Nuclear Security in the Uranium Extraction Industry

IAEA
International Atomic Energy Agency

IAEA NUCLEAR SECURITY SERIES AND RELATED PUBLICATIONS

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

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

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

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

RELATED PUBLICATIONS

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

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

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

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

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

NUCLEAR SECURITY IN THE URANIUM EXTRACTION INDUSTRY

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

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

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

NUCLEAR SECURITY IN THE URANIUM EXTRACTION INDUSTRY

INTERNATIONAL ATOMIC ENERGY AGENCY
VIENNA, 2016

For further information on this publication, please contact:

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

NUCLEAR SECURITY IN THE URANIUM EXTRACTION INDUSTRY

IAEA-TDL-003
ISBN 978-92-0-110815-9

Printed by the IAEA in Austria
February 2016

FOREWORD

Uranium ore concentrate (UOC) in various chemical forms is a valuable commodity in the commercial nuclear market and a potential target for unauthorized removal. With the global expansion of uranium production capacity, control of UOC is emerging as a potential weak link in the nuclear supply chain. UOC is considered to be source material for both peaceful and non-peaceful purposes. Its protection, control and management thus pose a key challenge for the international community, including States, regulatory bodies and industry.

UOC is produced in various chemical forms. The chemical form of the final product is also dependent upon several factors, such as the chemical form of the ore bodies containing the uranium, the concentration of uranium within the ore body, the capital equipment cost for mills, the cost of raw materials to extract the uranium, regulatory requirements associated with environmental compliance and other cost factors that affect profit margin. The majority of uranium mines and mills produce UOC in the form of U_3O_8.

The IAEA has developed this publication to assist States in implementing prudent management practices in the uranium industry for the prevention and detection of, and response to, unauthorized removal of UOC. Currently there is limited international guidance applicable to the protection of UOC. The Convention on the Physical Protection of Nuclear Material and its 2005 Amendment, as well as IAEA Nuclear Security Series No. 13, Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5), state that natural uranium is to be protected in accordance with prudent management practice. However, they do not describe specific measures that would meet this criterion.

This publication provides information for State regulatory bodies and industry operators on prudent management practice for protecting UOC from unauthorized removal during production, storage and transport; it does not cover incident response. The measures for prudent management practice described can be adopted in the form of regulations or applied as voluntary standards. In either case, the regulations or voluntary standards would supplement existing requirements for environmental protection, radiation protection and radiological safety. The measures described here may not be universally applicable. States, regulatory bodies and industry may choose to tailor their implementation of this information to meet their national threat and other circumstances.

This publication also provides practical information for the uranium industry and enables mill/concentration plant and transport operators to document how the measures they have implemented to protect UOC from unauthorized removal are prudently managed.

The IAEA conducted a regional seminar on good practices in the processing and control of uranium ore from 23 to 27 April 2012 in Windhoek, Namibia, to discuss regulatory issues associated with safe and secure production of UOC. The outcomes from that regional seminar are included within the measures described in this publication.

This publication describes a suggested interpretation of “prudent management practice” in the context of the uranium industry in terms of the actions that would be taken by the different parties if that interpretation were followed. The information provided here is not international consensus guidance, and therefore is not expressed as “should” statements, but is intended to show States or organizations that wish to follow the suggested approach how it can be done. The publication does not deal with the safeguards obligations with respect to UOC.

This publication was prepared in a series of seven consultancy meetings with input from more than thirty experts from ten Member States, including experts from three operating organizations of uranium extraction industry facilities.

EDITORIAL NOTE

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

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

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

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

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

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

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

CONTENTS

1. INTRODUCTION

1.1. BACKGROUND

UOC is an integral component of nuclear energy production and is considered source material for a peaceful nuclear power programme and as such needs to be processed, stored and transported by authorized personnel. As well as being radioactive material, it could also be source material for constructing nuclear weapons; however several additional steps of conversion, enrichment, reconversion and assembly would be needed to produce material suitable for use in a nuclear weapon. Practical security measures are therefore needed against the unauthorized removal or misuse of UOC or its precursors.

UOC within the extraction and concentration process, up to the point of precipitation, can be adequately protected using common industrial security measures typical of industrial facilities. UOC that has been precipitated and is being or has been concentrated, purified and transported needs specific additional security measures to address the risk of unauthorized removal, as the material in this form is more attractive to potential adversaries.

Currently, there is limited international guidance applicable to the protection of UOC. The Convention on the Physical Protection of Nuclear Material (CPPNM) and its 2005 Amendment, as well as IAEA Nuclear Security Series No. 13, Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5), state that natural uranium would be protected in accordance with “prudent management practice”. However, neither the CPPNM nor INFCIRC/225/Revision 5 describes specific measures which would constitute “prudent management practice”, incorporating the principle of defence in depth as defined in INFCIRC/225/Revision 5.

1.2. OBJECTIVE

This publication aims to provide States and operators with advice for defining, implementing, maintaining or enhancing their nuclear security regime for the protection of UOC against unauthorized removal, thereby filling the gap left by the CPPNM and INFCIRC/225 in defining prudent management practice. It provides advice to regulatory bodies and industry for applying this recommendation by implementing prudent measures to protect, control and manage UOC in processing, storage and transport. Collectively, these measures are considered to constitute prudent management practice.

1.3. SCOPE

The uranium extraction industry includes the following activities [2]:

— Exploration: The discovery and sampling process that is the commencement of UOC production.

— Mining: The process of removing the uranium resource from the ground. This is typically open cut or underground mining and also includes in situ and heap leach processes. Uranium can also be extracted as a co-product where uranium is mined in combination with other minerals.

— Milling: The process of grinding the ores and the early removal of uranium from the host rock.

— Extraction/concentration: The process of concentrating the uranium into intermediate forms of UOC, which includes primarily[1] ammonium diuranate from acid solutions and sodium diuranate from alkaline solutions.

— Precipitation/purification: The conversion of intermediate forms of UOC to uranium dioxide, uranium trioxide, uranyl peroxide or triuranium octoxide.

