive material, disused sources as well as radioactive waste. However, the international bases for conducting an IPPAS mission for radioactive material is the Code of Conduct on the Safety and Security of Radioactive Sources [1], which focuses on Category I–III sealed radioactive sources, and the Guidance on the Import and Export of Radioactive Sources [2]. Therefore, the core scope of the source security module of IPPAS is intended primarily to address the security of Category I–III radioactive sources throughout their life cycle: manufacture, supply, receipt, possession, storage, use, transfer, import, export, transport, maintenance and recycling or disposal. At the request of the host State (and agreement of the IAEA), the scope may be expanded to address Category IV and V sealed sources, unsealed radioactive material and/or radioactive waste[2].

The IPPAS mission scope is in addition to, and not a substitute for, other requirements and recommendations established for safety or for radiation protection purposes for radioactive material, associated facilities and associated activities. The scope is only intended to address safety in relation to its interface with security. Where this scope overlaps, the IPPAS team should obtain background information from recent safety and other IAEA mission reports to the host State. This may answer many general questions as well as reduce the burden on the State to provide repetitive data to the IAEA.

The mission scope covers the following areas:

- Assignment of nuclear security responsibilities.
- Legislative and regulatory framework:
    - State;
    - Regulatory body;
    - Operator, shipper and/or carrier.
- International cooperation and assistance.
- Identification and assessment of threats.
- Risk based nuclear security systems and measures:
    - Risk management;
    - Interface with the safety system.
- Sustaining the nuclear security regime.
- Planning and preparedness for, and response to, nuclear security events.
- Import and export of radioactive material.
- Detection of nuclear security events.
- Security of radioactive material in use and storage:
    - Security system;

[1] Those responsible for the security of facilities containing *nuclear material* that could be a potential target both for *unauthorized removal* for use in a nuclear explosive device and for *unauthorized removal* for subsequent exposure or dispersal should consider both the recommendations in this publication and those in IAEA Nuclear Security Series No. 13. In these cases, the more stringent recommendations and security measures should be applied. When a facility contains *nuclear material* and *other radioactive material*, the protection requirements for both should be considered and implemented in a consistent and non-conflicting manner in order to achieve an adequate level of security.

[2] In the case of radioactive waste, this is in a form that is no longer usable for any associated activity and is practically irrecoverable, thereby minimizing the potential for environmental dispersal. Specific factors of disposal (e.g. activity concentration of the radioactive waste, its dispersability, the robustness of the radioactive waste package and its accessibility) should also be considered as part of the graded approach; thus, the requirements used as basis in Chapter 10 may not fully apply.

        - Security management.
- Security of radioactive material in transport.

5.3.1. Documents and data to be provided in advance by the host State

The proper preparation of the IPPAS team, as well as the effective conduct of the mission, requires the host State to provide the following information (in the agreed language) in advance:

- Procedure on categorization of radioactive material, both in facilities and for transport, and the establishment of the relative security levels.
- Relevant information on the inventory of the radioactive sources in use, storage or transport within the State, including their categorization, as available.
- Description of the constitutional and legal system of the State[3]:
    - Primary legislation are laws enacted by the State legislative body (e.g. the congress/parliament/local legislatures and ordinances);
    - Secondary (subordinate) legislation are legislative regulations issued by the government/cabinet or administrative agency/body pursuant to the primary legislation;
    - List of all relevant regulations, guides or technical standards that are required to be used or complied with by the applicant(s);
    - Explanatory publications or guidance by the regulatory authority to assist the operator, shipper and/or carrier to implement the security regulations;
    - Explanatory materials or guidance by the regulatory authority to explain how or why the regulations were developed as they currently exist (the assumptions made during the development process).
- Description of all the government ministries or competent authorities, including the regulatory body, involved in the State's security system, their responsibilities and how they interrelate, including overall coordination mechanisms.
- Procedures for threat and vulnerability assessments, their review and application to facilities, if appropriate.
- Regulatory body organizational structure; description of the regulatory body's legal status, responsibilities and its objectives as defined by law.
- Organizational structure and security responsibilities of the operator(s) to be visited.
- Internal regulatory body procedures for granting an authorization:
    - Copy of regulatory body procedures;
    - Example of authorization without sensitive information;
    - Example security plan for a facility, or for transport without names or addresses.
- Inspection procedures:
    - Inspection planning documentation;
    - Example inspection record.
- Enforcement policy and associated procedures
- State's most recent report on implementation of the Code of Conduct on the Safety and Security of Radioactive Sources.

[3] It may not be possible to translate or provide complete procedures in all cases. Short descriptions or extracts of relevant parts with references may suffice.

5.4. IPPAS MISSION PROCESS

The IPPAS mission is a process for providing a comprehensive peer review of, and advice for, improving a State's security regime as it exists for radioactive material, associated facilities and associated activities. When visiting a facility or transporter, the advisory process may be similar to an inspection conducted by a State's competent authority to determine compliance with the State's regulatory requirements for the security of radioactive material. The difference between the two is that the basis for IPPAS recommendations and suggestions is the guidance provided in the Code of Conduct, the IAEA NSS, and international practice rather than on the State's regulatory requirements.

An advisory mission conducted by an IPPAS team does not replace the regulatory function of the State's competent authority. It provides the State with an independent assessment of the status of its nuclear security regime and advice to the State in the form of recommendations and suggestions addressing the State's nuclear security regime for radioactive material at all levels (competent authorities, operators, shippers and carriers). The mission also recognizes good practices by the competent authority, operators, shippers and/or carriers, which could be shared in future missions and incorporated into international guidance.

The mission involves meetings with representatives of the competent authority and other organizations that have responsibilities in the security of radioactive material, associated facilities and associated activities, including transport. These responsibilities may include legislative drafting, licensing and regulation, response and threat definition.

Recommendations provided by the IPPAS team should be based on:

- The Code of Conduct on the Safety and Security of Radioactive Sources [1];
- IAEA NSS No. 14, Nuclear Security Recommendations on Radioactive Material and Associated Facilities[4] [3];
- Guidance on the Import and Export of Radioactive Sources [2].

Suggestions on specific details with regard to practical implementation of security systems and security management measures (see Chapters 10–13 of this Guideline) provided by the IPPAS team should be based on:

- IAEA NSS No. 11, Security of Radioactive Sources [4];
- IAEA NSS No. 9, Security in the Transport of Radioactive Material [5];
- UN Model Regulations on the Transport of Dangerous Goods [6].

Suggestions regarding specific issues, if appropriate, may also be based on:

- IAEA Safety Standards Series No. RS-G-1.9, Categorization of Radioactive Sources [7];
- IAEA, Dangerous Quantities of Radioactive Material (EPR-D-values) [8];
- IAEA Safety Standards Series No. GSR Part 1, Governmental, Legal and Regulatory Framework for Safety [9].

[4] References to IAEA NSS No. 13, Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities [10], and to IAEA NSS No. 15, Nuclear Security Recommendations on Nuclear and Other Radioactive Material out of Regulatory Control [11], are included in this module. The IPPAS team should refer to these publications, as appropriate.

5.5. ASSIGNMENT OF NUCLEAR SECURITY RESPONSIBILITIES

5.5.1. Objectives

This section provides the basis for recommendations and suggestions, as well as the data to be collected, in relation to:

- The definition of nuclear security responsibilities and their assignment to competent authorities;
- The integration and coordination of these responsibilities;
- The communication and exchange of information between competent authorities;
- The cooperation between competent authorities.

5.5.2. Basis for recommendations

- IAEA NSS No. 14, para. 3.2:

"The State should clearly define and assign nuclear security responsibilities to *competent authorities*, noting that they may include *regulatory bodies*, law enforcement, customs and border control, intelligence and security agencies, health agencies, etc. Provision should be made for appropriate integration and coordination of responsibilities within the State's *nuclear security regime*. Clear lines of responsibility and communication should be established and recorded between the *competent authorities*."

- IAEA NSS No. 14, para. 3.3:

"The State should ensure effective overall cooperation and relevant information sharing between the *competent authorities*. This should include sharing of relevant information (such as information about the *threat* to be protected against and other useful intelligence) in accordance with national regulations."

5.5.3. Documentation

In addition to the material provided by the State in advance of the IPPAS mission, the following documentation is expected to be requested by the team for review during the mission:

- Relevant Memorandums of Understanding or Agreements;
- Communication plans between the competent authorities;
- Procedures on the management of sensitive information;
- Procedures for communication and coordination among competent authorities in connection with response to nuclear security events.

5.5.4. Data to be collected/specimen questions

Determine if and how:

- Nuclear security responsibilities are clearly defined and assigned to the competent authorities;
- Responsibilities are integrated and coordinated (no overlapping or not covered responsibilities exist);
- Clear lines of responsibilities are established and recorded between the competent authorities;
- Clear communication lines are established and recorded between the competent authorities;
- Effective cooperation is maintained between the competent authorities, especially when the regulatory body comprises multiple agencies;
- Every relevant piece of information is shared between the competent authorities;
- Exercises are conducted among competent authorities to evaluate the efficiency and effectiveness of cooperative mechanisms and, if so, how the experiences and best practices from these exercises are shared.

5.6. LEGISLATIVE AND REGULATORY FRAMEWORK

5.6.1. Objectives

This section provides the basis for the recommendations and suggestions, as well as the data to be collected, in relation to:

- The current legal framework for radioactive source security (including establishment of regulatory authorities and criminalization of acts involving radioactive sources);
- The security requirements for radioactive material;
- The independence of competent authorities from operators, shippers and/or carriers, the competent authorities' financial and human resources;
- The regulatory framework of registration, authorizations, inspections, reporting and enforcement;
- The interface between security and safety;
- The protection of sensitive information;
- How the legislative and regulatory framework is implemented by the regulatory body.

5.6.2. State

5.6.2.1. Basis for recommendations

- IAEA NSS No. 14, para. 3.4:

"The State should establish, implement, and maintain an effective national legislative and regulatory framework to regulate the nuclear security of *radioactive material*, *associated facilities* and *associated activities*, which:

- Takes into account the risk of *malicious acts* involving *radioactive material* that could cause *unacceptable radiological consequences*;
- Defines the *radioactive material*, *associated facilities* and *associated activities* which are subject to the *nuclear security regime* in terms of nuclides and quantities of *radioactive material* present;
- Prescribes and assigns governmental responsibilities to relevant entities including an independent *regulatory body*;
- Places the prime responsibility on the *operator*, *shipper* and/or carrier for implementing and maintaining security measures for *radioactive material*;
- Establishes the *authorization* process for *radioactive material*, *associated facilities* and *associated activities*. As appropriate, the *authorization* process concerning the security of *radioactive material* could be integrated within one defined for safety or radiation protection;
- Establishes the inspection process for security requirements;
- Establishes the enforcement process for the failure to comply with security requirements established under legislative and regulatory framework;
- Establishes sanctions against the *unauthorized removal* of *radioactive material* and *sabotage* of *associated facilities* and *associated activities*;
- Takes into account the interface between security and safety of *radioactive material*."

- IAEA NSS No. 14, para. 3.5:

"The State should take appropriate steps within the legislative and regulatory framework to establish and ensure the proper implementation of its *nuclear security regime* throughout the life cycle of the *radioactive material*."

- IAEA NSS No. 14, para. 3.6:

"The State should designate one or more *competent authorities*, including a *regulatory body,* for the establishment, implementation and maintenance of a *nuclear security regime*, which have a clearly defined legal status and independence from the *operator, shipper* and/or carrier and which have the legal authority to enable them to perform their responsibilities and functions effectively."

- IAEA NSS No. 14, para. 3.7:

"The State should ensure that the *regulatory body* and other *competent authorities* are adequately provided with the necessary authority, competence and financial and human resources to fulfil their assigned nuclear security responsibilities."

- IAEA NSS No. 14, para. 3.8:

"The State should establish requirements in accordance with national practices to ensure appropriate protection of specific or detailed information, which could compromise the security of *radioactive material, associated facilities* and *associated activities* if the information were disclosed."

- IAEA NSS No. 14, para. 3.9:

"The State should ensure that measures, consistent with national practices, are in place to ensure the trustworthiness of persons with authorized access to sensitive information or, as applicable, to *radioactive material*, *associated facilities* and *associated activities*."

- IAEA NSS No. 14, para. 3.10:

"The State should establish, develop and maintain a national register of *radioactive material* over thresholds defined by the State. This national register should, as a minimum, include Category 1 and 2 radioactive sealed sources, as described in the Code of Conduct on the Safety and Security of Radioactive Sources. Other *radioactive material* could, as appropriate, be included in this register."

- IAEA NSS No. 14, para. 4.26:

"Security requirements for *radioactive material* in transport should be developed by the State to minimize the likelihood of loss of control, or *malicious acts*. To the extent *nuclear material* is a potential target for *unauthorized removal* and subsequent dispersion, those requirements should also apply."

5.6.2.2. Documentation

In addition to the material provided by the State in advance of the IPPAS mission, the following documentation is expected to be requested by the team for review during the mission:

- Budget allocations at the competent authorities;
- Procedures on the management of sensitive/classified information;
- Qualification requirements for security related job positions;

- Procedures on security vetting of personnel;
- Rules/procedures for maintaining the national register of radioactive material.

5.6.2.3. Data to be collected/specimen questions

Determine if and how:

- The nuclear security regime of radioactive material, associated facilities and associated activities takes into account the risk of malicious acts involving radioactive material (that could cause unacceptable radiological consequences).
- The radioactive material, associated facilities and associated activities forming the scope of the nuclear security regime are defined (in terms of nuclides and quantities present) in the legislation.
- The legislation prescribes and assigns governmental responsibilities to relevant entities, including an independent regulatory body, for the establishment, implementation and maintenance of a nuclear security regime.
- The competent authorities have a clearly defined legal status and independence from the operator, shipper and/or carrier.
- The competent authorities have the legal authority, competence, and financial and human resources to fulfil their assigned responsibilities.
- The legislation places the prime responsibility on the operator, shipper and/or carrier for implementing and maintaining security measures.
- The legislation and the regulatory framework establish a security related authorization process that could be integrated within one defined for safety/radiation protection.
- The legislation and the regulatory framework establish the inspection process for security requirements.
- The legislation and the regulatory framework establish the enforcement process for the failure to comply with the established requirements.
- The legislation and the regulatory framework establish sanctions against the unauthorized removal of radioactive material and the sabotage of associated facilities and associated activities.
- The legislation and the regulatory framework take into account the interface between security and safety of radioactive material.
- The legislation and the regulatory framework cover the whole life cycle of the radioactive material.
- The legislation and the regulatory framework establish requirements for the definition, classification and protection of sensitive information.
- The legislation and the regulatory framework establish requirements for checking the trustworthiness of persons having authorized access to sensitive information or to radioactive material, associated facilities and associated activities.
- The legislation and the regulatory framework establish a national register of radioactive material.

5.6.3. Regulatory body

5.6.3.1. Basis for recommendations

- IAEA NSS No. 14, para. 3.11:

"The *regulatory body* should implement the legislative and regulatory framework and authorize activities only when they comply with its nuclear security regulations. Where it is required, the security plan, as defined in paras 4.20 and 4.21, can be used by the regulatory body in its determination for issuance of an authorization."

- IAEA NSS No. 14, para. 3.12:

"The *regulatory body* should verify continued compliance with nuclear security regulations and relevant authorization conditions, notably through periodic inspections and ensuring that corrective action is taken, when needed. Inspections of security measures implemented by an *operator, shipper* and/or carrier could be performed together with inspections for verifying compliance with other regulatory requirements, such as radiation protection and safety. The security plan could be referred to by the *regulatory body* for these activities."

5.6.3.2. Documentation

In addition to the material provided by the State in advance of the IPPAS mission, the following documentation is expected to be requested by the team for review during the mission:

- Guidelines on how the operator, shipper and/or carrier should comply with security requirements;
- Regulatory procedures on authorization;
- Regulatory procedures on inspection;
- Regulatory procedures on enforcement.

5.6.3.3. Data to be collected/specimen questions

Determine if and how:

- The regulatory body implements the legislative and regulatory framework.
- The regulatory body authorizes activities only when they comply with the nuclear security regulations.
- The regulatory body requires the security plans of operators, shippers and/or carriers provide the basis for authorization (and inspections).
- The regulatory body verifies the continued compliance with regulations and licence conditions through periodic inspections (could be together with safety/radiation protection related inspections) and ensures that corrective action is taken when needed and imposes sanctions for non-compliance.

5.6.4. Operator, shipper and/or carrier

5.6.4.1. Basis for recommendations

- IAEA NSS No. 14, para. 3.13:

"The legislative and regulatory framework should require that the *operator*, *shipper* and/or carrier:

- Comply with all applicable regulations and requirements established by the State and the *regulatory body*.
- Implement security measures that comply with requirements established by the State and the *regulatory body*.
- Establish quality management programmes that provide:
    - Assurance that the specified requirements relating to nuclear security are satisfied;
    - Assurance that the components of the *nuclear security system* are of a quality sufficient for their tasks;
    - Quality control mechanisms and procedures for reviewing and assessing the overall effectiveness of security measure.
- Report to the *regulatory body* and/or to any other *competent authority*, all *nuclear security events* involving *radioactive material*, *associated facilities* and *associated activities* according to national practices.
- Cooperate with and assist any relevant *competent authorities* in the case of a *nuclear security event.*"

5.6.4.2. Documentation

In addition to the material provided by the State in advance of the IPPAS mission, the following documentation is expected to be requested by the team for review during the mission:

- Security procedures of the operator, shipper and/or carrier to be visited;
- Security related quality management programme of the operator, shipper and/or carrier to be visited;
- Procedures of the operator, shipper and/or carrier to be visited on reporting nuclear security events to the competent authorities;
- Procedures of the operator, shipper and/or carrier to be visited on cooperation with, and assistance to, the competent authorities in the case of a nuclear security event.