— Packaging/transport: The movement of the UOC to and from the various stages of the process.

In following a graded approach to the implementation of nuclear security in the uranium industry, allowance is made for the increasing need to protect natural uranium as it is concentrated and purified during the final stages of the process and subsequently transported. The security risks associated with the first three steps in the process, i.e. exploration, mining and milling, are not a nuclear security concern, as these steps do not produce any material that is in a form and concentration attractive to adversaries. Accordingly, these first three steps are not covered further in this publication, and this advice primarily addresses security in the extraction/concentration, precipitation/purification and packaging/transport steps (see Annex III). Appendix IV provides additional details in support of this reasoning.

As the number of conversion facilities worldwide is limited, and the form of converted uranium can be fundamentally different from UOC, conversion facilities are not covered in this publication. Therefore, nuclear security for natural uranium conversion facilities will be addressed in other guidance.

The radiological consequences arising from the sabotage of UOC in production facilities are relatively low and are similar in magnitude to the consequences arising from the sabotage of other chemical or industrial targets at such facilities. Therefore, this publication does not address sabotage further. However, the measures recommended here to address the threat of unauthorized removal would also address the threat of sabotage.

Depending on the threat and other national circumstances, the State may choose to address nuclear security in the uranium industry through promotion of security measures to be applied voluntarily rather than through establishment of security regulations. In such cases, the advice in this publication may be helpful in applying such voluntary measures.

1.4. STRUCTURE

After this introduction, Section 2 describes the framework that a State would establish to address all applicable State obligations associated with UOC. Section 3 describes the risk informed approach that a State would consider in implementing its physical protection regime for UOC. Section 4 describes a State's considerations in designing and operating a security programme for UOC. Finally, Section 5 describes recommended prudent management measures for the security of UOC. A series of Appendices (I–IV) and Annexes (I–III) provide examples relating to some of the measures described in the main text.

2. FRAMEWORK FOR PROTECTING UOC

The State's nuclear security regime would include systems and measures for the protection of UOC against unauthorized removal. The following paragraphs describe the elements of such a regime, identified in IAEA Nuclear Security Series No. 13, Nuclear Security Recommendations on Physical

[1] The various chemical forms of uranium ore concentrate, or yellowcake, from the mining, milling and recovery process include ammonium diuranate or ADU from acid solutions in the form $(NH_4)_2U_2O_7$, sodium diuranate from alkaline solutions in the form of $Na_2U_2O_7$, uranium trioxide [UO_3], uranyl peroxide [UO_4] and triuranium octoxide [U_3O_8]. UOC is defined in this publication as pure U_3O_8 (85% U).

Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5) [1], which have particular relevance to the security of UOC.

The IAEA has determined for safeguards[2] purposes that, the timeliness goal for detection of diversion of a significant quantity of natural uranium (10 tonnes or approximately 35 drums or a single 20-foot shipping container of UOC) is one year[3]. However, for nuclear security purposes, it is considered that detecting unauthorized removal of a quantity of UOC equivalent to a single drum within one month is prudent. Other quantities that are a fractional percentage of throughput (e.g., 0.3%) for a defined time period may also be considered prudent for in process inventory. Therefore, the security measures described in this document seek to achieve that stronger detection goal. This can be accomplished by establishing a security programme that includes physical protection and inventory control measures to address threats from outsiders and insiders, as well as collusion between them. Physical protection measures include detection, delay and response measures to prevent unauthorized access to UOC in process, in storage and in transit. These measures provide effective security against outsiders acting either independently or in collusion with insiders. Inventory control measures include a combination of technical and administrative controls, such as process monitoring, item counting and ledgers that provide the capability to track and trace each drum or container from the time it is filled or loaded up to the point where the UOC is fed into the conversion process.

This advice suggests that security measures be applied on a graded basis, taking into account the current evaluation of the threat, the relative attractiveness of the material and the potential consequences resulting from unauthorized removal. The requisite level of security is achieved through a combination of physical protection and inventory control measures [1]. These measures are consistent with and support the quality assurance and control measures that are commonly implemented in the uranium industry. Some of the recommended measures may already be in place for safety purposes in some States. However, they are included for completeness in this document because they may not always be present.

2.1. STATE RESPONSIBILITY

(Fundamental Principle A: Responsibility of the State [1])

The State should establish a regime that addresses all applicable State obligations associated with the physical protection of nuclear material, including UOC. The physical protection regime is part of the State's national security regime and should address the security risks to persons, property, society and the environment arising from the processing, storage and transport of UOC.

The scope of the State's physical protection regime in relation to UOC will depend on the involvement of the State in the uranium industry, for example, whether it is a producer State (producing uranium for domestic use and/or export), a transit State (uranium is only transported through the State), a destination State (imports and uses uranium) or a combination of these.

Although not a responsibility of States, they should facilitate international cooperation regarding prudent management practice for nuclear security in the uranium industry, particularly in relation to international transport of materials associated with the industry.

---

[2] Based on INFCIRC/540 (Corrected)

[3] UOC is considered to be indirect use material. See Table II, paragraph 3.14 of the IAEA Safeguards Glossary, 2001 Edition, International Nuclear Verification Series No. 3 for more information on the definition of significant quantity, paragraph 4.26 for the definition of indirect use material and paragraph 3.20 for more information on timeliness detection goals.

2.2. LEGISLATIVE AND REGULATORY FRAMEWORK

(Fundamental Principle C: Legislative and Regulatory Framework [1])

The State is responsible for enacting legislation, adopting regulations, issuing licences and promulgating standards to give effect to proper implementation of the State's physical protection regime. The most effective way of applying such legislative instruments to the security of UOC will depend on the nature of the State's involvement in the uranium industry.