5.6.4.3. Data to be collected/specimen questions

Determine if and how:

- The legislative and regulatory framework requires the operator, shipper and/or carrier to comply with regulations and requirements.
- The legislative and regulatory framework requires the operator, shipper and/or carrier to implement security measures.
- The legislative and regulatory framework requires the operator, shipper and/or carrier to establish quality management programmes (assurance of compliance, adequate quality of security system

components, quality control procedures for reviewing and assessing the overall effectiveness of the implemented security measures).
- The legislative and regulatory framework requires the operator, shipper and/or carrier to report nuclear security events to the regulatory body and/or to any other competent authority.
- The legislative and regulatory framework requires the operator, shipper and/or carrier to cooperate with and assist any relevant competent authority in the case of a nuclear security event.

5.7. INTERNATIONAL COOPERATION AND ASSISTANCE

5.7.1. Objectives

This section provides the basis for the recommendations and suggestions, as well as the data to be collected, in relation to:

- How the State cooperates with other States and provides assistance to them if requested;
- The participation of the State in relevant international databases and activities.

5.7.2. Basis for recommendations

- IAEA Code of Conduct, para. 12:

"Every State should ensure that information concerning any loss of control over radioactive sources, or any incidents, with potential transboundary effects involving radioactive sources, is provided promptly to potentially affected States through established IAEA or other mechanisms."

- IAEA NSS No. 14, para. 3.14:

"States are encouraged to cooperate and consult, and to exchange information on nuclear security techniques and practices, either directly or through relevant international organizations."

- IAEA NSS No. 14, para. 3.15:

"States concerned should, in accordance with their national law, provide cooperation and assistance to the maximum feasible extent in the location and recovery of *radioactive material* to any State that so request."

- IAEA NSS No. 14, para. 3.16:

"For the purpose of reporting *nuclear security events*, States should consider establishing suitable arrangements to enable them to participate in relevant regional and international databases and international activities in accordance with their national legislation. One example is the IAEA's Incident Trafficking Database (ITDB). Consideration should also be given to other bilateral and multilateral support arrangements."

5.7.3. Documentation

In addition to the material provided by the State in advance of the IPPAS mission, the following documentation is expected to be requested by the team for review during the mission:

- International/multilateral cooperation and assistance agreements and information exchange procedures, reports on results of international/multilateral cooperation and assistance programmes;
- Bilateral cooperation and assistance agreements and information exchange procedures;
- Documents on participation in IAEA and other relevant international security programmes;
- Reports to the IAEA's Incident and Trafficking Database, if such exist;

- Procedures on communication with other States and the IAEA in relation to reporting and responding to nuclear security events;
- Update on implementation of the Code of Conduct on the Safety and Security of Radioactive Sources;
- Bilateral agreements related to transport security (e.g. cross border interface agreements);
- Membership in regional organizations for competent authorities;
- Membership in multilateral security initiatives.

5.7.4. Data to be collected/specimen questions

Determine if and how:

- The State cooperates and consults with other States to exchange information on nuclear security techniques and practices.
- The State provides cooperation and assistance in the location and recovery of radioactive material to any State that so request.
- The State participates in relevant regional and international databases and international activities.

5.8. IDENTIFICATION AND ASSESSMENT OF THREATS

5.8.1. Objectives

This section provides the basis for the recommendations and suggestions, as well as the data to be collected, in relation to:

- The national threat assessment and/or DBT and its update;
- How the regulatory body obtains threat information from other State authorities;
- How the threat related information is used as a basis for determining security requirements for operators, shippers and/or carriers;
- The procedures for informing operators, shippers and/or carriers about threat information.

5.8.2. Basis for recommendations

- IAEA NSS No. 14, para. 3.17:

"The State should assess its national *threat* for *radioactive material*, *associated facilities* and *associated activities*. The State should periodically review its national *threat*, and evaluate the implications of any changes in the *threat* for the design or update of its *nuclear security regime*."

- IAEA NSS No. 14, para. 3.18:

"The *regulatory body* should use the results of the *threat assessment* as a common basis for determining security requirements for *radioactive material* and for periodically evaluating their adequacy. The *regulatory body* should have access to information from other State authorities on present and foreseeable *threats* involving *radioactive material*."

- IAEA NSS No. 14, para. 4.2:

"The determination of a national *threat* to *radioactive material* in use, storage and transport and *associated facilities* is a key step in establishing the required security measures. The results of the *threat assessment* should be used as a common basis for determining security requirements, developed by the *regulatory body* and evaluating security measures, implemented by the *operator*, *shipper* and/or carrier."

5.8.3. Documentation

In addition to the material provided by the State in advance of the IPPAS mission, the following documentation is expected to be requested by the team for review during the mission:

- The most recent threat assessment, or a description or summary, if possible, or at least a description of how the threat assessment was used to define the legislative and regulatory requirements;
- The threat basis which is applied to operators, shippers and/or carriers of radioactive material, if possible.

5.8.4. Data to be collected/specimen questions

Determine if and how:

- The State assesses its national threat.
- The State periodically reviews its national threat and evaluates the implications of any changes in the threat for the design or update of its nuclear security regime.
- The regulatory body has access to threat related information from other competent authorities.
- Insider threats are taken into account in the threat assessment.[5]
- The regulatory body uses the results of the threat assessment as a common basis for security requirements and evaluating the security measures implemented by the operator, shipper and/or carrier.
- The regulatory body provides threat information to operators, shippers and/or carriers.

5.9. RISK BASED NUCLEAR SECURITY SYSTEMS AND MEASURES

5.9.1. Objectives

This section provides the basis for the recommendations, as well as the data to be collected, in relation to:

- How the legislative and regulatory framework takes into account the potential threats, potential consequences and likelihood of *malicious acts*:
- Steps towards reducing the risk associated with radioactive material;
- The application of the graded approach;
- The established security levels;
- The application of the defence in depth approach.

5.9.2. Risk management

5.9.2.1. Basis for recommendations

- IAEA NSS No. 14, para. 3.19:

"The State should follow a structured risk management approach to reduce the risks of *malicious acts* to an acceptable level. The State should assess the potential *threats*, the potential consequences and the likelihood of *malicious acts*, and then develop a legislative and regulatory framework that provides for efficient and effective security measures to address the *threat*."

[5] For insider threats, reference should be made to IAEA NSS No. 8, Preventive and Protective Measures Against Insider Threats.

- IAEA NSS No. 14, para. 3.20:

"The State should decide what level of risk is acceptable and what level of effort is justified to protect *radioactive material*, *associated facilities* and *associated activities* against the *threat* so as to reduce the risk to an acceptable level, given the availability of resources, the benefit of the protected asset to society, and other priorities. The required security measures may take advantage of other measures established for radiological safety purposes."

- IAEA NSS No. 14, para. 3.22:

"The State should consider ways of reducing the nuclear security risk associated with *radioactive material,* particularly *radioactive sources*, for example by encouraging the use of an alternative radionuclide, chemical form, or non-radioactive technology, or by encouraging device designs that are more tamper resistant."

- IAEA NSS No. 14, para. 3.23:

"The *regulatory body* should develop requirements by using a *graded approach* applying the principles of risk management including a categorization of *radioactive material*."

- IAEA NSS No. 14, para. 3.24:

"The *regulatory body* should develop requirements based on the concept of *defence in depth*. Security requirements for *radioactive material* require a designed mixture of hardware (security devices), procedures (access control, follow-up, etc.) and facility design."

- IAEA NSS No. 14, para. 4.3:

"Security requirements for *radioactive material* should be based on a *graded approach*, taking into account the principles of risk management, including such considerations as the level of *threat* and the relative attractiveness of the material for a *malicious act* leading to potential *unacceptable radiological consequences* (based on such factors as quantity, its physical and chemical properties, its mobility, and its availability and accessibility). Security requirements should be adapted depending on whether the *radioactive material* concerned is a sealed source, unsealed source, disused sealed source or waste, and should cover transport."

- IAEA NSS No. 14, para. 4.4:

"A categorization system should be established that implements the *graded approach* by associating security levels (required degrees of protection) with specific types and quantities of *radioactive material*, thereby ensuring greater levels of protection for *radioactive material* for which a *malicious act* could result in higher consequences. The categorization system should take aggregation of *radioactive material* into account as appropriate. As a starting point, the categorization system should take into account international guidance such as the Code of Conduct on the Safety and Security of Radioactive Sources or the Regulations for the Safe Transport of Nuclear Material (TS-R-1)."

- IAEA NSS No. 14, para. 4.5:

"The State should define a threshold for *radioactive material* that does not represent a substantial security concern and that should be controlled to prevent *unauthorized removal* and unauthorized access through prudent management practice."

- IAEA NSS No. 14, para. 4.6:

"The *regulatory body* should establish goals or objectives that define the required outcome of *nuclear security systems* for each security level."

- IAEA NSS No. 14, para. 4.27:

"The design of an adequate transport security system should incorporate the concept of *defence in depth* and use a *graded approach* to achieve the objective of preventing *malicious acts,* taking into account the potential vulnerability of the *radioactive material*."

- IAEA NSS No. 14, para. 4.28:

"Security of *radioactive material* in transport should, in addition to recommendations in this publication, take into account the United Nations Recommendations for the Transport of Dangerous Goods — Model Regulations, which include security requirements for the transport of dangerous goods and are implemented by many States and international modal organizations."

5.9.2.2. Documentation

Most of the documentation for this Section should have been provided in advance of the mission. Any missing or additional documentation should be provided to the team during the mission.

5.9.2.3. Data to be collected/specimen questions

Determine if and how:

- The legislative and regulatory framework provides for efficient and effective security measures based on the national threat assessment, potential consequences and the likelihood of malicious acts.
- The State has taken a decision on the level of risk that is deemed acceptable.
- The risk is reduced to an acceptable level, given the availability of resources and the benefit of the radioactive material, associated facility and associated activities to the society.
- The required security measures take advantage of other measures established for radiological safety purposes.
- The State has considered the use of alternative (less attractive) radionuclide and chemical forms or non-radioactive technology and more tamper resistant device design.
- The graded approach is developed by the regulatory body based on categorization of radioactive material.
- Requirements are developed based on the defence in depth approach, including a designed mixture of hardware, procedures and facility design.
- Security requirements are adapted depending on whether the radioactive material concerned is a sealed source (special attention is paid to a mobile and portable radioactive source), unsealed source, disused sealed source or radioactive waste and whether the radioactive material is in use, storage or transport.

- The categorization of radioactive material is in accordance with international guidance, such as the Code of Conduct on Safety and Security of Radioactive Sources and the UN Model Regulations or the State has an explanation for any deviations.
- A threshold is defined for radioactive material that does not represent a substantial security concern, which material is protected through prudent management practice.
- The security levels (required degree of protection) are established, based on categorization.

5.9.3. Interface with the safety system

5.9.3.1. Basis for recommendations[6]

- IAEA NSS No. 14, para. 3.25:

"Recognizing that both safety and security have a common aim — to protect persons, society and the environment from harmful effects of radiation — a well-coordinated approach in safety and in security is mutually beneficial, the State should ensure that:

- Consultation and coordination are maintained between those responsible for safety and security to ensure efficient security of *radioactive material* and to ensure that regulatory requirements are consistent, especially when responsibility for safety and security is assigned to different *competent authorities*;
- Major decisions regarding safety and security require participation of experts in safety and in security on a continual basis;
- The safety and security interfaces should be strengthened by building safety culture and *nuclear security culture* into the management system."

- IAEA NSS No. 14, para. 3.26:

"The State should ensure that a balance is maintained between safety and security throughout the *nuclear security regime*, from the development of the legislative framework to implementation of security measures."

- IAEA NSS No. 14, para. 3.27:

"The *competent authorities* should ensure that security measures for *radioactive material*, *associated facilities* and *associated activities* take into account those measures established for safety and are developed so that they do not contradict each other, during both normal and emergency situations."

- IAEA NSS No. 14, para. 3.28:

"The *competent authorities* working with the *operator* should ensure to the extent possible that security measures during a response to a *nuclear security event* do not adversely affect the safety of the personnel. Security personnel should manage their actions in a way that maintains the safety of all potentially affected persons, whether on or off-site."

[6] GSR Part 1 Requirement 12: "The government shall ensure that, within the governmental and legal framework, adequate infrastructural arrangements are established for interfaces of safety with arrangements for nuclear security…."

5.9.3.2. Documentation

In addition to the material provided by the State in advance of the IPPAS mission, the following documentation is expected to be requested by the team for review during the mission:

- Regulatory procedures on authorization;
- Regulatory procedures on inspection planning;
- Minutes of joint meetings of those responsible for safety and security;
- Procedures of the operator, shipper and/or carrier to be visited on preparation of a licence application;
- Signature of the person responsible for safety on the approval sheet of the contingency plan;
- Signature of the person responsible for security on the approval sheet of the emergency plan.

5.9.3.3. Data to be collected/specimen questions

Determine if and how:

- The regulatory requirements identify safety and security interfaces in order to maximize synergies and minimize duplication.
- The requirements for safety and security are consistent and do not contradict each other during either normal operation or emergency situations.
- Consultation and coordination are performed between those responsible for safety and security.
- Major decisions regarding safety or security require the participation of experts from both safety and security.
- Security and safety inspections are conducted jointly or separately and, if the latter, do the results of one inform the other?
- The security measures of competent authorities during a response to a nuclear security event do not adversely affect, to the extent possible, the safety of any person, whether on- or off-site.

5.10. SUSTAINING THE NUCLEAR SECURITY REGIME

5.10.1. Objectives

This section provides the basis for the recommendations, as well as the data to be collected, in relation to:

- The recognition that a credible threat exists and that nuclear security is important to counter this threat;
- The development and maintenance of a nuclear security culture;
- The recognition that nuclear security is a long term commitment;
- The availability of the necessary human and financial resources;
- The availability of training at all levels.

5.10.2. Basis for recommendations

- IAEA NSS No. 14, para. 3.29:

"The State should commit the necessary resources, including human and financial resources, to ensure that its *nuclear security regime* is sustained and effective in the long term to provide adequate nuclear security for *radioactive material*."

- IAEA NSS No. 14, para. 3.30:

"The State should promote a *nuclear security culture*."

- IAEA NSS No. 14, para. 3.31:

"All organizations and individuals involved in implementing nuclear security should give due priority to the *nuclear security culture* with regard to *radioactive material*, to its development and maintenance necessary to ensure its effective implementation in the entire organization."

- IAEA NSS No. 14, para. 3.32:

"The foundation of a *nuclear security culture* should be the recognition that a credible *threat* exists, that preserving nuclear security is important, and that the role of the individual is important."

- IAEA NSS No. 13, para. 3.56:

"The State should establish a sustainability programme to ensure that its *physical protection regime* is sustained and effective in the long term by committing the necessary resources."

- IAEA NSS No. 13, para. 3.57:

"*Operators*, *shippers* and carriers should establish sustainability programmes for their *physical protection system*. Sustainability programmes should encompass:

  - Operating procedures (instructions).
  - Human resources management and training.
  - Equipment updating, maintenance, repair and calibration.
  - *Performance testing* and operational monitoring.
  - Configuration management (the process of identifying and documenting the characteristics of a facility's *physical protection system* — including computer systems and software — and of ensuring that changes to these characteristics are properly developed, assessed, approved, issued, implemented, verified, recorded and incorporated into the facility documentation).
  - Resource allocation and operational cost analysis."

5.10.3. Documentation

In addition to the material provided by the State in advance of the IPPAS mission, the following documentation is expected to be requested by the team for review during the mission:

- Security policies and programmes of the competent authorities, the operator, shipper and/or carrier which are designed to promote a security culture;
- Budget allocations at the competent authorities;
- Training programmes (basic, advanced and refresher trainings);
- Training records on staff participation.

5.10.4. Data to be collected/specimen questions

Determine if and how:

- Nuclear security culture is established and promoted.
- Training programmes are established to ensure ongoing security awareness.
- The operating budget identifies resource needs and planned funding allocations.

- Necessary resources, including human and financial resources, are available for sustaining an effective nuclear security regime.
- Procedures are in place for operating, updating, maintaining, repairing and calibrating security system components.
- Procedures are in place to conduct *performance testing* of the security system and its components.
- Procedures are in place to evaluate the effectiveness of the security system and a budget is available to replace or update components.

5.11. PLANNING AND PREPAREDNESS FOR AND RESPONSE TO NUCLEAR SECURITY EVENTS

5.11.1. Objectives

This section provides the basis for the recommendations, as well as the data to be collected, in relation to:

- The operator's contingency plan;
- The State's response plan.