The State's national legislative and regulatory framework should address the following:

— Identifying the State's domestic threat in relation to UOC;

— Establishing and reviewing security requirements for UOC, including a system of evaluation, licensing and enforcement;

— Evaluating security systems on a regular basis in order to identify security deficiencies, take account of advances in technology and address potential changes in the threat;

— Placing the prime responsibility for the implementation of security of UOC on facility operators, consigners and carriers;

— Requiring submission of a security plan by the operator, consignor or carrier to the regulatory body;

— Developing a programme for verifying continued compliance with the security regulations and licences through periodic inspections and ensuring that corrective actions are taken when needed through enforcement;

— Developing processes and procedures to identify, classify and control sensitive information regarding UOC, the unauthorized disclosure of which could compromise security;

— Determining the required trustworthiness of personnel with authorized access to UOC or security sensitive information;

— Reporting of, and responding to, nuclear security events involving UOC.

2.3. COMPETENT AUTHORITY

(Fundamental Principle D: Competent Authority [1])

— The State's legislation should establish one or more competent authorities, including a regulatory body, to carry out roles and responsibilities in relation to the physical protection of UOC.

— The regulatory body and other competent authorities should cooperate to ensure that the legislative and regulatory framework is effectively and efficiently implemented.

— The regulatory body responsible for supervision of UOC should be effectively independent of any other body in charge of the promotion or utilization of nuclear energy, such as the marketing of UOC.

— The regulatory body should have the appropriate powers and resources to carry out its roles, including enforcement of compliance with regulatory requirements. Enforcement powers should include the ability to levy fines, suspend or revoke licences and seek criminal prosecution for unauthorized removal of UOC.

— The regulatory body should establish a system of licensing for the security of UOC in process, in storage and in transit. Licences covering nuclear security may be separate or be combined

with licences issued for other purposes, such as safety and environmental protection. Practical measures implemented to address radiological safety and environmental protection may also be beneficial to securing UOC.

— The regulatory body should establish appropriate measures to ensure the promotion of a culture of sharing and following best practices for control of UOC within the uranium industry.

2.4. RESPONSIBILITIES OF LICENCE HOLDERS

(Fundamental Principle E: Responsibilities of Licence Holders [1])

Operators, shippers and carriers should be assigned the primary responsibility for implementing, maintaining and testing security measures in accordance with national requirements and their security plan. While operators may be allowed, depending on a State's regulatory requirements, to appoint a third party to carry out actions and tasks related to security, the operator should retain the prime responsibility for regulatory compliance. Operators, shippers and carriers should be required to ensure that their personnel and contractors are suitably trained to meet regulatory requirements. Operators and shippers should be made responsible for developing and maintaining a nuclear security culture, in cooperation with the State.

2.5. IDENTIFICATION AND ASSESSMENT OF THREATS

(Fundamental Principle G: Threat [1])

The threat relative to UOC consists of persons or groups of persons with motivation, intention and capability to attempt unauthorized removal. The State should assess its national threat for UOC and produce an evaluation of these threats — based on available intelligence, law enforcement and open source information — that describes the motivations, intentions and capabilities of such persons or groups of persons. The threat assessment should consider insider threats, i.e. individuals with authorized access to UOC facilities or UOC in transport who could attempt unauthorized removal or who could aid an external adversary to do so.

Notwithstanding the current threat assessment, the State should also consider any new specific or increased threats and/or changes to threat levels and evaluate the implications of any changes in the threat for the performance of its physical protection regime. This information should be provided to the regulatory body.

The regulatory body should provide threat based information to the operator so that it can appropriately design and implement its security system.

2.6. RISK MANAGEMENT

The important risk associated with UOC is that of its unauthorized removal and subsequent further processing with the intent to construct a nuclear explosive device, which could lead to subsequent dispersal. The State would ensure that its physical protection regime is capable of keeping this risk to an acceptable level through risk management. Specifically, the State would assess the threat as discussed above, estimate the consequences of unauthorized removal and develop a legislative, regulatory and programmatic framework that ensures appropriate effective physical protection measures are put in place. See the example given in Annex I.

2.7. GRADED APPROACH

(Fundamental Principle H: Graded Approach [1])

Prudent management practice follows a graded approach for the protection of the UOC in process, in storage and in transit. The scope, depth and rigour of security requirements for UOC should take into

account the principles of risk management, including the level of threat, the relative attractiveness of the material and the potential magnitude of the consequences of unauthorized removal. Nuclear security measures should become more rigorous as the uranium concentration increases. The graded approach should also address changes in threat. The State may establish a default set of permanent security measures that are in place at all times. Additional measures may also be defined that take effect when the State notifies the operator of an increased threat.

2.8. CONTINGENCY PLANS

(Fundamental Principle K: Contingency Plans [1])

The State should establish a contingency plan consisting of predefined sets of actions for response to actual or attempted unauthorized removal of UOC. The regulatory body should ensure that the operator prepares its own contingency plans to effectively counter the threat. Contingency plans should be appropriately exercised by all operators and authorities concerned. Arrangements should be made to ensure that during emergency conditions and exercises, the effectiveness of security measures is maintained as far as practicable. The operator should be required to initiate its contingency plan after detection and assessment of any malicious act.

2.9. NUCLEAR SECURITY, SAFETY AND SAFEGUARDS

The State's physical protection regime would promote coordination between nuclear security, safety and safeguards especially since under a comprehensive safeguards agreement a State is obliged to establish and maintain a system for the accounting for and control of nuclear material. Worker health and safety and environmental protection measures would be used, where possible and when prudent, to support nuclear security in cases where the measures implemented for one system also support the objective of the others. Regulatory bodies, operators and shippers would be encouraged to take advantage of the synergies between the application of security, safety and (where applicable) safeguards measures in the uranium industry, especially where implementation of these roles is shared.

3. DEVELOPING A RISK BASED APPROACH

Nuclear security in the uranium industry would follow a risk based approach. Consideration should be given to the threat, the attractiveness and the vulnerability of UOC, and the potential harmful consequences of unauthorized removal of such material.

3.1. THREAT

A threat is a person or group of persons with the motivation, capability and intention of unauthorized removal of UOC. The motivations, capabilities and intentions of such persons may vary significantly from threat to threat, from time to time and from State to State, and the threat(s) to be considered as a basis for designing nuclear security measures for uranium in process and the UOC in storage and during transit would be determined in the State's national threat assessment.