5.11.2. Basis for recommendations

- IAEA Code of Conduct, para. 22(o):

"Every State should ensure that its regulatory body is prepared, or has established provisions, to recover and restore appropriate control over orphan sources, and to deal with radiological emergencies and has established appropriate response plans and measures."

- IAEA NSS No. 14, para. 3.33:

"The *regulatory body* should ensure that the *operator's* security plan includes measures to effectively respond to a *malicious act* consistent with the *threat*."

5.11.3. Documentation

In addition to the material provided by the State in advance of the IPPAS mission, the following documentation is expected to be requested by the team for review during the mission:

- Contingency and emergency plans and procedures of the competent authorities, and of the operator, shipper and/or carrier to be visited.

5.11.4. Data to be collected/specimen questions

Determine if and how:

- Operators' security plans are required to include measures to respond effectively to a security event.
- State level plan exists to deal with radiological emergencies.
- The interface between emergency and contingency planning is ensured at State level and operator level.

5.12. IMPORT AND EXPORT OF RADIOACTIVE MATERIAL

5.12.1. Objectives

This section provides the basis for the recommendations, as well as the data to be collected, in relation to:

- The State's requirements and authorization system for import and export of Category I and II sources;

- Coordination between exporters and importers regarding security issues on the export/import of radioactive material.

5.12.2. Basis for recommendations

- IAEA Code of Conduct, para. 23:

"Every State involved in the import or export of radioactive sources should take appropriate steps to ensure that transfers are undertaken in a manner consistent with the provisions of the Code and that transfers of radioactive sources in Categories 1 and 2 of Annex 1 of this Code take place only with the prior notification by the exporting State and, as appropriate, consent by the importing State in accordance with their respective laws and regulations."

- IAEA Code of Conduct, para. 24:

"Every State intending to authorize the import of radioactive sources in Categories 1 and 2 of Annex 1 to this Code should consent to their import only if the recipient is authorized to receive and possess the source under its national law and the State has the appropriate technical and administrative capability, resources and regulatory structure needed to ensure that the source will be managed in a manner consistent with the provisions of this Code."

- IAEA Code of Conduct, para. 25:

"Every State intending to authorize the export of radioactive sources in Categories 1 and 2 of Annex 1 to this Code should consent to its export only if it can satisfy itself, insofar as practicable, that the receiving State has authorized the recipient to receive and possess the source and has the appropriate technical and administrative capability, resources and regulatory structure needed to ensure that the source will be managed in a manner consistent with the provisions of this Code."

- IAEA Code of Conduct, para. 26:

"If the conditions in paragraphs 24 and 25 with respect to a particular import or export cannot be satisfied, that import or export may be authorized in exceptional circumstances with the consent of the importing State if an alternative arrangement has been made to ensure the source will be managed in a safe and secure manner."

- IAEA Code of Conduct, para. 27:

"Every State should allow for re-entry into its territory of disused radioactive sources if, in the framework of its national law, it has accepted that they be returned to a manufacturer authorized to manage the disused sources."

- IAEA Code of Conduct, para. 28:

"Every State which authorizes the import or export of a radioactive source should take appropriate steps to ensure that such import or export is conducted in a manner consistent with existing relevant international standards relating to the transport of radioactive material."

- IAEA Code of Conduct, para. 29:

"Although not subject to the authorization procedures outlined in paragraphs 24 and 25 above, the transport of radioactive sources through the territory of a transit or transshipment State should be

conducted in a manner consistent with existing relevant international standards relating to the transport of radioactive material, in particular paying careful attention to maintaining continuity of control during international transport."

- IAEA NSS No. 14, para. 3.34:

"The State should take appropriate steps, including coordination between importer and exporter States prior to the transfer, to reduce the likelihood of *malicious acts* in connection with the import or export of quantities of *radioactive material* above thresholds that it defines. At a minimum, these steps should encompass requirements concerning Categories I and II sealed *radioactive sources*, consistent with the Guidance on the Import and Export of Radioactive Sources."

5.12.3. Documentation

In addition to the material provided by the State in advance of the IPPAS mission, the following documentation is expected to be requested by the team for review during the mission:

- Procedures on authorization of export and import, including enforcement measures;
- Requests for consent, shipment notifications between exporting and importing States;
- Bilateral arrangements between exporting and importing States;
- Agreement between exporting and importing facilities to be examined, if such agreement exists, for the return of disused sources to the supplier.

5.12.4. Data to be collected/specimen questions

Determine if and how:

- The State has established procedures for the authorization and control of exports of Categories I and II radioactive sources, consistent with the Guidance on the Import and Export of Radioactive Sources, including the evaluation by the State of the application for an export authorization submitted by the exporting facility; obtaining the consent of the importing State prior to authorizing the export (Category I sources only); and providing notification to the importing State prior to the specific shipments.
- The State has established procedures for the authorization and control of imports of Categories I and II sources consistent with the Guidance on the Import and Export of Radioactive Sources.
- The State has appropriate measures in place for enforcing these procedures.
- The State has nominated a point of contact (either a person or a position) for the purpose of facilitating the export and/or import of radioactive sources in accordance with the Code and the Import–Export Guidance.
- The State has made available to the IAEA its responses to the Importing and Exporting States Questionnaire (Annex I of the Import–Export Guidance).
- Authorization of export/import includes the checking by the State/exporting facility what/how the security measures are implemented by the State/importing facility.

5.13. DETECTION OF NUCLEAR SECURITY EVENTS

5.13.1. Objectives

This section provides the basis for the recommendations, as well as the data to be collected, in relation to:

- How nuclear security events (including absence or discrepancies of radioactive material, regulatory non-compliance, loss of regulatory control) must be detected, investigated, and reported by the operator.

5.13.2. Basis for recommendations

- IAEA NSS No. 14, para. 3.35:

"The *regulatory body* should establish requirements for *operators*, *shippers* and/or carriers to have appropriate and effective security measures to detect *nuclear security events* and to report any such event promptly with the aim of providing a timely response. These requirements should consider those made in IAEA Nuclear Security Series No. 15, Nuclear Security Recommendations on Nuclear and Other Radioactive Material out of Regulatory Control."

- IAEA NSS No. 14, para. 4.25:

"Any absence or discrepancy regarding the presence or amount of *radioactive material*, particularly during an inventory, should be promptly investigated. *Operators* should be required to promptly report to the *regulatory body* and other relevant *competent authorities* (e.g. law enforcement) upon determination of loss and control of *radioactive material*."

- IAEA NSS No. 15, para. 5.17:

"The *competent authority* with regulatory responsibility should require *authorized persons* to report immediately any regulatory non-compliance which they suspect could have nuclear security implications. Such a report would enable the *competent authority* to assess the event and alert other *competent authorities* with the aim of preventing a consequent criminal or unauthorized act with nuclear security implications."

- IAEA NSS No. 15, para. 5.18:

"The *competent authority* with regulatory responsibility should develop procedures and protocols to assist *authorized persons* to report their regulatory non-compliances having nuclear security implications."

- IAEA NSS No. 15, para. 5.19:

"The State should ensure that *competent authorities* are legally empowered to require *authorized persons* to immediately report lost, missing or stolen nuclear or other *radioactive material* for which they hold an *authorization*. Such a report should be regarded as *detection* by an information alert of a potential criminal act, or an unauthorized act, with nuclear security implications."

- IAEA NSS No. 15, para. 5.20:

"The State should ensure that any *competent authority* that issues *authorizations* related to nuclear or other *radioactive material*, and that receives a report that such material has been reported as lost, missing or stolen, promptly inform other relevant *competent authorities*."

- IAEA NSS No. 15, para. 5.21:

"The *competent authorities* responsible for implementing *nuclear security measures* related to customs and border control should report the *detection* of any nuclear or other *radioactive material* that is not under *regulatory control* to other relevant *competent authorities*, including the *regulatory body*."

5.13.3. Documentation

In addition to the material provided by the State in advance of the IPPAS mission, the following documentation is expected to be requested by the team for review during the mission:

- Regulatory guidelines, backed by national law, defining a nuclear security event and identifying the authorized person(s) responsible for the reporting;
- Regulatory requirements, procedures or protocols for the prompt reporting of nuclear security events by operator, shipper and/or carrier;
- Regulatory procedures or guidance for assisting an operator, shipper and/or carrier to report regulatory non-compliance;
- Regulatory procedures or arrangements for investigating nuclear security events reported by the operator, shipper and/or carrier;
- Procedures for disseminating nuclear security event information among relevant competent authorities (specifically between competent authorities responsible for border and customs issues and the regulatory authority);
- Investigation reports, including lessons learned and corrective actions from previous nuclear security events taken by the operator, shipper and/or carrier.

5.13.4. Data to be collected/specimen questions

Determine if and how:

- Detection, investigation, and prompt reporting of security events are required by the competent authorities, including the regulatory body.
- Detection, investigation and prompt reporting of security events are performed by the operator, shipper and/or carrier to be visited.
- Investigation of nuclear security events is conducted by the competent authorities, including the regulatory body.

5.14. SECURITY OF RADIOACTIVE MATERIAL IN USE AND STORAGE

This section of the Guidelines concerns:

- The degree to which the regulatory security requirements for radioactive material, associated facilities and associated activities meet international commitments, obligations and guidance;
- The radioactive material, associated facilities and associated activities assessed or visited during the IPPAS mission.

5.14.1. Objectives

From the regulatory body, to determine the:

- Regulatory approach followed (prescriptive, performance based, combined);
- Established goals and objectives for security levels;
- Requirements for security functions (detection, delay, response and response);
- Requirements for security management measures.

From the operator, to determine the:

- Scope and contents of the security plan;

- The implemented detection, delay, and response measures;
- The implemented security management measures.

5.14.2. Basis for recommendations

- IAEA NSS No. 14, para. 4.8:

"Security requirements should be developed by the State that protect *radioactive material* from *unauthorized removal* or loss of control and should address both security systems and security management. To the extent *nuclear material* is a potential target for *unauthorized removal* and subsequent dispersion, those requirements should also apply."

- IAEA NSS No. 14, para. 4.9:

"*Radioactive material* that represents a substantial security concern (above a threshold defined by the State) should require security measures commensurate with the security levels defined in paras 4.4 and 4.5. For each security level, the State should require graded security measures considering those described below. Particular measures may be required for mobile and portable radioactive sources."

5.14.3. Security system

5.14.3.1. Basis for recommendations

- IAEA NSS No. 14, para. 4.10:

"The *regulatory body* should require *operators* to implement a security system that meets applicable *nuclear security regime* objectives. The system should be designed to adequately perform the security functions of detection, delay, and response (as described below) in order to deter and prevent *malicious acts*. While deterrence is not measurable, it is clear that a suitably robust security system can help to deter a *malicious act*. In implementing a *graded approach*, the objectives of security systems could range from preventing a *malicious act* to reducing its likelihood."

- IAEA NSS No. 14, para. 4.11:

"Detection measures should be implemented for the discovery and assessment of an attempted or actual intrusion which could have the objective of *unauthorized removal* or *sabotage* of *radioactive material*. Detection can be achieved by such means as visual observation, video surveillance, electronic sensors, accountancy records, seals and other tamper indicating devices, and process monitoring systems. In implementing a *graded approach*, the objectives of detection measures could range from immediate detection, assessment and communication of any unauthorized access to subsequent detection of *unauthorized removal* through tamper indicators or periodic physical checks."

- IAEA NSS No. 14, para. 4.12:

"Delay measures should be implemented to impede an adversary's attempt to gain unauthorized access or to remove *radioactive material* or *sabotage associated facilities*, generally through multiple barriers or other physical means, such as locked doors, cages, tie-downs or the like. A measure of delay is the time, after detection, that is required by an adversary to remove the *radioactive material* or sabotage the *associated facilities*. In implementing a *graded approach*, the objectives of delay measures could range

from providing sufficient delay after detection to allow response personnel to interrupt *malicious acts* to providing delay to allow for timely pursuit following *unauthorized removal*."

- IAEA NSS No. 14, para. 4.13:

"Response measures should be implemented following detection and assessment. The *operator* should be required to make appropriate arrangements to communicate with law enforcement personnel following detection and assessment in order that they may perform the response. In implementing a *graded approach*, the objectives of response measures could range from providing immediate response with sufficient resources to interrupt *malicious acts* to providing alarm notification to allow the appropriate authority to investigate the event."

- IAEA NSS No. 14, para. 4.14:

"The *operator* should cooperate with and assist the *competent authorities* as appropriate in their efforts to locate and recover the *radioactive material*, including cooperation in on-site and off-site response."

- IAEA NSS No. 14, para. 4.15:

"The level of protection against *sabotage* may differ from that against *unauthorized removal*. *Nuclear security systems* designed to protect *radioactive material* from *unauthorized removal* generally also provide some degree of protection of the *radioactive material* and *associated facilities* against *sabotage*. If the *regulatory body* becomes aware of a specific *threat* of *sabotage* against particular *radioactive material* or particular facilities, the *regulatory body* should require additional or more stringent security measures to increase the level of protection against *sabotage*."

- IAEA NSS No. 14, para. 4.16:

"*Operators* should be required to implement security management measures, addressing access control, trustworthiness, information protection, preparation of a security plan, training and qualification, accounting, inventory and event reporting. The stringency of required security management measures should vary as appropriate based on the *graded approach*."

- IAEA NSS No. 14, para. 4.26:

"Security requirements for *radioactive material* in transport should be developed by the State to minimize the likelihood of loss of control, or *malicious acts*. To the extent *nuclear material* is a potential target for *unauthorized removal* and subsequent dispersion, those requirements should also apply."

- IAEA NSS No. 14, para. 4.31:

"Security measures should be based on a categorization of *radioactive material* and structured into security levels for transport (e.g. basic and enhanced). Security levels should be defined using a *graded approach* that is based on an evaluation of the *threat* to the material and its potential to generate unacceptable consequences."

5.14.3.2. Basis for suggestions

- See Appendix I.

5.14.3.3. Documentation

The data below should be collected from the regulatory authority:

- Regulatory materials or guidance for implementing the regulatory requirements (such as licence application procedures).

The data below should be collected from the visited operator regarding its practice:

- Organizational structure of the operator.
- Security plan of the operator, including a description of the implemented detection and delay systems and their components:
    - Description of the measures applicable to deterrence;
    - Procedures of the operator on detection and assessment;
    - Procedures of the operator on response measures, including communication between response forces and the facility (response plan);
    - Procedures of the operator on the search and recovery of missing radioactive material.
- Procedures for reviewing and updating the security plan on a regular basis.
- Procedures of the operator for security management:
    - Procedures of the operator on access control, including personnel and visitors;
    - Procedures of the operator on trustworthiness checking;
    - Procedures of the operator on the management of sensitive information;
    - Procedures on inventory recording and control of radioactive material;
    - Procedures of the operator on the search and recovery of missing radioactive material;
    - Maintenance and testing plan of the operator in relation to physical protection systems and components;
    - Maintenance records of the operator in relation to physical protection systems and components;
    - Records of the operator on the testing of the effectiveness of the physical protection system;
    - Qualification and training records of the operator;
    - Regular and occasional reports of the operator on security management issues.

5.14.3.4. Data to be collected/specimen questions

From the regulatory body, determine if and how:

- The regulations follow a performance based, prescriptive or combined approach.
- The regulator requires the operator to cooperate with and assist relevant competent authorities, as appropriate, in their efforts to locate and recover the radioactive material, both on- and off-site.
- Any departures from international guidance are justified and explained.
- Goals and objectives are established by the regulatory body for each security level.
- Security requirements against unauthorized removal address both security systems and security measures.

- The security requirements for radioactive material also apply to the extent nuclear material is a potential target for unauthorized removal and subsequent dispersal or exposure (sabotage is considered under IAEA NSS No. 13).
- Requirements are established for security functions (i.e. deterrence, detection, delay and response) to be implemented by operators, shippers and/or carriers.
- Additional or more stringent security measures are required to be implemented by an operator, shipper and/or carrier, if the regulatory body becomes aware of a specific threat against particular radioactive material, particular facilities or particular shipments.
- To the extent a performance based approach is used:
    - The regulator has clearly defined the goal for each security level, as well as security objectives for each security function in the regulations using a graded approach and based upon the defined threat or threat assessment;
    - The regulator requires the facility to conduct a vulnerability assessment as the basis for developing security measures that meet the assigned objectives;
    - The regulator has established procedures for determining that the operator's proposed security measures for detection, delay, response and security management meet regulatory requirements based upon the operator's vulnerability assessment;
    - The regulator requires procedures for modifying the security system to address increased threats (including sabotage).
- To the extent a prescriptive approach is used:
    - The regulator has clearly defined a list of security objectives in the regulations using a graded approach and based upon the defined threat or threat assessment;
    - The regulations specify required security measures which cover detection, delay, response and security management and which meet the objectives for each security level (see Tables 6–8 of IAEA NSS No. 11);
    - Regulatory procedures for determining that the operator's security measures meet regulatory requirements;
    - Procedures for the regulatory authority to review, evaluate and update the required security measures, both on a regular basis and in response to changes in the threat;
    - Regulatory requirements and procedures for additional security measures related to increased threats;
    - Specific security measures are required for mobile and portable sources and for sources which can be easily removed from their shielded housing (e.g. brachytherapy);
    - More stringent security measures are required to protect against sabotage if the regulatory body becomes aware of a specific sabotage threat.