3.2. TARGETS

For the purposes of this document, the target is uranium in process (during the concentration stage), in storage and in transit. The material generally becomes more attractive as a target as the uranium concentration increases during the concentration process and potentially more vulnerable when it reaches concentrated form. The attractiveness of uranium also depends on the amounts involved and its removability, i.e. the ease with which, if unauthorized access were gained, the material could be removed and subsequently handled by an adversary.

Nuclear security requirements would also consider a time limit for detecting unauthorized removal of a defined target quantity of UOC. The time limit and defined target quantity would be set by the

regulatory body, depending on the State's acceptance of risk. Material in the various stages of mining, milling, concentration, purification and product storage can be compared against the target quantity as the basis for a graded approach to the application of nuclear security measures for each process and facility (see Appendix III).

3.3. RISK SCENARIO

The relevant risk scenario for uranium in process, in storage or in transit is unauthorized removal. In this scenario, the insider/outsider or both would gain access to, and remove, the defined target.

3.4. VULNERABILITY ASSESSMENT

A vulnerability assessment provides a systematic means of evaluating the effectiveness of security systems against the defined threat. Operators, shippers and carriers would carry out vulnerability assessments based on the current threat assessment and regulatory requirements.

3.5. APPLICATION OF THE RISK BASED APPROACH TO URANIUM

A vulnerability assessment is an important part of a risk based approach and would form the basis for implementing security measures. It identifies and documents the level of protection required. More specifically, the purpose of this assessment is to:

- Identify and assess potential threats to UOC and associated sensitive information;
- Identify UOC and associated sensitive information that needs protection;
- Assess the risks associated with each threat by estimating the likelihood of the unauthorized removal of UOC occurring and rating the potential consequences of the threat being realized;
- Identify existing vulnerabilities and appropriate security measures to reduce the residual risk.

Operators, shippers and carriers should be encouraged to undertake such assessments for UOC in process, in storage and in transit to ensure appropriate security measures are taken commensurate with real or potential threats, including insider threats. Such assessments will help ensure that the implementation of security measures follows the graded approach. The competent authority would provide applicable threat based information to operators so that they can appropriately design and implement their security systems.

4. CONSIDERATIONS FOR DESIGNING AND OPERATING A SECURITY PROGRAMME

The regulatory body, as part of the licensing process, would require each operator to develop a security programme based on the following measures identified in their security plans (Facility security plan and Transport security plan):

- A security policy statement, demonstrating commitment to comply with regulatory requirements;
- Definition of security responsibilities;
- Security functions that implement prudent management practice through administrative and physical controls;
- Establishing and maintaining a security culture;

— A security plan that documents compliance with regulatory requirements for physical protection, inventory control and transport security, including provision for reporting a security event and provision for implementing an effective response;

— Administrative controls and procedures;

— Quality assurance, to ensure that security systems and management practices meet applicable requirements;

— Security of sensitive information.

4.1. SECURITY POLICY

Operators, shippers and carriers would be required to develop a policy statement that demonstrates their commitment to comply with applicable nuclear security requirements.

4.2. SECURITY MANAGEMENT

Security management provides an organizational structure identifying security responsibilities that includes provision for ensuring adequate resources (personnel and funding) for security. It also includes developing procedures, policies, records and plans for the security systems and for an effective security culture. Security management also includes developing procedures for the proper handling of sensitive information and protecting it against unauthorized disclosure.

4.2.1. Security functions

The operator would be required to employ the defence in depth principle in the design of its security systems. This principle calls for multiple layers of protection, including both administrative controls and physical controls, which adversaries would have to overcome or circumvent to achieve their objectives.

A security system would be designed to perform the basic security functions of detection, delay and response to prevent unauthorized removal of UOC. A combination of these physical protection measures provides for deterrence against unauthorized removal:

— Deterrence discourages an adversary from attempting to commit a malicious act.

— Detection can be achieved by several means, including visual observation, electronic sensors, accountancy records, seals and other tamper indicating devices, process monitoring systems and other means. Each detection measure needs a corresponding method to assess the cause of the alarm.

— Delay impedes an adversary’s attempt to gain unauthorized access to or to remove UOC, generally through barriers (e.g. fences, locks) or other physical means.

— Response encompasses the actions undertaken following detection to prevent adversaries from achieving their objective. These actions, typically performed by security or law enforcement personnel or other State agencies, include interrupting and subduing an adversary during the attempted unauthorized removal.

An appropriate combination of effective detection, delay and response measures will result in a security programme that serves as an effective deterrent, or if deterrence fails, is effective in preventing adversaries from achieving their objective of unauthorized removal of UOC in target quantities.

4.2.2. Nuclear security culture

Operators would be required to promote an effective nuclear security culture. Guidance on nuclear security culture is provided in IAEA Nuclear Security Series No. 7.

4.2.3. Security plan

Operators and shippers would be required to develop and implement security plans for the management of uranium in process, and UOC in storage and in transit. The security plans would include contingency plans. Such plans would form part of the facilities' overall management plans and would include predefined sets of actions for responding to, and effectively countering, unauthorized acts indicative of attempted unauthorized removal during normal operational activities as well as during anticipated security events and other emergency situations that could affect security. The security plan would address physical protection, inventory control and transport security of the UOC. The security plan would be periodically exercised, reviewed and, as appropriate, revised. The tables in Section 5 provide examples of prudent management measures, which would be documented in the security plan as outlined in Appendix I.

4.2.4. Administrative controls and procedures

Administrative controls and procedures would be developed to identify the roles and responsibilities of key personnel to implement physical protection, inventory control and transport security measures, as applicable, and to respond to, and report, nuclear security events. Procedures would also provide specific security related instructions to all personnel involved in the processing, storage and transport of UOC.

4.2.5. Quality assurance

Operators and shippers would be required to implement an independent quality assurance programme. The programme would verify and ensure that all aspects of the operator's security programme are functioning in accordance with the operator's documented performance criteria and in compliance with all State regulatory requirements. The quality assurance programme would address the following areas:

- Security management and functions;
- Personnel training and qualifications;
- Quality improvement;
- Control of documents and records;
- Control of work processes;
- Compliance of overall programme to regulatory requirements;
- Evaluation, including performance testing.

4.2.6. Information security

Operators and shippers would be required to protect the confidentiality of sensitive information pertaining to security matters and its integrity as relevant pursuant to applicable State regulations. Access to such information would be limited to personnel on a need to know basis and whose trustworthiness has been verified. Any information that could assist an adversary with unauthorized removal would be considered sensitive. The security programme would include procedures to ensure that sensitive information requiring protection is reliably identified. Security measures would be

developed and implemented for the handling and controlling of sensitive information. Such measures would address:

— Information storage: Measures would be taken to prevent unauthorized access to sensitive information when it is not in use, for example, by storing it in a locked receptacle.

— Transmission: Measures would be taken when transmitting sensitive information to ensure that the intended recipient is authorized to receive the information and to prevent unauthorized access.

— Reproduction: Procedures would be implemented to ensure that sensitive documents are not reproduced unnecessarily and that, when they are reproduced, only the necessary number of copies are made.

— Destruction: When documents or media containing sensitive information are no longer needed, measures would be taken to ensure that they are destroyed in a manner that prevents their reconstruction.

Information security procedures and measures would be documented in the security plan.

5. PRUDENT MANAGEMENT MEASURES

This section describes suggested prudent management measures for nuclear security in the uranium extraction industry.

The suggested prudent management measures are based on a generic application of the graded approach. Minimum measures would apply in all circumstances. Supplemental measures may apply in either of two circumstances: if the UOC is more vulnerable to unauthorized removal or if the threat has increased. The physical protection measures primarily address outsider threats. The inventory control measures address insider threats. The transport security measures address outsider, insider or a combination of both.

The suggested prudent management measures are presented in tables 1–3. These specific measures are in addition to the functional elements of a security programme described in Section 4. The tables are organized as follows. The first column indicates the security level, corresponding to the degree of protection warranted, based on the graded approach. The second column describes each suggested prudent management measure. The next three/four columns indicate the security function or functions performed by the suggested measure. The final three columns identify the material form to which the recommended measure applies. As indicated in the introductory text for physical protection, inventory control and transport security measures, the particular security levels and target material forms are specific to each table. All suggested measures would be implemented through the use of high quality, proven equipment and technology, which satisfy national or international quality standards.

These measures are not intended as a prescriptive approach to securing UOC. They would be considered as a set of possible measures to support implementation of the State physical protection regime in accordance with a risk based approach to a nuclear security programme for UOC.

5.1. PHYSICAL PROTECTION MEASURES

Table 1 describes suggested physical protection measures for prudent management of uranium in process and UOC in storage. Uranium contained within the majority of the extraction and concentration processes up to the point of precipitation can be adequately protected using minimum physical protection measures typical of industrial sites. The table refers to measures to achieve this security level as minimum physical protection measures. Uranium that is precipitated, concentrated and purified needs supplemental measures to address the potential for unauthorized removal because material in this form is more attractive and, once the process is complete, is more easily removable.

The table refers to the measures to achieve this security level as supplemental physical protection measures due to increased attractiveness and removability. The design and rigour of these supplemental physical protection measures will depend upon the assessed threat under normal operating conditions. The State may also require the operator to further strengthen physical protection measures to address a specific or increased threat. The table refers to the measures to achieve this security level as supplemental physical protection measures due to increased threat.

For each security measure, the first four columns indicate the security function(s) the measure performs and the remaining three columns identify the material to which the recommended measure applies: Uranium in concentrated solutions in the extraction and concentration process up to the point of precipitation, uranium precipitate is in the concentration and purification stage of the process and UOC powder in drums after the concentration and purification process. These measures, if properly implemented, will strengthen controls on UOC at the facility in preventing unauthorized removal of material. Virtually all physical protection measures provide some level of deterrence against an internal adversary. Table 1 provides an indication of deterrence for an external adversary.

TABLE 1. PHYSICAL PROTECTION MEASURES

Security level	Security measure	Security function				Material form		
		Deterrence	Detection	Delay	Response	Solution	Precipitate	Powder
Minimum physical protection measures	PS.M.1 Administrative controls that restrict access to authorized personnel at the site boundary. These administrative controls would include procedures for identifying and controlling visitor access.	X	X			X	X	X
	PS.M.2 Administrative controls to ensure that those process monitoring systems also used for security purposes are not compromised by any changes in facility design.		X			X	X	
	PS.M.3 Signs and postings that provide notification that access to the area is restricted to authorized personnel and that access to the area could expose individuals to chemical and radiological hazards.	X				X	X	X
	PS.M.4 Barriers such as fences, gates and entry control points that may or may not be manned and which identify a defined exterior boundary of the facility or critical areas within the facility.	X		X		X	X	X
	PS.M.5 Visual inspections of the process and storage areas to detect access by unauthorized personnel, unauthorized access to the process systems or storage areas or other anomalous conditions.	X	X			X	X	X
	PS.M.6 Detection assessment procedures and response arrangements.		X		X	X	X	X

TABLE 1. PHYSICAL PROTECTION MEASURES (cont.)