From the operator, determine if and how:

- The operator has documented clearly in a security plan (see Appendix II of IAEA NSS No. 11 for a list of topics) how it meets all security requirements of the regulatory authority.
- Detection measures (i.e. visual observation, video surveillance, electronic sensors, accountancy records, seals and other tamper indicating devices, process monitoring systems) are implemented by the operator.
- Objectives of detection measures, in implementing a graded approach, range from immediate detection, assessment and communication of any unauthorized access to subsequent detection of unauthorized removal through tamper indicators or periodic physical checks.

- Delay measures after detection (i.e. locked doors, cages, tie-downs) through multiple barriers or other physical means are implemented by the operator.
- Delay after detection, in implementing a graded approach, ranges from providing sufficient delay to allow response personnel to interrupt malicious acts to provision of sufficient delay to allow for timely pursuit following unauthorized removal.
- Response measures are implemented by the operator and coordinated with any identified response forces.
- Objectives of response measures, in implementing a graded approach, range from immediate response with sufficient resources to interrupt malicious acts to provision of alarm notification to allow the appropriate authority to investigate the event.
- Specific security measures are implemented for mobile and portable sources.
- The insider threat is managed by the operator.
- The operator has procedures to cooperate with and assist the competent authorities, as appropriate, in their efforts to locate and recover the radioactive material, both on- and off-site.

5.14.4. Security management

5.14.4.1. Basis for recommendations

- IAEA NSS No. 14, para. 4.16:

"*Operators* should be required to implement security management measures, addressing access control, trustworthiness, information protection, preparation of a security plan, training and qualification, accounting, inventory and event reporting. The stringency of required security management measures should vary as appropriate based on the *graded approach*."

- IAEA NSS No. 14, para. 4.17:

"The *operator* should be required to provide a means of physically controlling access that allows only individuals with authorized access to enter areas where *radioactive material* is present. Unescorted access should be limited to individuals with authorized access with a demonstrated need for such access in the performance of their jobs. Other individuals should be allowed access to this area only if they are escorted or observed by an individual authorized for unescorted access, or if compensatory measures for the security of *radioactive material* have been implemented."

- IAEA NSS No. 14, para. 4.18:

"The *competent authority* should ensure that the trustworthiness and reliability of individuals with authorized access to *radioactive material* and/or security sensitive information are verified in accordance with the State's national practices. In implementing a *graded approach*, the objectives of trustworthiness measures could range from confirmation of identity to a comprehensive background check by the legitimate national authority, including a verification of references to determine the integrity and reliability of each person. The determination of trustworthiness and reliability is a key measure in mitigating the *threat* posed by *insiders*."

- IAEA NSS No. 14, para. 4.19:

"*Operators* should be required to limit access to security sensitive information to those people who need that information in order to perform their jobs. Key elements of information protection include identifying the information that must be protected; designating individuals with authorized access to such information; and protecting such information from disclosure to individuals who do not have this access."

- IAEA NSS No. 14, para. 4.20:

"*Operators* should be required to develop, implement, test, periodically review, revise as necessary a security plan and comply with its provisions. The plan should describe the overall *nuclear security system* in place to protect the *radioactive material* and should include measures to address an increased threat level, response to *nuclear security events* and the protection of sensitive information. *Operators* should demonstrate to the *regulatory body* how it is meeting security requirements. The security plan should be subject to information protection."

- IAEA NSS No. 14, para. 4.21:

"The security plan should include:

  - A description of the *radioactive material* and the environment for its use and storage;
  - A description of the specific security concerns to be addressed;
  - A description of the security system implemented and its objectives;
  - Security procedures to provide guidance to *operator* personnel for operating and maintaining security measures, and the security procedures to be followed before and after maintenance;
  - Administrative aspects, including defining the roles and responsibilities of individuals with security responsibilities, access authorization processes, trustworthiness determination processes, information protection processes, inventories and records, event reporting, and review and revision of the security plan (including maximum time between reviews);
  - How procedural and administrative security measures will be scaled to meet increased levels of *threat* as assessed by the State;
  - Response actions including cooperation with relevant *competent authorities* in the location and recovery of *radioactive material* consistent with national practice."

- IAEA NSS No. 14, para. 4.22:

"*Operators* should be required to ensure that all personnel with security responsibilities are appropriately trained and qualified prior to commencing their responsibilities and afterwards periodically."

- IAEA NSS No. 14, para. 4.23:

"*Operators* should, consistent with a *graded approach*, be required to account for radioactive sources, particularly in the case of mobile sources."

- IAEA NSS No. 14, para. 4.24:

"*Operators* should be required to establish and maintain a list of *radioactive material* under its responsibility. At intervals prescribed by the *regulatory body*, *operators* should verify that *radioactive material* is present at its authorized location. Inventory verification can be used as part of detection measures."

- IAEA NSS No. 14, para. 4.25:

"Any absence or discrepancy regarding the presence or amount of *radioactive material*, particularly during an inventory, should be promptly investigated. *Operators* should be required to promptly report to the *regulatory body* and other relevant *competent authorities* (e.g. law enforcement) upon determination of loss of control of *radioactive material*."

5.14.4.2. Basis for suggestions

- See Appendix II.

5.14.4.3. Documentation

In addition to the material provided by the State in advance of the IPPAS mission, the following documentation is expected to be requested by the team for review during the mission:

- Security plan of the operator:
    - Budget and resource planning;
    - Organizational structure of the operator;
    - Procedures on updating the security plan;
    - Procedures on access control, including both personnel and visitors;
    - Procedures on trustworthiness checks;
    - Procedures on the management of sensitive information;
    - Procedures on inventory recording and control of radioactive material;
    - Procedures on the search and recovery of missing radioactive material;
    - Maintenance and testing plan/procedures for the physical protection systems and their components;
    - Qualification and training procedures and requirements;
    - Procedures for reporting inventory discrepancies;
    - Procedures for acceptance and transfer of sources into and out of the facility.
- Operator records:
    - Maintenance records in relation to physical protection systems and components;
    - Records on testing the effectiveness of the physical protection system;
    - Accounting and inventory records;
    - Staff training records.
- Regular and occasional reports of the operator to the regulatory body on security management issues.

5.14.4.4. Data to be collected/specimen questions

From the regulatory body, determine if and how:

- Requirements for the implementation of security management measures address access control, trustworthiness, information protection, preparation of a security plan, training and qualification,

accounting, inventory and event reporting exist, the stringency of which varies as appropriate, based on the graded approach.

From the operator, determine if and how:

- The operator provides the means for physically controlling access to allow only individuals with authorized access to areas where radioactive material is present:
    - Unescorted access is limited by the operator to individuals with authorized access and a demonstrated need for such access in the performance of their jobs;
    - Other individuals are allowed by the operator to gain access to such areas only if they are escorted or observed by an individual authorized for unescorted access, or if compensatory measures for the security of the radioactive material have been implemented;
- The trustworthiness and reliability of individuals with authorized access to radioactive material and/or security sensitive information are verified at the request of or by the operator:
    - Objectives of trustworthiness measures, in implementing a graded approach, range from confirmation of identity to a comprehensive background check (including verification of references to determine the integrity and reliability of each person);
    - The insider threat is managed by the operator.
- Access to security sensitive information is limited by the operator to those who need to know the information to perform their jobs:
    - Information protection includes identification of sensitive information, designation of personnel with a need to know and protection of sensitive information from disclosure to those who do not have proper access.
- A security plan is developed, implemented, tested, periodically reviewed and revised as necessary by the operator:
    - The security plan describes the overall nuclear security system in place and the security management measures that have been implemented;
    - The security plan includes measures to address an increased threat level;
    - The security plan demonstrates how the regulatory security requirements are complied with;
    - The security plan is subject to information protection.
- All personnel of the operator with security responsibilities are appropriately trained and qualified prior commencing their responsibilities and afterwards periodically.
- The operator establishes and maintains an inventory list of radioactive material under its responsibility with regularity according to the graded approach:
    - The operator accounts for radioactive sources with regularity according to the graded approach;
    - The operator promptly investigates any absence or discrepancy in inventory, and promptly reports to the regulatory body and to other relevant competent authorities upon determination of loss of control over radioactive material.

5.15. SECURITY OF RADIOACTIVE MATERIAL IN TRANSPORT

This section of the Guidelines concerns the radioactive material in transport reviewed or followed during the IPPAS mission; thus, the following data should be collected from the regulatory body and visited/reviewed shipper and/or carrier regarding its practice.

5.15.1. Objectives

This section provides basis for the recommendations as well as the data to be collected in connection to the security of radioactive material in transport. The objective of this section is to obtain information in relation to:

- Transport security requirements and regulations;
- Implemented detection, delay and response measures;
- Transport security plan;
- Implemented security management measures;
- International transports.

5.15.2. Basis for recommendations

- IAEA NSS No. 14, para. 4.26:

"Security requirements for *radioactive material* in transport should be developed by the State to minimize the likelihood of loss of control, or *malicious acts*. To the extent *nuclear material* is a potential target for *unauthorized removal* and subsequent dispersion, those requirements should also apply."

- IAEA NSS No. 14, para. 4.27:

"The design of an adequate transport security system should incorporate the concept of *defence in depth* and use a *graded approach* to achieve the objective of preventing *malicious acts*, taking into account the potential vulnerability of the *radioactive material*."

- IAEA NSS No. 14, para. 4.28:

"Security of *radioactive material* in transport should, in addition to recommendations in this publication, take into account the United Nations Recommendations for the Transport of Dangerous Goods — Model Regulations, which include security requirements for the transport of dangerous goods and are implemented by many States and international modal organizations."

- IAEA NSS No. 14, para. 4.29:

"For air transport, security measures should be carried out in accordance with the applicable security provisions of the Convention on International Civil Aviation and the International Civil Aviation Organization's Technical Instructions for the Safe Transport of Dangerous Goods by Air. For maritime transport, security measures should be carried out in accordance with the applicable security provisions of the International Ship and Port Facility Security Code and of the International Maritime Dangerous Goods Code as required by the International Convention for the Safety of Life at Sea (SOLAS 74 amended)."

- IAEA NSS No. 14, para. 4.30:

"The transport security system should be designed to take into account the:

- Quantity and the physical/chemical form of the *radioactive material*;
- Mode(s) of transport;
- Package(s) being used."

- IAEA NSS No. 14, para. 4.31:

"The *graded approach* for transport security should be based at least on the properties and quantities of *radioactive material* being shipped:

- Material posing very low potential radiological consequences should be subject only to prudent management practices;
- Material with limited potential radiological consequences should be subject to basic security measures;
- Material posing higher potential radiological consequences should be subject to enhanced security measures."

- IAEA NSS No. 14, para. 4.32:

"The achievement of effective transport security should include considering transport schedules, routing including security of passage, and information security."

- IAEA NSS No. 14, para. 4.33:

"The basic level of security measures should include requiring that consignors, carriers, consignees and other persons engaged in the transport of *radioactive material* implement graded security systems or other arrangements to deter, detect, delay and respond to *malicious acts* affecting the conveyance or its cargo. These arrangements should be operational and effective at all times. This can be achieved by the following:

- When *radioactive material* is temporarily stored at transit sites (such as warehouses and marshalling yards), appropriate security measures should be applied to the *radioactive material* consistent with the measures applied during use and storage.
- Individuals engaged in the transport of *radioactive material* should receive training, including training in the elements of security awareness.
- Security measures should be applied, verified prior to shipment, and remain effective during transport.
- Information on required security measures, including how to respond to a *nuclear security event* during transport, should be provided in writing to crew members.
- Trustworthiness of persons engaged in the transport of *radioactive material* should be established commensurate with their security responsibilities and in accordance with national practices.
- Security related information should be communicated to consignors and carriers engaged in the transport of *radioactive material*.
- The consignee should be informed by the consignor in advance of the planned shipment of the mode of transport and expected delivery time and should notify the consignor on receipt or non-receipt within the expected delivery time frame.
- The movement of packages and/or conveyances containing *radioactive material* should be monitored appropriately.
- Communication should be available to ensure response or provide assistance to the crew.
- Packages and/or conveyances should not be left unattended for any longer than is absolutely necessary."

- IAEA NSS No. 14, para. 4.34:

"Enhanced security measures should include requiring that consignors, carriers, consignees and other persons engaged in the transport of *radioactive material* should develop, adopt, implement, periodically review as necessary and comply with the provisions of a transport security plan. Responsibility for and ownership of the transport security plan should be clearly defined. The plan should describe the overall *nuclear security system* in place to protect the *radioactive material* in transport and should include measures to address an increased *threat* level, response to *nuclear security events* and the protection of sensitive information."

- IAEA NSS No. 14, para. 4.35:

"In certain circumstances, security measures additional to those above should be considered depending on the assessment of the prevailing threat or the attractiveness of the material being transported. In such cases possibly relevant only to certain categories or quantities of *radioactive material* or to particularly sensitive transports, additional security measures should be applied."

- IAEA NSS No. 14, para. 4.36:

"When establishing security measures to protect against a *malicious act* particularly *sabotage,* the safety features of the design of the transport package, container and conveyance should be taken into account."

- IAEA NSS No. 14, para. 4.37:

"If the current or potential *threat* warrants additional security measures to protect against *sabotage*, consideration should be given to:

  - Postponing the shipment;
  - Rerouting the shipment to avoid high threat areas;
  - Enhancing the robustness of the package or the vehicle;
  - Enhancing route surveillance to observe the current environment;
  - Providing (additional) escorts or guards."

- IAEA NSS No. 14, para. 4.38:

"For international transport, *shippers* and/or carriers should ensure in advance that any State by State variations in security requirements are applied and should determine the point at which the responsibility for security is transferred."

5.15.3. Basis for suggestions

- See Appendix III.

5.15.4. Documentation

- Transport security plan of the shipper and/or carrier, including a description of the implemented detection, delay systems and components;
- Procedures of the shipper and/or carrier on the updating of the transport security plan;
- Procedures of the shipper and/or carrier on transport routing and scheduling;
- Procedures of the shipper and/or carrier on response measures including communication between response forces;
- Procedures of the shipper and/or carrier on detection and response;

- Procedures on shipper and/or carrier on the operation of the transport control centre;
- Organizational structure of the shipper and/or carrier;
- Procedures of the shipper and/or carrier on access control;
- Procedures of the shipper and/or carrier on trustworthiness checking;
- Procedures of the shipper and/or carrier on the management of sensitive information;
- Procedures of the shipper and/or carrier on communication with the relevant persons involved, including the consignor;
- Maintenance and testing plan of the shipper and/or carrier in relation to physical protection systems and components;
- Maintenance records of shipper and/or carrier in relation to physical protection systems and components;
- Records of the shipper and/or carrier on the testing of the effectiveness of the physical protection system;
- Qualification and training records of the shipper and/or carrier;
- Regular and occasional reports of the shipper and/or carrier on security management issues;
- International transport arrangements, if appropriate;
- Agreement between exporting and importing facilities, if appropriate;
- Written instructions for the transport crew members and/or escorts.

5.15.5. Data to be collected/specimen questions

Determine if and how:

- The applied transport security system takes into account the quantity and the physicochemical form of the radioactive material, the mode(s) of transport and the package(s) used.
- The applied transport security system, in implementing a graded approach, is based on the properties and quantities of the radioactive material being shipped.
- The transport security includes considering transport schedules, routing (including security of passage) and information security.
- The applied level of security measures (i.e. basic security measures, enhanced security measures or prudent management) includes security systems or other arrangements to deter, detect, delay and respond to malicious acts affecting the conveyance or its cargo.
- The security systems and other arrangements are operational and effective at all time.
- On the basic level of security measures:
    - Security measures applied during use and storage are applied during temporary storage transit sites.
    - Individuals engaged in the transport receive training, including training in the elements of security awareness.
    - Security measures are applied, verified prior to shipment and remain effective during transport.
    - Security measures (including response measures) are provided to crew members in writing.
    - Trustworthiness of persons engaged in the transport is verified.
    - Security related information is communicated to consignors and carriers engaged in the transport.
    - The consignee is informed by the consignor in advance of the shipment of the mode of transport and expected delivery time and the consignee confirms receipt of the radioactive material within the delivery time frame.

        - The movement of packages and/or conveyances is monitored.
        - Communication is available to ensure response or provide assistance to the crew.
        - Packages and/or conveyances are not left unattended for any longer than absolutely necessary.
- On the enhanced level of security measures (in addition to those listed at the basic level), consignors, carriers, consignees and other persons engaged in the transport develop, adopt, implement, periodically review and revise, as necessary, and comply with the provisions of a transport security plan. The transport security plan describes the overall nuclear security system in place and security management measures implemented (including measures addressing an increased threat level).
- Additional security measures are applied depending on the assessment of prevailing threat or the attractiveness of the material transported (i.e. postponing the shipment, rerouting the shipment, enhancing the robustness of the package or vehicle), enhancing route surveillance, providing additional escorts or guards).
- Security measures against a malicious act (particularly sabotage) take into account the design safety features of the transport package, container and conveyance.
- For international transport, shippers and/or carriers comply with the security requirements of the other concerned States.
- For international transport, shippers and/or carriers determine the point where the responsibility for security is transferred.