Security level	Security measure	Security function				Material form		
		Deterrence	Detection	Delay	Response	Solution	Precipitate	Powder
Supplemental physical protection measures due to increased attractiveness and removability	PS.S.1 Administrative controls that restrict access to process components containing uranium. These controls need to cover both normal operations and maintenance activities.		X				X	X
	PS.S.2 Administrative controls that require the use of approved vehicles to move UOC within the defined boundary of the site.		X					X
	PS.S.3 Administrative controls that require the use of approved containers for storage and transport of UOC. Use of these containers for any other purpose would be prohibited.		X	X				X
	PS.S.4 Performance testing with documentation which verifies that process monitoring equipment used for security purposes is properly maintained and tested to meet its design specifications.		X			X	X	
	PS.S.5 Administrative controls that limit the number of full drums in the product packaging area. Controls such as this will increase the probability of detecting unauthorized removal of a single drum.		X					X
	PS.S.6 Physical barriers that restrict access to the drum and transport container storage area to authorized personnel. The types of barrier that could be used include robust fencing, lockable doors, gates and block walls.	X		X				X
	PS.S.7 Industrial surveillance cameras to monitor process components containing concentrated cakes or powders and drums in the packaging and storage area(s).	X					X	X
	PS.S.8 A tamper indicating device to detect unauthorized access to process equipment and drums.	X	X				X	
	PS.S.9 A tamper indicating device to detect unauthorized access to UOC in storage and in transit.	X	X					X
	PS.S.10 Independent verification of access authorization to the drum packaging area, drum storage area and the transport container storage area.	X	X	X			X	X

TABLE 1. PHYSICAL PROTECTION MEASURES (cont.)

Security level	Security measure	Security function					Material form	
		Deterrence	Detection	Delay	Response	Solution	Precipitate	Powder
Supplemental physical protection measures due to increased attractiveness and removability	PS.S.11 Detailed procedures for supplemental measures if the threat to the facility is increased on the basis of credible information. Such procedures will ensure that supplemental measures can be quickly implemented in a structured manner to address the increased risk. For example: • PS.S.11.a Radiological surveys of all equipment and personnel exiting the facility. This is a common radiological safety measure that is required to limit the spread of contamination off-site and could be used to support supplemental measures under an increased threat environment. • PS.S.11.b Administrative requirement to implement a two person rule in the drum packaging and storage area. • PS.S.11.c Restriction of access to essential personnel and vehicles. • PS.S.11.d Notification and coordination with local law enforcement. • PS.S.11.e Increased surveillance measures. Additional physical protection measures may also apply, as required by the regulatory body.	X	X	X	X	X	X	X

5.2. INVENTORY CONTROL MEASURES

In addition to physical protection measures, operators would implement inventory control measures. These measures would consider material in process and in storage at the facility. The primary objectives of an inventory control system are to:

— Maintain accurate, timely, complete and reliable information on the location, quantities and characteristics of uranium in process or UOC in storage at the facility;

— Maintain control over uranium to ensure continuity of knowledge, thereby enhancing its ability to detect and prevent unauthorized removal.

To enhance nuclear security for timely detection of unauthorized removal of uranium, an effective inventory control system would also accomplish the following:

— Provide for prompt investigation and resolution of any anomaly indicating a possible loss of uranium, assistance in determining if unauthorized removal has actually occurred and performance of an emergency inventory, if required;

— Provide information helpful to the recovery of missing uranium;

— Provide the capability to assist in detecting misuse of the facility's processing/handling equipment;

— Act as a deterrent by providing the capability to detect insider activities related to unauthorized removal of uranium, if they occur.

Table 2 describes suggested inventory control measures. These tools, if properly implemented, will help detect and deter unauthorized removal at two security levels: (i) minimum inventory control security measures and (ii) supplemental inventory control security measures of pre-target (concentrated solutions) and target material (See 3.2). The measures associated with minimum inventory control security measures would be implemented at all times. The supplemental inventory control security measures could be selected depending on the attractiveness and removability of the UOC. In addition, if the insider threat increases, the frequency of inventory control administrative controls would be increased commensurately.

TABLE 2. INVENTORY CONTROL MEASURES

Security level	Security measure	Security function			Material form		
		Deterrence	Detection	Response	Solution	Precipitate	Powder
Minimum inventory control measures	IC.M.1 Methods and procedures to evaluate the inventory control programme to sustain effective performance.	X			X	X	X
	IC.M.2 Quality assurance procedures which demonstrate that facility process monitoring equipment is maintained and capable of detecting unauthorized removal.	X	X			X	
	IC.M.3 A qualified sampling and analysis programme to accurately determine uranium inventory and throughput.	X	X		X	X	X
	IC.M.4 Use of calibrated scales to accurately determine the mass of UOC in drums. Regular recalibration of scales.	X	X				X
	IC.M.5 Methods and procedures to estimate the bulk process inventory.	X	X			X	X
	IC.M.6 Administrative controls to balance raw material consumption against the number of drums produced over a defined period of time.	X	X				X
	IC.M.7 Information management systems that track the location and quantity of uranium in process and in storage. This information would be protected in accordance with information protection procedures.	X	X			X	X
	IC.M.8 Administrative controls to investigate and resolve indications of unauthorized removal of UOC.	X	X	X		X	X
	IC.M.9 Duplicate samples of the final product for independent analysis to resolve inconsistencies between the shipper and the receiver.	X	X				X
	IC.M.10 Unique identification of each drum and shipping container of UOC with a durable form of marking.	X	X				X

TABLE 2. INVENTORY CONTROL MEASURES (cont.)

Security level	Security measure	Security function			Material form		
		Deterrence	Detection	Response	Solution	Precipitate	Powder
	IC.S.1 Administrative controls to prevent unauthorized removal of UOC during maintenance activities where UOC is directly accessible.	X				X	
	IC.S.2 Independent assessment of the sampling and analysis programme by an organization external to the facility.	X	X			X	X
	IC.S.3 An inventory control plan that clearly defines control measures to detect and resolve indicators of unauthorized removal.	X	X			X	X
Supplemental inventory control measures due to increased attractiveness and removability	ICS.4 Administrative controls to track movement of drums between the process packaging area and the drum storage area and to document transfers of drums from the facility to the transporter.	X	X				X
	IC.S.5 Routine drum inventories to detect unauthorized removal from the storage area. **Note:** This is considered a minimal requirement for the drum packaging and drum storage areas.	X	X				X
	IC.S.6 Administrative procedures to receive, distribute, apply and track tamper indicating devices.	X	X				X
	IC.S.7 Administrative or technical controls that independently verify the number of drums filled over a defined period of time (e.g. per shift).	X				X	
	IC.S.8 Administrative controls to restrict removal of UOC using unauthorized pathways (e.g. sanitary waste containers, construction debris).	X	X			X	X

5.3. TRANSPORT SECURITY MEASURES

5.3.1. General considerations

All transporters (shippers, carriers, consignees) and other persons engaged in the transport of UOC would apply security measures commensurate with their responsibilities and the risk of unauthorized removal [3]. Such measures complement the use of manifests prepared by operators, shippers and carriers of the UOC cargo.

In view of the potential vulnerability of UOC in transport, the design of an adequate transport security system would incorporate the concept of defence in depth and use a graded approach to achieve the objective of preventing the UOC from being vulnerable to unauthorized removal [3]. The achievement of effective security in transport can be assisted by considering transport schedules, routing information and procedures and arrival verification.

The competent authority would, at its discretion, provide information to transporters regarding the potential threat to UOC in transport. Transporters would take all threat information into consideration when implementing security measures. For international transport, the threat information for each State involved in such transport would be considered.

All transporters (e.g. shippers, carriers, consignees) and other persons engaged in the transport of UOC would have the responsibility for implementing and maintaining security measures for the transport of UOC in accordance with State requirements, including security measures for intermediate storage of UOC during transit or at the port [3]. The security measures defined in Table 3 can be used for reference.

The operator would have procedures in place that will initiate an enquiry about the status of shipping containers that are not received by the intended recipient at the expected time. Through the course of the enquiry, if it is determined that the UOC has been lost or stolen or if it appears to have been tampered with, procedures would immediately be implemented to locate and recover the UOC [3].

Unless overriding safety or operational considerations dictate otherwise, UOC would be carried in secure and closed or sheeted conveyances. Specifically designated personnel would verify the integrity of locks and seals before dispatch and on arrival. Shipping manifests would also be verified at all stops, borders and transfer points.

In the event that UOC needs to be transported on open conveyances, it may be necessary for the State to consider — in view of the nature of the UOC or prevailing threat — whether supplemental measures would be applied.

5.3.2. International shipments

Appropriate arrangements would be established between receiving and transit States and relevant intergovernmental organizations to promote cooperation, harmonization and information exchange and to ensure that UOC under their respective jurisdictions is adequately protected. The designated regulatory body in each State would be identified to the other States and to the IAEA. Before an international shipment is undertaken, the originating State would confirm that the security requirements of the receiving State and any transit States will be met.

5.3.3. Prudent management measures

Table 3 lists suggested prudent management measures for the security of UOC during transport at two security levels: (i) minimum transport security measures for all shipments and (ii) supplemental security measures for consideration depending on threat. As indicated, specific measures may apply to UOC in transit or in intermediate storage during transport.

For maritime transport, shipment is required to be carried out in accordance with the applicable security provisions of the ISPS Code and of the International Maritime Dangerous Goods Code as required by the Convention for the Safety of Life at Sea (SOLAS 74 amended) [3]. These provisions would be supplemented by the advice in this publication.

TABLE 3. TRANSPORT SECURITY MEASURES

Security level	Security measure	Security function				UOC powder	
		Deterrence	Detection	Delay	Response	In transit	Intermediate storage
Minimum transport security measures	TS.M.1 Administrative controls and transport personnel training on reporting procedures associated with accidents and/or transport delays.	X				X	
	TS.M.2 Approved primary and alternative, if available, transport routes in accordance with State requirements.	X				X	
	TS.M.3 Restriction of access to shipping information to individuals on a need to know basis.	X	X			X	X
	TS.M.4 Contingency plans for transport and interim storage locations developed in coordination with all relevant competent authorities to address unexpected delays due to accidents, natural disasters, social unrest or other occurrences.					X	X
	TS.M.5 Industrial packages, typically a 200 L drum, shipping containers and labelling in compliance with all international standards for transport of UOC (e.g. IAEA Safety Standards Series No. TS-R-1).					X	X
	TS.M.6 Trustworthiness determinations for all personnel involved in transport and intermediate storage of UOC.	X				X	X
	TS.M.7 Administrative controls that prohibit transportation of other cargo with UOC in the same shipping container or on the same conveyance.		X			X	
	TS.M.8 Administrative controls that require drums and shipping containers of UOC to be physically segregated from other cargo when in interim storage.		X				X
	TS.M.9 Application of tamper indicating devices to all shipping containers, each with a unique identification. Procedures to control and track tamper indicating devices for each shipping container.		X			X	X
	TS.M.10 Determination of the gross weight of each container. Verification of this weight, when possible, during transport and upon receipt. (NOTE: Not necessary if there is no indication of tamper – see TS.M.9)	X	X			X	
	TS.M.11 Monitoring progress of transport of UOC by road using periodic communication (e.g. radio or mobile phone) or electronic tracking device (e.g. transponder) as defined in the transport security plan.	X	X		X	X	
	TS.M.12 Communications capabilities for the transport vehicle and transport personnel to facilitate immediate reporting of activities that put UOC at increased risk.	X	X			X	

TABLE 3. TRANSPORT SECURITY MEASURES (cont.)

Security level	Security measure	Security function				UOC powder	
		Deterrence	Detection	Delay	Response	In transit	Intermediate storage
Minimum transport security measures	TS.M.13 Evaluation of the contents of each shipping container within an acceptable period of time following receipt to identify any shipper/receiver differences. Procedures to address identified differences. Immediate notification made by the receiver to the shipper and the regulatory body of any differences.	X	X			X	
	TS.M.14 Administrative controls to verify the serial number and tamper indicating device number for each shipping container at interim storage locations.	X	X				X
	TS.M.15 Administrative controls to investigate and resolve indications of unauthorized removal of UOC.				X	X	X
	TS.M.16 Pre-shipment inspection of all transport security measures in accordance with the transport security plan.	X	X			X	

TABLE 3. TRANSPORT SECURITY MEASURES (cont.)