5.16. APPENDIX I: BASIS FOR SUGGESTIONS FOR SECURITY SYSTEM FROM IAEA NSS No. 11

- IAEA NSS No. 11, Section 4.1: Establish graded security levels with corresponding goals and objectives (sections extracted):

Each security level has a corresponding goal. The goal defines the overall result that the security system should be capable of providing for a given security level. The following goals have been developed:

- **Security level A**: *Prevent* unauthorized removal of a source.
- **Security level B**: *Minimize the likelihood* of unauthorized removal of a source.
- **Security level C**: *Reduce the likelihood* of unauthorized removal of a source.

TABLE 2. SECURITY LEVELS AND SECURITY OBJECTIVES

Security functions	**Security objectives**		
	Security level A *Goal: Prevent unauthorized removal**	**Security level B** *Goal: Minimize likelihood of unauthorized removal**	**Security level C** *Goal: Reduce likelihood of unauthorized removal**
Detect	Provide immediate detection of any unauthorized access to the secured area/source location		
	Provide immediate detection of any attempted unauthorized removal of the source, including by an insider	Provide detection of any attempted unauthorized removal of the source	Provide detection of unauthorized removal of the source
	Provide immediate assessment of detection		
	Provide immediate communication to response personnel		
	Provide a means to detect loss of source through verification		
Delay	Provide delay after detection sufficient for response personnel to interrupt the unauthorized removal	Provide delay to minimize the likelihood of unauthorized removal	Provide delay to reduce the likelihood of unauthorized removal

Response	Provide immediate response to assessed alarm with sufficient resources to interrupt and prevent the unauthorized removal	Provide immediate initiation of response to interrupt the unauthorized removal	Implement appropriate action in the event of unauthorized removal of a source
Security management	Provide access controls to source location that effectively restrict access to authorized persons only		
	Ensure trustworthiness of authorized individuals		
	Identify and protect sensitive information		
	Provide a security plan		
	Ensure a capability to manage security events covered by security contingency plan (see Definitions)		
	Establish security event reporting system		

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

- IAEA NSS No. 11, Section 4.2.2: Assigning security levels (sections extracted):

TABLE 5. RECOMMENDED DEFAULT SECURITY LEVELS FOR COMMONLY USED SOURCES

Category	**Source**	**A/D**	**Security level**
I	RTGs Irradiators Teletherapy sources Fixed multibeam teletherapy (gamma knife) sources	$A/D \geq 1000$	A
II	Industrial gamma radiography sources High/medium dose rate brachytherapy sources	$1000 > A/D \geq 10$	B
III	Fixed industrial gauges that incorporate high activity sources Well logging gauges	$10 > A/D \geq 1$	C

IV	Low dose rate brachytherapy (except eye plaques and permanent implants) Industrial gauges that do not incorporate high activity sources Bone densitometers Static eliminators	$1 > A/D \geq 0.01$	Apply measures as described in the International Basic Safety Standards
V	Low dose rate brachytherapy eye plaques and permanent implant sources XRF devices Electron capture devices Mossbauer spectrometry sources Positron emission tomography (PET) check sources	$0.01 > A/D$ and $A >$ exempt	

- IAEA NSS No. 11, Section 4.3.1: Introduction for security level A measures:

Detection

Security objective: Provide immediate detection of any unauthorized access to the secured area/source location.

Security measures: Electronic intrusion detection system and/or continuous surveillance by operator personnel.

Electronic sensors linked to an alarm or continuous visual surveillance by operator personnel indicate unauthorized access to the secured area (see the section on Delay below) or source location. Care should be taken to ensure that intrusion detection measures cannot be bypassed. For sources in use, such measures should detect unauthorized access to the secured area where the source is used. For sources in storage, such measures should detect unauthorized access to the locked room or other location where the source is stored. For mobile or portable sources in use, continuous visual surveillance may be the only feasible means of immediate intrusion detection.

Security objective: Provide immediate detection of any attempted unauthorized removal of the source (e.g. an insider).

Security measures: Electronic tamper detection equipment and/or continuous surveillance by operator personnel.

Electronic sensors linked to an alarm or continuous visual surveillance by operator personnel indicate attempted unauthorized removal of a source. Care should be taken to ensure that tamper detection measures cannot be bypassed. For mobile sources in use, continuous visual surveillance may be the only feasible means of detecting attempted unauthorized removal. Note, however, that if continuous surveillance is chosen as a security measure, continuous visual surveillance may require observation by at least *two* individuals at all times to protect against an insider scenario.

Security objective: Provide immediate assessment of detection.

Security measures: Remote monitoring of CCTV or assessment by operator/response personnel.

Once an intrusion detection or tamper detection alarm has been triggered, there should be an immediate assessment of the cause of the alarm. Assessment can be performed by operator personnel at the source location, through CCTV or by persons immediately deployed to investigate the cause of the alarm. For mobile or portable sources in use, or in other instances where intrusion detection or tamper detection is provided by continuous visual surveillance by operator personnel, assessment should be performed concurrently with detection by the operator personnel keeping the source under continuous visual surveillance.

Security objective: Provide immediate communication to response personnel.

Security measures: Rapid, dependable, diverse means of communication, such as phones, cellular phones, pagers and radios.

If the assessment confirms that unauthorized access or attempted unauthorized removal has occurred, immediate notification should be made to response personnel by operator personnel with diverse (at least two) means of communication such as landline telephones, auto-dialers, cellular phones, radios or paging devices.

Security objective: Provide a means to detect loss through verification.

Security measures: Daily checking through physical checks, CCTV, tamper indicating devices, etc.

Daily checking should consist of measures to ensure that the sources are present and have not been tampered with. Such measures could include physical checks that the source is in place, remote observation through CCTV, verification of seals or other tamper evident devices and measurements of radiation or other physical phenomena that would provide an assurance that the source is present. For sources in use, verifying that the device is functional may be sufficient.

Delay

Security objective: Provide delay after detection sufficient for response personnel to interrupt the unauthorized removal.

Security measures: System of least two layers of barriers (e.g. walls, cages) which together provide delay sufficient to enable response personnel to interdict.

A balanced system comprising at least two barriers should separate the source from unauthorized personnel and provide sufficient delay following detection to enable response personnel to intercede before the adversary can remove the source. For sources in use, such measures may include a locked device in a secured area to separate the device from unauthorized personnel. For sources in storage, such measures may include a locked and fixed container or a device holding the source in a locked storage room, thus separating the container from unauthorized personnel. For mobile sources in use, continuous visual surveillance by operator personnel may substitute for one or both layers of barriers.

Response

Security objective: Provide immediate response to assessed alarm with sufficient resources to interrupt and prevent the unauthorized removal.

Security measures: Capability for immediate response with size, equipment and training to interdict.

The operator should establish protocols to ensure immediate deployment of response personnel without delay in response to an alarm. The response should be both immediate and adequate. *Immediate* means that responders should arrive, once notified, in a time shorter than the time required to breach the barriers and perform the tasks needed to remove the source. *Adequate* means that the response team is of sufficient size and capability to subdue the adversary. Response may be a directly employed security force, a third party security team, local police, or national gendarmerie.

- IAEA NSS No. 11, Section 4.3.1: Introduction for security level B measures:

Detection

Security objective: Provide immediate detection of any unauthorized access to the secured area/source location.

Security measures: Electronic intrusion detection equipment and/or continuous surveillance by operator personnel.

Electronic sensors linked to an alarm or continuous visual surveillance by operator personnel indicate unauthorized access to the secured area (see section on 'Delay' below) or source location. Care should be taken to ensure that intrusion detection measures cannot be bypassed. For sources in use, such measures should detect unauthorized access to the secured area where the source is used. For sources in storage, such measures should detect unauthorized access to the locked room or other location where the source is stored. For mobile or portable sources in use, continuous visual surveillance may be the only feasible means of intrusion detection.

Security objective: Provide detection of any attempted unauthorized removal of the source.

Security measures: Tamper detection equipment and/or periodic checks by operator personnel.

Tamper detection equipment or visual surveillance by operator personnel made during periodic checks can indicate attempted unauthorized removal of a source. Care should be taken to ensure that tamper detection measures cannot be bypassed. This may be facilitated by the use of electronic tamper detection equipment. For mobile or portable sources in use, continuous visual surveillance may be the only feasible means of detecting attempted unauthorized removal.

Security objective: Provide immediate assessment of detection.

Security measures: Remote monitoring of CCTV or assessment by operator/response personnel.

Once an intrusion detection alarm has been triggered, there should be an immediate assessment of the cause of the alarm. Assessment can be performed by operator personnel at the source location, through CCTV or by persons immediately deployed to investigate the cause of the alarm. For mobile or portable sources in use, or in other instances where intrusion detection or tamper detection is provided by continuous visual surveillance by operator personnel, assessment should be performed concurrently with detection by the operator personnel keeping the source under continuous visual surveillance.

Security objective: Provide immediate communication to response personnel.

Security measures: Rapid, dependable means of communication, such as phones, cellular phones, pagers and radios.

If the assessment confirms that unauthorized access or attempted unauthorized removal has occurred, immediate notification should be made to response personnel by operator personnel with dependable

means of communication such as landline telephones, auto-dialers, cellular phones, radios or paging devices.

Security objective: Provide a means to detect loss through verification.

Security measures: Weekly checking through physical checks, tamper detection equipment, etc.

Weekly checking consists of measures to ensure that the sources are present and have not been tampered with. Such measures could include physical checks that the source is in place, verification of seals or other tamper evident devices, and measurements of radiation or other physical phenomena that would provide an assurance that the source is present. For sources in use, verifying that the device is functional may be sufficient.

Delay

Security objective: Provide delay to minimize the likelihood of unauthorized removal.

Security measures: System of two layers of barriers (e.g. walls, cages).

A balanced system of two barriers should separate the source from unauthorized personnel. For sources in use, such measures may include a locked device in a secured area, separating the device from unauthorized personnel. For sources in storage, such measures may include a locked and fixed container or a device holding the source and a locked storage room, separating the container from unauthorized personnel. For mobile or portable sources in use, continuous visual surveillance by operator personnel may substitute for barriers.

Response

Security objective: Provide immediate initiation of response to interrupt unauthorized removal.

Security measures: Equipment and procedures to initiate response immediately.

The operator should establish protocols to ensure immediate deployment of response personnel without delay, in response to an alarm, to interrupt the adversary's action. Response may be a directly employed security force, a third party security team, local police, or national gendarmerie. The response should be coordinated with local authorities to mitigate the potential consequences.

- IAEA NSS No. 11, Section 4.3.1: Introduction for security level C measures:

Detection

Security objective: Provide detection of unauthorized removal of the source.

Security measures: Tamper detection equipment and/or periodic checks by operator personnel.

Operators should verify that the sources are present. Measures could include physical checks that the source is in place, verification of seals or other tamper indicating devices and measurements of radiation or other physical phenomena that would provide an assurance that the source is present. For sources in use, verifying that the device is functional may be sufficient.

Security objective: Provide immediate assessment of detection.

Security measures: Assessment by operator or response personnel.

Once tamper detection or a physical check indicates a source may be missing, there should be an immediate assessment of the situation to determine whether an unauthorized removal has actually occurred.

Security objective: Provide a means to detect loss through verification.

Security measures: Monthly checking through physical checks, tamper indicating devices, etc.

Monthly checking consists of measures to ensure that the sources are present and have not been tampered with. Such measures could include physical checks that the source is in place, verification of seals or other tamper indicating devices and measurements of radiation or other physical phenomena that would provide an assurance that the source is present. For sources in use, verifying that the device is functional may be sufficient.

Delay

Security objective: Provide delay to reduce the likelihood of unauthorized removal of a source.

Security measures: One barrier (e.g. cage, source housing) or more under observation by operator personnel.

At least one physical barrier should separate the source from unauthorized personnel. For sources in use, such measures may include the source housing or use of the source in a secured area. For sources in storage, such measures may include a locked and fixed container, a device holding the source or a locked storage room to separate the container from unauthorized personnel. For mobile or portable sources in use, continuous visual surveillance by operator personnel may substitute for the barrier.

Response

Security objective: Implement appropriate action in the event of unauthorized removal of a source.

Security measures: Procedures for identifying necessary actions in accordance with contingency plans.

Regulatory procedures should ensure that any suspected unauthorized removal or loss of a source is assessed and, if confirmed, reported to the appropriate authority without delay. This should be followed by an effort to locate and recover the source and investigate the circumstances leading to the event.

- IAEA NSS No. 11, Section 4.2.3.4: Mobile, portable and remote sources:

Sources used in field applications (e.g. radiography and well logging) are typically contained in devices designed for portability and are frequently transported between job sites. The ease of handling these devices and their presence in vehicles outside secured facilities make them attractive targets for unauthorized removal.

Recognizing that security measures for fixed sources may not be practical for application to sources used in the field, alternative measures should be applied to achieve the security objective. Please refer to the detection and delay measures for security levels B and C (Section 4.3.1), as well as the illustrative security measures for mobile sources in Appendix IV.

Sources that are used in remote locations could be removed by unauthorized personnel and transported out of the area before effective response is possible.

The regulatory body may wish to consider mobility, portability and location when assigning a security level to a source or may wish to consider additional measures within the assigned security level to compensate for these conditions.

5.17. APPENDIX II: BASIS FOR SUGGESTIONS FOR SECURITY MANAGEMENT FROM IAEA NSS No. 11

- IAEA NSS No. 11, Section 3.2 Security culture (sections extracted):

Security culture may be enhanced by various means including, as appropriate:

- Assigning responsibility for the security of radioactive sources to a senior staff member, but ensuring that staff members are aware that security is a shared responsibility across the whole organization;
- Documenting legal and regulatory security responsibilities applying to the operator and bringing this to the attention of relevant managers, staff and, where appropriate, all employees and contractors;
- Ensuring threat awareness and training security managers, response personnel and all personnel with secondary responsibilities for security;
- Addressing security matters in staff and contractor induction courses;
- Providing security instructions and ongoing security awareness briefings to staff and contractors, and training and evaluation of the lessons learned;
- Conducting regular performance testing and preventive maintenance.

- IAEA NSS No. 11, Section 4.1: Establish graded security levels with corresponding goals and objectives (sections extracted):

Each security level has a corresponding goal. The goal defines the overall result that the security system should be capable of providing for a given security level. The following goals have been developed:

- **Security level A**: *Prevent* unauthorized removal of a source.
- **Security level B**: *Minimize the likelihood* of unauthorized removal of a source.
- **Security level C**: *Reduce the likelihood* of unauthorized removal of a source.

TABLE 2. SECURITY LEVELS AND SECURITY OBJECTIVES

Security functions	**Security objectives**		
	Security level A *Goal: Prevent unauthorized removal**	**Security level B** *Goal: Minimize likelihood of unauthorized removal**	**Security evel C** *Goal: Reduce likelihood of unauthorized removal**
Detect	Provide immediate detection of any unauthorized access to the secured area/source location		

	Provide immediate detection of any attempted unauthorized removal of the source, including by an insider	Provide detection of any attempted unauthorized removal of the source	Provide detection of unauthorized removal of the source
	Provide immediate assessment of detection		
	Provide immediate communication to response personnel		
	Provide a means to detect loss of source through verification		
Delay	Provide delay after detection sufficient for response personnel to interrupt the unauthorized removal	Provide delay to minimize the likelihood of unauthorized removal	Provide delay to reduce the likelihood of unauthorized removal
Response	Provide immediate response to assessed alarm with sufficient resources to interrupt and prevent the unauthorized removal	Provide immediate initiation of response to interrupt the unauthorized removal	Implement appropriate action in the event of unauthorized removal of a source
Security management	Provide access controls to source location that effectively restrict access to authorized persons only		
	Ensure trustworthiness of authorized individuals		
	Identify and protect sensitive information		
	Provide a security plan		
	Ensure a capability to manage security events covered by security contingency plan (see Definitions)		
	Establish security event reporting system		

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

- IAEA NSS No. 11, Section 4.2.2: Assigning security levels (sections extracted):

TABLE 5. RECOMMENDED DEFAULT SECURITY LEVELS FOR COMMONLY USED SOURCES

Category	Source	A/D	Security level
I	RTGs Irradiators Teletherapy sources Fixed multibeam teletherapy (gamma knife) sources	A/D $\geq$ 1000	A
II	Industrial gamma radiography sources High/medium dose rate brachytherapy sources	1000 > A/D $\geq$ 10	B
III	Fixed industrial gauges that incorporate high activity sources Well logging gauges	10 > A/D $\geq$ 1	C
IV	Low dose rate brachytherapy (except eye plaques and permanent implants) Industrial gauges that do not incorporate high activity sources Bone densitometers Static eliminators	1 > A/D $\geq$ 0.01	Apply measures as described in the International Basic Safety Standards
V	Low dose rate brachytherapy eye plaques and permanent implant sources XRF devices Electron capture devices Mossbauer spectrometry sources Positron emission tomography (PET) check sources	0.01 > A/D and A > exempt	

- IAEA NSS No. 11, Section 4.3.1: Introduction for security level A measures:

Security objective: Provide access controls to source location that effectively restrict access to authorized persons only.

Security measures: Identification and verification, for example, lock controlled by swipe card reader and personal identification number, or key and key control.

Access control is intended to limit access to the source location to authorized persons, generally by allowing such persons to disable temporarily physical barriers such as a locked door (delay measures) upon verification of the person's identity and access authorization. (In the context of medical exposure,

patients do not need to be 'authorized' since they are escorted to the source and are under constant surveillance by the medical staff.)

The identity and authorization of a person seeking access can be verified by such measures as:

- Personal identification number (PIN) to activate a door control reader;
- A badge system which may also activate an electronic reader;
- A badge exchange scheme at an entry control point;
- Biometric features to activate a door control device.

Upon verification of a person's access authorization, the system allows that person to enter the secured area or source location, e.g. by opening a lock. A combination of two or more verification measures should be required, e.g. the use of a swipe card and a PIN; or the use of a swipe card and a controlled key; or a PIN and a computer password; or the use of a controlled key and visual verification of identity by other authorized personnel. For sources in use, such measures should control access to the area where the source is used. For sources in storage, such measures should control access to the locked room or other location where the source is stored. For mobile sources in use, continuous visual surveillance by multiple operator personnel may substitute for access control.

Security objective: Ensure trustworthiness of authorized individuals.

Security measures: Background checks for all personnel authorized for unescorted access to the source location and for access to sensitive information.

An individual's trustworthiness should be assessed through a satisfactory background check before that person is allowed unescorted access to radioactive sources, locations where they are used or stored or any sensitive, related information. The nature and depth of background checks should be in proportion to the security level of the radioactive source and in accordance with the State's regulations or as determined by the regulatory body. As a minimum, background checks should involve confirmation of identity and the verification of references to determine the integrity, character and reliability of each person. The process should be periodically reviewed and supported through ongoing attention by supervisors and managers to ensure that personnel at all levels continue to act responsibly and reliably and any concerns, in this context, are made known to the relevant authority.

Security objective: Identify and protect sensitive information.

Security measures: Procedures to identify sensitive information and protect it from unauthorized disclosure.

As well as providing security for radioactive sources, it is necessary to protect related information, which may include documents, data on computer systems and other media that can be used to identify details of:

- The specific location and inventory of sources;
- The relevant security plan and detailed security arrangements;
- Security systems (e.g. intruder alarms), including performance and installation diagrams;
- Temporary or longer term weaknesses in the security programme;
- Security staffing arrangements and the means of response to events or alarms;
- Planned dates, routes and mode of shipment or transfer of sources;
- Contingency plans and security response measures.

Regulatory guidance should also provide for:

- Control, storage, preparation, identification, marking and transmission of documents or correspondence containing the sensitive information;
- Recommended methods for the destruction of documents containing sensitive information;
- Arrangements covering the declassification and management of documents when they are obsolete or no longer sensitive.

Security objective: Provide a security plan.

Security measures: A security plan which conforms to regulatory requirements and provides for response to increased threat levels.

A security plan should be prepared for each facility by its operator. For examples of content of a security plan, see Appendix II. Security plans may be authorized by the regulatory body and reviewed at prescribed intervals during the inspection process to ensure that they reflect the current security system. Security plans may be different for mobile and portable use sources, or for sources stored between periods of use. Most plans are likely to contain sensitive information about protective security arrangements and should therefore be managed accordingly. The security plan should also allow for an efficient and prompt transition to an enhanced level of security, in the case of an increase in the security threat.

Security objective: Ensure a capability to manage security events covered by security contingency plans.

Security measures: Procedures for responding to security related scenarios.

At each facility, security contingency plans should be drawn up for a range of events, including:

- A suspected or threatened malicious act.
- A public demonstration which has the potential to threaten the security of sources.
- An intrusion into the secured area by unauthorized person(s). This could range from simple trespass to a determined attack by those seeking to remove or interfere with radioactive sources.

The operator should develop reasonably foreseeable scenarios involving such events and procedures for responding to them. Security contingency plans should be shared with appropriate authorities and exercised at regular intervals.

Security objective: Establish security event reporting system.

Security measures: Procedures for timely reporting of security events.

The operator should develop procedures for reporting security events to the regulatory body, first responders, and others as appropriate within a time frame required by the regulatory body, commensurate with the security significance of the event. Events to be reported may include:

- Discrepancy in accounting data;
- Suspected or actual theft of a radioactive source;
- Unauthorized intrusion into a facility or source storage area;
- The discovery of a suspected or actual explosive device in or near a facility or store;
- Loss of control over a radioactive source;
- Unauthorized access to, or unauthorized use of, a source;
- Other malicious acts that threaten authorized activities;
- Suspicious events or sightings which might indicate planning for a sabotage attack, an intrusion or removal of a source;
- Failure or loss of security systems that are essential to the protection of radioactive sources.

- IAEA NSS No. 11, Section 4.3.1: Introduction for security level B measures:

Security objective: Provide access controls to source location that effectively restrict access to authorized persons only.

Security measures: One identification measure.

The purpose of access control is to limit access to the source location to authorized persons, generally by allowing such persons to disable temporarily physical barriers such as locked doors (delay measures) upon verification of the person's identity and access authorization (in the context of medical exposure, patients do not need to be 'authorized').

The identity and authorization of a person seeking access can be verified by such measures as:

- A PIN to activate a door control reader;
- A badge system which may also activate an electronic reader;
- A badge exchange scheme at an entry control point;
- Biometric features to activate a door control device.

Upon verification of a person's access authorization, the system would allow that person to enter the secured area or source location, e.g. by opening a lock. At least one identification measure should be required, e.g. the use of a swipe card, PIN, computer password, controlled key or visual verification of identity by other authorized personnel. For sources in use, such measures should control access to the area where the source is used. For sources in storage, such measures should control access to the locked room or other location where the source is stored. For mobile or portable sources in use, continuous visual surveillance by operator personnel may substitute for access control.

Security objective: Ensure trustworthiness of authorized individuals.

Security measures: Background checks for all personnel authorized for unescorted access to the source location and for access to sensitive information.

An individual's trustworthiness should be assessed through a satisfactory background check before that person is allowed unescorted access to radioactive sources, locations where they are used or stored, or any sensitive, related information. The nature and depth of background checks should be in proportion to the security level of the radioactive source and in accordance with the State's national regulations or as determined by the regulatory body. As a minimum, background checks should involve confirmation of identity and the verification of references to determine the integrity, character and reliability of each person. The process should be periodically reviewed and supported through ongoing attention by supervisors and managers to ensure that personnel at all levels continue to act responsibly and reliably and any concerns, in this context, are made known to the relevant authority.

Security objective: Identify and protect sensitive information.

Security measures: Procedures to identify sensitive information and protect it from unauthorized disclosure.

As well as providing security of radioactive sources, the security system should protect related information, which may include documents, data on computer systems and other media that can be used to identify details of:

- The specific location and inventory of sources;
- The relevant security plan and detailed security arrangements;

- Security systems (e.g. intruder alarms), including performance and installation diagrams;
- Temporary or longer term weaknesses in the security programme;
- Security staffing arrangements and the means of response to events or alarms;
- Planned dates, routes and mode of shipment or transfer of sources;
- Contingency plans and security response measures.

Regulatory guidance should also provide for:

- Control, storage, preparation, identification, marking and transmission of documents or correspondence containing the sensitive information;
- Recommended methods for the destruction of documents containing sensitive information;
- Arrangements covering the declassification and management of documents when they are obsolete or no longer sensitive.

Security objective: Provide a security plan.

Security measures: A security plan which conforms to regulatory requirements and provides for response to increased threat levels.

A security plan should be prepared for each facility by its operator. For examples of content of a security plan, see Appendix II. Security plans may be approved by the regulatory body and reviewed at prescribed intervals during the inspection process to ensure that they reflect the current security system. Security plans may be different for mobile and portable use sources, or for sources stored during periods of use. Most plans are likely to contain sensitive information about protective security arrangements and should therefore be managed accordingly. The security plan should also allow for an efficient and prompt transition to an enhanced level of security, in the case of an increase in the security threat.

Security objective: Ensure a capability to manage security events covered by security contingency plans.

Security measures: Procedures for responding to security related scenarios.

At each facility, contingency plans should be drawn up for a range of events, including:

- A suspected or threatened malicious act.
- A public demonstration which has the potential to threaten the security of sources.
- An intrusion into the secured area by unauthorized person(s). This could range from simple trespass to a determined attack by those seeking to remove or interfere with radioactive sources.

The operator should develop reasonably foreseeable scenarios involving such events and procedures for responding to them. Contingency plans should be shared with appropriate authorities and exercised at regular intervals.

Security objective: Establish security event reporting system.

Security measures: Procedures for timely reporting of security events.

The operator should develop procedures for reporting security events to the regulatory body, first responders, and others, as appropriate, within a time frame required by the regulatory body, commensurate with the security significance of the event. Events to be reported may include:

- Discrepancy in accounting data;
- Suspected or actual theft of a radioactive source;
- Unauthorized intrusion into a facility or source storage area;

- The discovery of a suspected or actual explosive device in or near a facility or store;
- Loss of control over a radioactive source;
- Unauthorized access to, or unauthorized use of, a source;
- Other malicious acts that threaten authorized activities;
- Suspicious events or sightings which might indicate planning for a sabotage attack, an intrusion or removal of a source;
- Failure or loss of security systems essential for the protection of radioactive sources.

- IAEA NSS No. 11, Section 4.3.1: Introduction for security level C measures:

Security objective: Provide access controls to source location that effectively restrict access to authorized persons only.

Security measures: One identification measure.

Access control is intended to limit access to the source location to authorized persons, generally by allowing such persons to disable temporarily physical barriers such as locked doors (delay measures) upon verification of the person's identity and access authorization. (In the context of medical exposure, patients do not need to be 'authorized'.)

The identity and authorization of a person seeking access can be verified by such measures as:

- A PIN to activate a door control reader;
- A badge system which may also activate an electronic reader;
- A badge exchange scheme at an entry control point;
- Biometric features to activate a door control device.

Upon verification of a person's access authorization, the system would allow that person to enter the secured area or source location, e.g. by opening a lock. At least one identification measure should be required, e.g. the use of a swipe card, PIN, computer password, controlled key or visual verification of identity by other authorized personnel. For sources in use, such measures should control access to the area where the source is used. For sources in storage, such measures should control access to the locked room or other location where the source is stored. For mobile or portable sources in use, continuous visual surveillance by operator personnel may substitute for access control.

Security objective: Ensure trustworthiness of authorized individuals.

Security measures: Appropriate methods for determining the trustworthiness of authorized individuals with unescorted access to radioactive sources and access to sensitive information.

An individual's trustworthiness should be assessed through a satisfactory background check before that person is allowed unescorted access to radioactive sources, locations where they are used or stored, or any sensitive, related information. The nature and depth of background checks should be in proportion to the security level of the source and in accordance with the State's national standards or as determined by the regulatory body.

Security objective: Identify and protect sensitive information.

Security measures: Procedures to identify sensitive information and protect it from unauthorized disclosure.

Regulatory provisions should ensure that the operator assesses whether those individuals with access to security information or radioactive sources are reliable. Unless determined as being trustworthy, they should not be granted unescorted access.

Security objective: Provide a security plan.

Security measures: Documentation of security arrangements and reference procedures.

Security arrangements and reference procedures should be adopted in the form of a security plan. For examples of the content of a security plan, see Appendix II.

Security objective: Ensure a capability to manage security events covered by security contingency plans.

Security measures: Procedures for responding to security related scenarios.

The security statement should include procedures for investigating and reporting any unauthorized access to, or removal of, a source.

Security objective: Establish a security event reporting system.

Security measures: Procedures for timely reporting of security events.

The operator should develop procedures for reporting of security events to the regulatory body, first responders, and others as appropriate within a time frame required by the regulatory body commensurate with the security significance of the event. Events to be reported may include:

- Discrepancy in accounting data;
- Suspected or actual theft of a radioactive source;
- Unauthorized intrusion into a facility or source storage area;
- Discovery of a suspected or actual explosive device in or near a facility or store;
- Loss of control over a radioactive source;
- Unauthorized access to, or unauthorized use of, a source;
- Other malicious acts that threaten authorized activities;
- Suspicious events or sightings which might indicate planning for a sabotage attack, an intrusion or removal of a source;
- Failure or loss of security systems that are essential to the protection of radioactive sources.

5.18. APPENDIX III: BASIS FOR SUGGESTIONS FOR TRANSPORT FROM IAEA NSS No. 9

- IAEA NSS No. 9, Section 4.1: Prudent management practices (paraphrased):

- Prudent management practices are basic control measures included in IAEA Safety Series No. 115, International Basic Safety Standards for Protection against Ionizing Radiation and for the Safety of Radiation Sources,IAEA NSS No. 9, Section 4.2: Basic security level (sections extracted):

All operators (consignors, carriers, consignees) and other persons engaged in the transport of radioactive material should apply security measures for the transport of radioactive material commensurate with their responsibilities and the level of threat.

Radioactive material should be transferred only to authorized operators. In normal circumstances, it is sufficient that there is an existing business relationship between a carrier and consignee/consignor. Where such a relationship does not already exist, a potential carrier's or consignee's suitability or capability to receive or transport radioactive material should be established by confirmation with relevant national regulatory authorities, or trade and industry associations, that the carrier's or consignee's interests are legitimate.

The operator should have procedures in place that would initiate an inquiry about the status of packages that are not delivered to the intended recipient at the expected time. Through the course of the inquiry, if it is determined that the package has been lost or stolen or if it appears to have been tampered with, procedures should immediately be initiated to locate and recover the package.

Unless there are overriding safety or operational considerations, packages of radioactive material should be carried in secure and closed or sheeted conveyances. However, such packages individually weighing more than 2000 kg that are sealed and secured to the conveyances may be transported on an open conveyance. The integrity of locks and seals should be verified before dispatch and on arrival by staff who are specifically and previously authorized by their employer to undertake this verification.

In the event that packages need to be transported on open conveyances, it may be necessary for the State to consider — in view of the nature of the radioactive material or prevailing threat — whether additional security measures should be applied. Such measures may include providing guards, shielding the package to provide for external pre-detonation to prevent or mitigate damage to the package in the event of a stand-off attack using rocket propelled armour piercing weapons or similar devices that are not easily defended against, and enhancing route surveillance or response capability. Packages should be shielded on the basis of advice from safety specialists.

Security awareness training should address the nature of security related threats, with due recognition of security concerns, methods to address such concerns and actions to be undertaken in the event of a security incident. It should include awareness of security plans (as appropriate) commensurate with the responsibilities of individuals and their part in implementing security plans.

Records of all security training undertaken should be kept by the employer and should be made available to the employee if requested.

Each crew member of any conveyance transporting radioactive material should carry means of positive identification during transport (an officially issued photographic identification or biometric record that uniquely identifies the individual).

In normal circumstances, and as appropriate to the mode of transport, it will be sufficient for the carrier of the conveyance to carry out a visual inspection to ensure that nothing has been tampered with or that nothing has been affixed to the package or conveyance that might compromise the security of the consignment.

At the basic security level, it is generally sufficient for these written instructions to contain no more than basic details of emergency contacts.

Operators should cooperate with each other and with the appropriate authorities to exchange information on applying security measures and responding to security incidents, where the exchange of information does not conflict with requirements for security in respect of sensitive information.

- IAEA NSS No. 9, Section 4.3: Enhanced security level (sections extracted):

In implementing national security provisions for shipments of radioactive material, the competent authority should establish a programme for identifying consignors or carriers engaged in the transport of radioactive material packages requiring the enhanced security level, for the purpose of communicating security related information.

The consignor, if requested or required, should provide advance shipment notification to the competent authority of any receiving or transit State.

When appropriate, tracking methods or devices may be used to monitor the movement of conveyances containing radioactive material. A simple tracking system will be able to track when a shipment has departed, whether the mode of transport has changed and if the material has been placed in interim storage or the consignment has been received. This information about status changes should be readily available to the appropriate parties (i.e. carriers, shippers and other operators). This tracking system may be as simple as a bar code system that provides information on the package location and status. The tracking system, in conjunction with a communications system and response procedures, will allow the operator and the competent authority to react in a timely manner to a malicious act, including theft of radioactive material.

- IAEA NSS No. 9, Section 4.4: Additional security measures (sections extracted):

Additional training, beyond basic security awareness, may be provided to persons engaged in the transport of radioactive material to ensure that they have the proper skills and knowledge for implementing specific security measures associated with their responsibilities.

Automated and real time tracking methods or devices may be required, where feasible, to permit a transport control centre to monitor remotely the movement of radioactive material conveyances and packages and the status of the material.

Persons engaged in the transport of radioactive material may be subject to formal national security clearance commensurate with their responsibilities.

Guards may be required to accompany certain transports to provide for continuous effective surveillance of the package and/or conveyance. In such cases, it will be important to ensure that guards are adequately trained (especially if they are armed), suitably equipped and fully aware of their responsibilities.

Prior to loading and shipment, appropriately trained personnel may be required to conduct a thorough search of the conveyance to ensure that it has not been tampered with in any way that could compromise security.

Appropriate exercises may be carried out in advance of a transport of radioactive material to ensure that contingency plans are adequately robust.

5.19. REFERENCES

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

[2] INTERNATIONAL ATOMIC ENERGY AGENCY, Guidance on the Import and Export of Radioactive Sources, IAEA, Vienna (2012).

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

[4] INTERNATIONAL ATOMIC ENERGY AGENCY, Security of Radioactive Sources,

IAEA Nuclear Security Series No. 11, IAEA, Vienna (2009).

[5] INTERNATIONAL ATOMIC ENERGY AGENCY, Security in the Transport of Radioactive Material, IAEA Nuclear Security Series No. 9, IAEA, Vienna (2008).

[6] UNITED NATIONS, Model Regulations on the Transport of Dangerous Goods, UN, New York (2013).

[7] INTERNATIONAL ATOMIC ENERGY AGENCY, Categorization of Radioactive Sources, IAEA Safety Standards Series No. RS-G-1.9, IAEA, Vienna (2005).

[8] INTERNATIONAL ATOMIC ENERGY AGENCY, Dangerous Quantities of Radioactive Material (EPR-D-values), IAEA, Vienna (2006).

[9] INTERNATIONAL ATOMIC ENERGY AGENCY, Governmental, Legal and Regulatory Framework for Safety, IAEA Safety Standards Series No. GSR Part 1, IAEA, Vienna (2010).

[10] 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).

[11] INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Recommendations on Nuclear and Other Radioactive Material out of Regulatory Control, IAEA Nuclear Security Series No. 15, IAEA, Vienna (2011).

6. COMPUTER SECURITY REVIEW (MODULE 5)

6.1. INTRODUCTION

The focus of this module is on computer systems related to physical protection and the creation, processing and storage of nuclear sensitive information. Computer based systems are used extensively in physical protection, nuclear safety, and nuclear material accountancy and control systems at nuclear facilities. These systems not only store and provide access to confidential information and communications, but also provide a wide range of control and monitoring functions. The loss or compromise of these systems could have a serious impact on nuclear security, nuclear safety and operations. These systems therefore should be protected against compromise.

Computer security is a component of the plant's overall nuclear security programme. The focus of computer security is prevention of, detection of, and response to malicious acts involving computer systems. Computer system attack objectives may include:

- Information gathering attacks potentially supporting the planning and execution of further malicious acts;
- Attacks disabling or compromising the attributes of one or several computers crucial to facility security or safety;
- Compromise of one or several computers combined with other concurrent modes of attack, such as physical intrusion.

Computer technologies and the associated threats are dynamic and rapidly changing. Continual self-evaluation and assessment is needed to ensure a robust computer security posture. IAEA NSS No. 17, Computer Security at Nuclear Facilities, is a primary reference for this IPPAS Guidelines module. IAEA NSS No. 17, Computer Security at Nuclear Facilities, provides guidance for conducting a comprehensive or tailored computer security assessment. This publication provides tailored guidance within the context of an IPPAS mission.

6.2. PURPOSE

The primary purpose of this module is to provide guidelines for IPPAS team members in the conduct of a computer security assessment component of a mission.

This module is also designed to provide, upon request, advice to Member States and to assist them in strengthening the effectiveness of the computer security aspects of their physical protection regimes in nuclear facilities, while recognizing that the ultimate responsibility for nuclear security is that of the State.

This module compares, to the extent feasible, the procedures and practices in a Member State's facility with accepted international guidance. This appraisal consists of a modular functional level review of the measures and procedures in place to evaluate the computer security regime with respect to physical protection. It is not intended to be a comprehensive review of the facility's computer security.

The mission report makes recommendations and/or suggestions that could contribute to improving the reviewed system. Commendable good practices are identified and may be communicated to other Member States for long term improvement.

6.3. SCOPE

The IPPAS mission may review the computer security aspects of the physical protection regime for all modes of operation or at the direction of the host country and may be tailored to concentrate on particular aspects. A computer security review may address the following areas as pertaining to physical protection:

- Computer security review: State level.
- Computer security review: Facility level:

    - Cross-cutting areas for computer security review:

(a) Risk management;
(b) Graded approach;
(c) Security culture;
(d) Human resource management.

    - Focused areas for computer security review:
        (a) Computer security policy;
        (b) Computer security management;
        (c) Computer asset management;
        (d) Physical protection and environmental security;
        (e) Computer operations management;
        (f) Computer access controls;
        (g) Computer systems acquisition, development and maintenance;
        (h) Detection of computer security events;
        (i) Computer security incident management;
        (j) Continuity management.

6.4. COMPUTER SECURITY REVIEW: STATE LEVEL

The State has the ultimate responsibility for establishing the requirements for confidentiality and the protection of information and computing systems related to physical protection, nuclear safety, and nuclear material accountancy and control. This includes information stored on electronic media and computing systems. Likewise the State maintains sensitive information related to the security, storage, and management of nuclear and radiological materials that requires protection. Finally the State via a competent authority establishes the regulatory and oversight framework for maintaining the security of nuclear and radiological facilities.

This section addresses the computer and information security regimes established at the State level that pertain to the physical protection of nuclear material and nuclear facilities.

6.4.1. Objectives of review

- To evaluate the information and computer security programmes established and managed at the State level.

6.4.2. Basis for recommendations/suggestions

- CPPNM Amendment, Fundamental Principle L: Confidentiality:

"The State should establish requirements for protecting the confidentiality of information, the unauthorized disclosure of which could compromise the physical protection of nuclear material and nuclear facilities."

- CPPNM Amendment, Fundamental Principle H: Graded Approach:

"Physical protection requirements should be based on a graded approach, taking into account the current evaluation of the threat, the relative attractiveness, the nature of the material and potential consequences associated with the unauthorized removal of nuclear material and with the sabotage against nuclear facilities or nuclear material."

- INFCIRC/225/Rev.5, para. 3.54:

"Management of a *physical protection system* should limit access to sensitive information to those whose trustworthiness has been established appropriate to the sensitivity of the information and who need to know it for the performance of their duties. Information addressing possible vulnerabilities in *physical protection systems* should be highly protected."

- INFCIRC/225/Rev.5, paras 4.10 and 5.19:

"Computer based systems used for physical protection, nuclear safety, and nuclear material accountancy and control should be protected against compromise (e.g. cyber attack, manipulation or falsification) consistent with the *threat assessment* or *design basis threat*."

6.4.3. Documentation and records of interest

- State level information protection and computer security policy/plan;
- Information protection/computer security legislation related to nuclear facilities;
- Record of computer security audits conducted at nuclear facilities;
- Record of security policy review and updates;
- Records of participation in international and national computer security exercises;
- National regulations and guides related to computer security;
- Policy and procedure for sensitive information classification, including computer storage and computer classification.

6.4.4. Data to be collected/specimen questions

- Determine if the State has established policy and legislation for protecting the confidentiality of information, the unauthorized disclosure of which could compromise the physical protection of nuclear/radiological material, and nuclear and radiological facilities.

- Determine if the State has developed and implemented a comprehensive national strategy addressing computer security for critical infrastructure components and key resources which includes nuclear facilities/radiological facilities and associated assets?

Describe the State's national threat assessment programme. Does it specifically identify threats relevant to the State's nuclear programme and industry, including cyber security threats?

- Does the State use a DBT? Does the DBT include a cyber threat component? Does a separate DBT exist for cyber threats? Describe how the cyber security threats are accounted for in the State's threat assessment.
- How is threat assessment information communicated to relevant organisations (e.g. regulators, facilities)?
- Determine if the State has established a national classification system that encompasses computer based systems related to nuclear security.
- How is the national classification system applied to the protection of computer based systems for nuclear/other radiological materials?
- Does the competent authority (i.e. regulatory body) set requirements for a computer security programme at regulated entities? Do such requirements include physical protection systems?
- Does the competent authority itself have an internal comprehensive computer security programme?
- Describe the State's incident response plans and response teams directed to address cyber intrusion/attacks against physical protection assets at nuclear facilities and related activities (i.e. transport). What is the composition, training and qualification of the response team?
- Describe how cyber attacks against physical protection assets at nuclear facilities and related activities (i.e. transport) are reported.
- What national level resources are designated to provide assistance during a computer incident that impacts physical protection at a nuclear/radiological facility or other regulated entity?
- Does the State conduct exercises to verify the appropriateness of computer security policy and procedures and communications procedures?
- Describe the level of training and qualification that regulatory inspectors have in conducting computer security inspections at nuclear/radiological facilities and other regulated entities. Are such inspections integrated with an inspection of physical protection assets?
- What is the inspection regime for periodic computer security inspections at facilities and other regulated entities?

6.5. COMPUTER SECURITY REVIEW: FACILITY LEVEL

This section provides details for evaluating specific areas of a computer security programme at a nuclear or other radiological facility, associated facility or other regulated entity as related to physical protection. In conducting this review, the reviewer may consider these questions across the spectrum of computing systems used to support physical protection systems. Specific systems of concern include:

- Perimeter monitoring/intrusion detection/surveillance/alarm assessment systems;

- Site access/physical access control systems;
- Accountancy and inventory control systems related to physical protection;
- Nuclear material accountancy and control systems;
- Voice and data communication infrastructure used in physical protection;
- Alarm and support systems/subsystems for the central alarm system;
- Security clearance and badging systems database;
- Training records associated with the physical protection guards and response forces.

These systems are contained within the physical protection domain, as specified in IAEA NSS 17 (Computer Security at Nuclear Facilities).

Each of the following sections is organized with an objective, a set of recommended documents for review consideration, and data to be collected. This listing of data is not meant to be an exhaustive list, but is meant to guide the assessor into important areas for discussion and subsequent evaluation.

6.5.1. Objective of review

- To determine if sensitive information and computer based systems important for nuclear security, nuclear safety, and nuclear material accountancy are identified and protected against malicious attack/compromise.

6.5.2. Basis for recommendations/suggestions

The basis for the development of the information and computer security regimes is derived from the recommendations listed below. The references are applied through all sections. Specific questions and information collection tasks are derived from IAEA technical guides, international computer security standards, and industry best practices.

- CPPNM, Art. 6:

"States Parties shall take appropriate measures consistent with their national law to protect the confidentiality of any information which they receive in confidence by virtue of the provisions of this Convention from another State Party or through participation in an activity carried out for the implementation of this Convention."

- CPPNM Amendment, Fundamental Principle L: Confidentiality:

"The State should establish requirements for protecting the confidentiality of information, the unauthorized disclosure of which could compromise the physical protection of nuclear material and nuclear facilities."

- CPPNM Amendment, Fundamental Principle H: Graded Approach:

"Physical protection requirements should be based on a graded approach, taking into account the current evaluation of the threat, the relative attractiveness, the nature of the material and potential consequences associated with the unauthorized removal of nuclear material and with the sabotage against nuclear facilities or nuclear material."

- INFCIRC/225/Rev.5, para. 3.54:

"Management of a *physical protection system* should limit access to sensitive information to those whose trustworthiness has been established appropriate to the sensitivity of the information and who need to know it for the performance of their duties. Information addressing possible vulnerabilities in *physical protection systems* should be highly protected."

- INFCIRC/225/Rev.5, para. 3.57:

"*Operator*s, *shippers* and carriers should establish sustainability programmes for their *physical protection system*. Sustainability programmes should encompass:

- Operating procedures (instructions).
- Human resource management and training.
- Equipment updating, maintenance, repair, and calibration.
- *Performance testing* and operational monitoring.
- Configuration management (The process of identifying and documenting the characteristics of a facility's *physical protection system* — including computer systems and software — and of ensuring that changes to these characteristics are properly developed, assessed, approved, issued, implemented, verified, recorded and incorporated into the facility documentation).
- Resource allocation and operational cost analysis."

- INFCIRC/225/Rev.5, paras 4.10 and 5.19:

"Computer based systems used for physical protection, nuclear safety, and nuclear material accountancy and control should be protected against compromise (e.g. cyber attack, manipulation or falsification) consistent with the *threat assessment* or *design basis threat*."

- INFCIRC/225/Rev.5, para. 6.7:

"Appropriate measures, consistent with national requirements and using a *graded approach*, should be taken to protect the confidentiality of information relating to *transport* operations, based on a need to know, including detailed information on the schedule and route. Great restraint should be applied in the use of any special markings on *conveyances*, and also in the use of open channels for transmission of messages concerning shipments of *nuclear material*. When a security relate message is transmitted, measures such as coding and appropriate routing should be taken to the extent practicable, and care should be exercised in the handling of such information."

- IAEA NSS No. 14, para. 4.19:

"*Operators* should be required to limit access to security sensitive information to those people who need that information in order to perform their jobs. Key elements of information protection include identifying the information that must be protected; designating individuals with authorized access to such information; and protecting such information from disclosure to individuals who do not have this access."

- IAEA NSS No. 14, para. 4.21:

"The security plan should include:

- A description of the *radioactive material* and the environment for its use and storage;
- A description of the specific security concerns to be addressed;
- A description of the security system implemented and its objectives;
- Security procedures to provide guidance to *operator* personnel for operating and maintaining security measures, and the security procedures to be followed before and after maintenance;
- Administrative aspects, including defining the roles and responsibilities of individuals with security responsibilities, access authorization processes, trustworthiness determination processes, information protection processes, inventories and records, event reporting, and review and revision of the security plan (including maximum time between reviews);
- How procedural and administrative security measures will be scaled to meet increased levels of *threat* as assessed by the State;
- Response actions including cooperation with relevant *competent authorities* in the location and recovery of *radioactive material* consistent with national practice."

- IAEA NSS No. 14, para. 4.32:

"The achievement of effective transport security should include considering transport schedules, routing including security of passage, and information security."

- IAEA NSS No. 14, para. 4.34:

"Enhanced security measures should include requiring that consignors, carriers, consignees and other persons engaged in the transport of radioactive material should develop, adopt, implement, periodically review as necessary and comply with the provisions of a transport security plan. Responsibility for and ownership of the transport security plan should be clearly defined. The plan should describe the overall nuclear security system in place to protect the radioactive material in transport and should include measures to address an increased threat level, response to nuclear security events and the protection of sensitive information."

6.5.3. Cross-cutting areas for review

Computer security related to nuclear security cross-cuts many activities in an organization. The following areas of computer security may be integrated across other review areas in the IPPAS mission and should be considered by all IPPAS assessors.

6.5.3.1. Risk management

Risk assessments assist a facility in determining the appropriate priorities and actions for managing information and computer security risks, including the identification and section of controls to manage these risks.

(a) Objective of review

- To assess risk management as applied to computer systems supporting physical protection.

(b) Documentation and records of interest

- Computer security risk assessment management plan.

(c) Data to be collected/specimen questions

- Does the organization have a mature risk management process in place that addresses threats, vulnerabilities and potential consequences?
- How does the organization receive/analyse threat data?
- How are cyber threats integrated into the risk analysis?
- How is the risk analysis implemented for computer systems supporting physical protection systems?
- What standards, references and methodologies are used?
- What is the scope of the risk analysis (e.g. organization, part of organization, system)?
- How is risk analysis performed, documented and used in conjunction with baseline security controls?
- Are residual risks identified, documented and accepted by the management? Are there specific incident handling procedures related to those residual risks?
- How often is a risk analysis conducted? Reviewed?
- What reliance do the physical protection system and measures have on computer and/or networking systems?
- Is a vulnerability assessment conducted?
- Does the vulnerability assessment include all access paths and persons having access?

6.5.3.2. Graded approach

The graded approach describes the application of security control measures proportional to the consequence of a malicious act.

(a) Objective of review

- To evaluate how the graded approach is applied to computer equipment supporting physical protection.

(b) Documentation and records of interest

- Risk assessment programme plan;
- Computer security management plan.

(c) Data to be collected/specimen questions

- How is the computer security zone concept applied?
- How are levels of protection assigned?

- What protection measures are prescribed or recommend for each level?
- Describe the defence in depth measures applied to computer physical protection assets.
- How do risk assessments influence the graded approach?
- Does the graded approach address all items identified during the risk assessment?

6.5.3.3. Security culture

Security responsibilities should be addressed prior and during employment in job descriptions and in the terms and conditions of employment.

(a) Objective of review

- To ensure that employees, contractors and third party users understand their roles and responsibilities related to security.

(b) Documentation and records of interest

- Computer security policy statement;
- Computer security awareness programme;
- Record of computer security awareness activities.

(c) Data to be collected

- How is computer security integrated into the security culture programme?
- How often do personnel receive computer security awareness training?
- How is the computer security culture assessed for effectiveness?
- What is the company policy on social media use?

6.5.3.4. Human resource management

(a) Objective of review

- To determine how the personnel security system and measures are applied to information protection and computer security.

(b) Documentation and records of interest

- Policy and procedure regarding computer use and security for employees, contractors and subcontractors.
- Records reflecting personnel computer use and security.
- What measures are taken to control the consistency between computer privileges and employee status (i.e. access rights management according to role)?
- What is the policy and procedure for personnel training (e.g. orientation, by function, refresher). Qualification, certification and training records and job placement requirements for computer security team individuals. What are the qualification, certification and training requirements in computer security for those responsible for maintaining computer systems supporting physical protection, including subcontractors?

- National laws/regulations associated with personal privacy.

(c) Data to be collected/specimen questions

- How often do personnel receive computer security awareness training?
- What is the procedure for gaining access to computers, applications and data?
- What is the process for granting access to sensitive data and applications?
- What is the company policy on social media use?
- What is the consequence for a violation of security procedure by a person?
- Are penalties adequate and correctly applied? Is good behaviour appropriately rewarded?
- Do all computers include a "Notice of Use Agreement" during logon?
- Do computers have a password protected screen saver? What is the time delay?
- What are the procedures for termination or transfer of employees who violate computer security requirements?
- Are computer user names, passwords and accounts for terminated employees immediately cancelled?

6.5.4. Focused areas for computer security review

6.5.4.1. Computer security policy

Management should set a clear policy direction in line with nuclear safety and security, and demonstrate support for, and commitment to, computer security through the issue and maintenance of a computer security policy across the organization.

A computer security policy should be defined, communicated, documented and periodically reviewed. This computer security policy should take into account nuclear security, nuclear safety, and nuclear material accountancy and control functions.

(a) Objective of review

- To verify there is adequate management direction and support for computer security in accordance with nuclear safety and security, as well as relevant laws, regulations and business requirements.

(b) Documentation and records of interest

- Computer security policy/plan;
- Facility security policy/plan;
- Computer security policy communications to employees;
- Record of computer security audits;
- Description of the process for computer security policy/procedure modifications;
- Record of security policy review and updates;
- Records of computer security exercises.

(c) Data to be collected/specimen questions

- Has the security policy been defined?

- Are the responsibilities clearly defined and corresponding authority and accountability assigned? What are the computer security objectives?
- Does the policy clearly state the security objectives?
- Is the policy consistent with other facility policies?
- How does the security policy address assets associated with physical protection and supporting systems?
- How is the security policy communicated to employees?
- How is management commitment demonstrated?
- How often is the policy reviewed for changes? Is there a record of review?
- How does the management evaluate the effectiveness of the policy?
- Does the security policy address all the computer security functional domains?
- If exceptions to the security policy exist, are these documented?
- Is the security policy communicated to third parties (subcontractors, etc.)?
- Does the policy follow current best practice guidance?

6.5.4.2. Computer security management

(a) Objective of review

- To verify that a management framework exists to initiate and control the implementation of computer security specific for physical protection assets.

(b) Documentation and records of interest

- Computer security policy/plan;
- Policy and procedure detailing the computer security management organization;
- Organization charts and job descriptions;
- Succession plan and hiring programme;
- Training programme, policy and records.

(c) Data to be collected/specimen questions

- Is the computer security policy applied/specified to the management of physical protection systems?
- Where in the organizational hierarchy do the computer security responsibilities reside?
- What is the structure of the computer security team? How large is the team?
- Does an interface between the physical protection officer and the computer security officer exist with clearly defined roles and responsibilities?
- What are the position requirements (i.e. background and education) for those assigned cyber security duties involving physical protection systems? Are all positions filled?
- Is there specialized cyber security training for those with security functions involving physical protection systems?
- Who is required to be trained, how often are they trained and what percentage has actually been trained?

6.5.4.3. Computer asset management

All assets should have a dedicated owner who is responsible for assigning appropriate controls. The implementation of specific controls may be delegated by the owner. In the case of delegation, the owner remains responsible for the proper protection of the assets.

(a) Objective of review

- To verify there is effective management of computing assets in support of physical protection.

(b) Documentation and records of interest

- Policy and procedures detailing the asset management system;
- Inventory of assets (computer systems, network equipment, software);
- Procedures and criteria for identifying computers within the scope of the computer security programme, if applicable;
- List/diagram of the physical location of inventoried assets;
- Inventory procedures, including periodicity and records of inventory updates;
- Functional diagram of systems and associated computer assets;
- Computer security zone model diagram (if applicable);
- Policy and procedures for sensitive information classification, including computer storage and computer classification.

(c) Data to be collected/specimen questions

- Who (persons, organizations) made the inventory?
- Who maintains the inventory? How often is it verified?
- Who has access to the inventory?
- Traceability of changes to the inventory.
- Protection of the inventory (including the backups).
- How asset classification is conducted? Is it documented? What is the quality?
- Is there a level of security defined according to the computer security zone? What are the security measures taken for each level?
- Do the physical locations match with the inventory?
- Does the zone model and physical location of a system (or part of it) match?
- How are assets labelled in accordance with their role in physical protection? How does the classification translate into logical zones (i.e. graded approach)?

6.5.4.4. Physical protection and environmental security

Prevention and security controls should be based on a risk assessment and the graded approach. Systems important to security should be housed in secure areas. They should be physically protected from unauthorized access, damage, and disruption. Due care should be taken to mitigate insider threat.

(a) Objective of review

- To verify that the environments of computer based systems important for nuclear security have adequate physical protection.

(b) Documentation and records of interest

- Facility security policy/plan;
- Computer security policy/plan;
- Functional diagram of systems and associated computer assets;
- Diagram of the physical layout of the facilities;
- List/diagram of the physical location of inventoried assets;
- Diagram/list of physical protection controls;
- Physical network cables/wiring diagrams, including locations;
- Procedure for relevant physical access control processes and access lists;
- Access control records;
- Organization charts and job descriptions, including authorized physical access.

(c) Data to be collected/specimen questions

- What are the designated security sensitive controlled areas?
- Describe the physical, technical and procedural access control mechanisms in place for each controlled/sensitive area.
- Are systems used for physical protection isolated in dedicated areas or resident within multiple use environments?
- Are physical protection measures adequate for computer systems of concern?
- What is the access or escort policy for third parties working in controlled areas?
- What is the policy for portable media and hand-held electronic devices in controlled areas?
- What is the disposal process for broken or replaced computer equipment?
- What is the disposal process for electronic media?
- What is the procedure for removing computer equipment and media off-site (e.g. bringing a laptop home to do work)?
- What is the procedure for bringing external (i.e. non-facility owned) equipment to use at work (e.g. laptop, thumb drive)?
- What are the security controls associated with protecting the computer environment (e.g. equipment cooling, flood prevention)?
- Do IP/communication ports exist outside the controlled/sensitive area (e.g. IP cameras, card readers)?

6.5.4.5. Computer operations management

The specific focus for this review is on computer systems pertaining to physical protection.

(a) Objectives of review

- To verify the existence of adequate operational procedures to ensure that the systems operate as intended;
- To verify the exfiltration and infiltration of data from and to computer systems are adequately protected against the introduction of new vulnerabilities;
- To verify the integrity of the computer communications.

(b) Documentation and records of interest

- Network architecture diagram;
- Data flow diagram identifying the interconnection between networks and data flow;
- Policy and procedure for configuration management;
- Risk analysis reports;
- Policy and procedure for patch management;
- Policy and procedure for computer system 'hardening';
- Policy and procedure for managing media (accessing, labelling, storage, transportation and sanitation);
- Policy and procedure for verifying and validating security controls implemented on computers and networks within the scope of the computer security programmes;
- Qualification/certification records for the individuals who are performing the verification and validation testing;
- Policy and procedure for digital exchange of information within the facilities and with external facilities;
- Policy and procedure for releasing information externally/to the public (e.g. corporate web site);
- Policy and procedure for handing publically available information;
- Policy and procedure for third party service delivery management for all classes of computers and networks within the scope of the computer security programme;
- Agreements with third parties regarding what networks within facility are allowed to be accessed by the third party and third party security solutions;
- Policy and procedure for dealing with subcontractors to third parties;
- Policy, procedure and record of exemptions to the computer security programme;
- Policy and procedure for using wireless devices;
- Policy and procedure for using portable computing devices, including mobile phones;
- Policy and procedure for usage restrictions and implementation for wireless technologies;
- Policy and procedure for continual monitoring and assessment of the computer security programme.

(c) Data to be collected/specimen questions

- Do security procedures address different modes of operation (e.g. shutdown, maintenance period) of the facility to capture different security concerns associated with them?
- Has the facility performed effective testing and analysis to ensure computer security controls operate and protect as they are intended?
- How has the host facility configured its computers regarding least and most privileged access?
- How has the host facility configured its computers to address known vulnerabilities?
- Does the host facility have a security analysis and testing programme (using vulnerability analysis, penetration testing or other means) to identify potential known and unknown vulnerabilities? What is the scope of the testing programme?

6.5.4.6. Computer access controls

This domain addresses requirements for access control, user access management, user responsibilities, network access control, operating system access control, application and information access control, and mobile computing and teleworking.

(a) Objective of review

- To evaluate the control of logical access to computer systems in the facility pertaining to physical protection.

(b) Documentation and records of interest

- Policy and procedure for computer access control (management of rights, account management);
- Policy for third parties to access system components both on-site and remotely;
- Policy for monitoring network traffic and investigating anomalies;
- Record of results of any access control audits;
- Policy and procedure for reviewing system access rights;
- Organization chart for computer administrative right management;
- Policy and procedure for passwords (complexity, duration and account lockout policy);
- Policy and procedure for privilege granting procedures and documentation;
- Description of employed authentication and encryption mechanisms;
- Access control logging and monitoring documentation;
- Policy and procedure for account authorization and accounting;
- Network access policy (e.g. switches security, unconnected sockets, virtual LANs);
- Network and traffic topologies;
- Security gateway policy (e.g. router access control lists, firewall rules);
- Diagram/list of wireless access points;
- Policy and procedure for remote access (who? when? why? which services?);
- Policy and procedure for modem use and security;
- Policy and procedure for administrative/high privilege accounts.

(c) Data to be collected/specimen questions

- Is there consistency between logical access control and physical access control?
- What is the process for granting/obtaining access to computer? Revocation and renewal processes?

- Check for the application of 'segregation of duties' and 'least privilege' policies, technical and/or procedural. Which systems are accessed in performing specific job functions?
- What are the login procedures? Have effective protection measures been implemented?
- How are encryption keys managed, specifically who has access to keys and how are they generated and protected?
- What is the procedure for changes in personnel situations (e.g. person moves to different department, change of duties, termination)?
- Which of these systems are accessed remotely? With what frequency? Why are these systems accessed remotely?
- In the case of wireless communications, is there a usage policy and an assessment programme?
- Have possible paths been identified that might compromise network supporting physical protection systems?
- In the case where usual logical access control measures cannot be managed in certain components, either for technical or for performance reasons, verify that compensating measures are employed (e.g. adapted procedures, increased physical security, personnel security, intrusion detection, auditing measures) according to the security level of the system.

6.5.4.7. Computer systems acquisition, development and maintenance

The security controls covered under this security domain include supply chain protection, correctness of software, integration of security capability, factory testing and acceptance testing.

(a) Objective of review

- To verify that the security and integrity of the computer systems is maintained throughout the system life cycle.

(b) Documentation and records of interest

- Policy and procedure for system, equipment and service acquisition, including development of security requirements for the acquired or developed systems;
- Description of requirements to protect against supply chain threats and vulnerabilities;
- Description of requirements for vendors to employ software quality, secure coding and validation methods to minimize flawed or malicious software;
- Description or demonstration of security requirements to create, implement and document security test and evaluation plans to ensure that the acquired products meet all specified security requirements;
- Description and demonstration of security requirements to maintain the integrity of the acquired system until the product is delivered to the facility;
- Description of how the facility verifies and validates that the security controls and measures implemented before product delivery are, at least, at the same level as where the computer system will be used;
- Test plan and results for verification and validation of code against the security design and configuration requirements for internally developed computer software code;

- Validation test plan and results for evaluating the effectiveness of implemented computer security controls.

(c) Data to be collected/specimen questions

- Is computer security being appropriately addressed by the vendors?
- Are security functions specified in the acquisition and development chain, considering that there may be multiple contractors and subcontractors?
- How is equipment protected onsite prior to and during installation?
- What testing occurs to evaluate security functions, at the factory and after installation?
- Are systems tested in a development environment prior to implementation as a production system?
- How is integration testing conducted? Does it evaluate the system against known attacks and exploits and can it discover unknown attacks and exploits?

6.5.4.8. Detection of computer security events

(a) Objective of review

- To verify the existence of robust computer security measures and processes intended to detect covert security attacks on computer based systems that are critical for the physical protection of nuclear material and facilities against unauthorized removal and sabotage.

(b) Documentation and records of interest

- Policy and procedure and description of methods used to detect unauthorized use or access of systems and/or networks;
- Policy and procedure for continuously monitoring and assessing insecure and rogue network connections;
- Policy and procedure for conducting scans for unauthorized wireless connections and wireless access points;
- Policy and procedure for handling the discovery of unauthorized wireless connections or access points;
- Description of resources devoted to detection of computer security events;
- Record of detected computer security intrusions.

(c) Data to be collected/specimen questions

- Who is responsible for detecting covert computer security intrusions?
- What education and training do these individuals have?
- What external resources are available to these individuals?
- How do these individuals keep current with respect to new cyber-attack methods and vulnerabilities?
- Are the critical computer systems continuously scanned for malicious cyber-attacks?
- Are simulated attacks conducted against the critical computer systems?

6.5.4.9. Computer security incident management

(a) Objective of review

- To ensure processes are in place to respond to and communicate computer security incidents involving physical protection systems (including events and vulnerabilities) and to mitigate effectively any potential impact.

(b) Documentation and records of interest

- Policy and procedures for incident management and communication plan;
- Sample or template of an incident report (the actual report is preferred);
- Procedure/considerations for cross-domain effects of incident response.

(c) Data to be collected/specimen questions

- Relationship between the computer incident response team, the physical security system management team and the physical security incident response team.
- Does the computer security incident management plan adequately address external and internal (i.e. insider) threats?
- Is there a clear classification scheme to characterize the incident?
- Is the escalation procedure clearly defined (criteria, points of contact)? Are sufficient technical resources identified and available?
- What is the communications process for the incident (internal and external)?
- Are proactive procedures adapted to support an investigation process, including computer forensics?
- What is the remediation process, including the identification and implementation of compensatory and corrective measures?
- Is there consistency between incident management and continuity management for computer security and physical protection systems?
- What is the link between computer security incident management and overall facility incident management?
- How, and how often, are the incident response plans and procedures exercised? Are external parties involved, and if so, what is their role?
- Has the facility participated in any coordinated computer incident exercises at a facility, regional (or State level?
- Have reporting criteria been identified for communicating computer security events to the competent authority?
- If a DBT is implemented and addresses cyber-attack, have criteria been defined with regard to a beyond DBT cyber event? If so, has a technical authority been identified and processes established to respond in such cases?

6.5.4.10. Continuity management

This domain addresses the restoration and management of continuous computer operations following disruptions caused by natural hazards, human error and malicious intent. Whereas the previous section

dealt with the initial response and mitigation of the incident, the focus of this domain is continuity and the recovery process.

(a) Objective of review

- To verify the existence of measures for the restoration and continuity of critical physical protection functions following major disruptions to normal computer systems and processes.

(b) Documentation and records of interest

- Policy and procedures for continuity management (continuity of operations plan);
- The list of applications and systems that have continuity management and the list of their owners (line and computer security organizations) and their respective responsibilities;
- Continuity of operations training records (including exercise reports).

(c) Data to be collected/specimen questions

- Are critical subsystems and interdependencies identified? Are contract agreements sufficient to support continuity objectives?
- Do critical systems and functions have appropriate levels of diversification and redundancy?
- Is the malicious dimension (intentional attack versus incidental failure) appropriately addressed in the continuity management?
- Is there consistency between incident management and continuity management?
- Are test plans for continuity and recovery of computer systems and recovery procedures (e.g. restoration and update of data between shutdown and restart) known, tested and reviewed?
- Has the workforce been trained on system recovery and continuity management? Who has been trained?
- How does continuity management address prioritization of access and resources during operational degradation?
- Has the facility conducted training exercises focused on system recovery and continuity management of physical protection systems for a cyber-event?
- Do backup systems exist to manage critical computer functions in the case of an incident/accident?
- What security controls are applied to the backup systems? How are backup systems and backup media protected?
- What is the architectural tie to the backup systems?
- How often are systems backed up? Do backups include system configurations, process software and databases?
- How, and how often, are restoration processes tested?
- Do procedures exist to support operations on the loss of computer functions?

MAIN CONTRIBUTORS TO DRAFTING AND REVIEW

Dal B.	Ministry of Foreign Affairs, Netherlands
Delaunay N.	International Atomic Energy Agency
Dudenhoeffer D. D.	International Atomic Energy Agency
George C.	International Atomic Energy Agency
Gorinov I.	Bulgarian Nuclear Regulatory Agency (BNRA), Bulgaria
Hagemann A.	Consultant, Germany
Hoffman R.	Idaho National Laboratories (INL), USA
Horvath K.	Hungarian Atomic Energy Authority (HAEA), Hungary
Isaksson S.	International Atomic Energy Agency
Jalouneix J.	Institut de Radioprotection et de Sûreté Nucléaire (IRSN), France
Matter J.	Consultant, USA
Ortiz S.	Sandia National Laboratories (SNL), USA
Price C.	Consultant, UK
Rawl R. R.	Consultant, USA
Stadalnikas A.	International Atomic Energy Agency
Wieland B.	Consultant, Switzerland

IAEA
International Atomic Energy Agency

No. 23

ORDERING LOCALLY

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

14-43071

INTERNATIONAL ATOMIC ENERGY AGENCY
VIENNA
ISSN 1816–9309