Security level	Security measure	Security function				UOC powder	
		Deterrence	Detection	Delay	Response	In transit	Intermediate storage
Supplemental transport security measures	TS.S.1 Levels of protection for interim storage facilities used to store UOC equivalent to the levels of protection for UOC in storage at the producer, as adjusted to address the local threat conditions.	X	X	X	X		X
	TS.S.2 Periodic inspections by the owner/operator of the interim storage facility to ensure security measures are in place prior to receipt of UOC.	X	X	X	X		X
	TS.S.3 Joint exercise of contingency plans on a periodic basis to ensure the operator, transport company, response force and regulatory body can respond in a timely and effective manner.	X	X	X	X	X	X
	TS.S.4 Random inspections to verify manifest inventory.	X	X			X	
	TS.S.5 Implementation of compensatory security measures when UOC is placed in temporary storage for extended periods of time due to transit disruptions.	X		X		X	X
	TS.S.6 Implementation of a two person rule for transport of UOC by road as defined in the transport security plan.	X	X		X	X	
	TS.S.7 Security patrols at interim storage areas to monitor for unauthorized access and/or unauthorized removal of UOC.	X	X		X		X
	TS.S.8 Consideration of security escorts to address specific threats as prescribed in the transport security plan.	X	X		X	X	

APPENDIX I:

WRITING A FACILITY SECURITY PLAN

The security plan would be developed in accordance with State regulatory requirements [4]. The plan would include all information necessary to describe the security programme, physical protection measures and inventory control measures being used for protection of the UOC. The level of detail and depth of content would be commensurate with the attractiveness and vulnerability of the material, as well as the threat to the UOC covered by the plan. The following topics would typically be included.

1. Introduction

A security plan documents effective implementation of national requirements associated with prudent management practice for UOC. It also provides facility and consignment personnel with specific instruction on how to implement prudent security measures for UOC in process, in storage and in transit. It is typically provided to the regulatory body for review and approval prior to licensing a facility and updated as necessary.

1.1. Overview

Summarize the purpose or mission of the facility and its operating organization, including the types of processing and storage of uranium conducted at the facility.

1.2. Material present

Describe the form and concentration of UOC in process and in storage at the facility.

1.3. Requirements

Describe the need for the security plan by considering the particular facility's circumstances, such as: (i) assessing the vulnerability of UOC and identifying adequate measures for protecting UOC against unauthorized removal and (ii) being part of, and integrated with, the organization's integrated management system.

1.4. Objective of the security plan

Describe the objectives to be satisfied by the security plan such as to: (i) document the design and operation of the facility's security system, physical protection measures and inventory control measures; (ii) demonstrate regulatory compliance by specifying in each relevant section which particular regulatory requirement is met and (iii) serve as an operational tool used by management and staff to integrate people, procedures and equipment into an effective security system.

1.5. Scope

Describe the coverage and any limitations of the security plan and its relation to other relevant documents or arrangements, such as measures implemented to address radiological safety and environmental protection. Reference would also be made to areas where security interacts with or impacts other management systems, especially those for safety.

1.6. Preparing and updating the security plan

Describe the process for developing, approving and updating the security plan, as well as its revision history within the organization's document control or quality management system. Describe how the security plan is reviewed and updated, at a prescribed interval specified by the regulatory body, as applicable, and as necessary to address new threat information, changes in facility operations or any other development that could affect the performance of the security system.

2. Facility description

2.1. Physical description

Describe the physical features of the facility and its surrounding environment, including diagrams and scale floor and building drawings and photographs. These descriptions would include:

(a) The location and layout of the facility, particularly indicating areas accessible to the public; roads and parking areas; nearest public thoroughfares; central security office; building and site perimeter; access points and physical barriers.

(b) The facility's surrounding environment, such as industrial, commercial, residential or other uses; indication of distances to the nearest police stations and other response services; proximity to other buildings, roads and other features of security or operational interest, such as other facilities with hazardous materials.

2.2. Operational description

Provide a description of the facility operations, including, as applicable, milling; leaching and filtration; extraction and stripping; precipitation, filtration and drying; packing and containerization; central storage and preparation for transport. At each stage, describe as applicable, UOC concentration, physical and chemical forms, processing methods employed and size, type and number of containers present.

2.3. Regulatory requirements

Identify and reference the applicable security requirements, if any. More specific reference to the particular regulatory requirement being satisfied would be given in other relevant sections of the security plan by stating the applicable provision of the regulations, licence, standards or other requirement.

3. Security programme

3.1. Security policy

Summarize or reproduce the facility's policy statement demonstrating its commitment to protect UOC from unauthorized removal.

3.2. Security management

Describe the facility's security management system that includes provision for:

(a) Clearly identifying the responsibilities of each individual for security and ensuring that each individual is suitably trained and qualified;

(b) Defining clear lines of authority for decisions on security;

(c) Ensuring adequate resources (personnel and funding) for the security programme;

(d) Developing procedures, policies, records and plans for the security programme and for an effective nuclear security culture;

(e) Developing procedures for the proper handling of sensitive information and protecting it against unauthorized disclosure.

3.3. Security culture

Describe how the facility promotes a security culture by ensuring that:

(a) Policies and procedures are established that identify security as being of the highest priority.

(b) Problems affecting security are promptly identified and corrected in a manner commensurate with their importance.

(c) Organizational arrangements and lines of communications are established that result in an appropriate flow of information on security at and between the various levels in the entire organization of the operator, shipper or carrier.

3.4. Administrative controls and procedures

Summarize the facility's administrative controls and procedures to identify the roles and responsibilities of key personnel to implement physical protection measures, inventory control measures and transport security measures, as applicable, and to respond to and report such nuclear security events, including reporting to off-site first responders.

3.5. Quality assurance

Describe the facility's independent quality assurance programme to verify and ensure that all aspects of its security programme are functioning in accordance with the security plan and in compliance with all applicable regulatory provisions, addressing the following areas:

(a) Security management and functions;

(b) Personnel training and qualifications;

(c) Quality improvement;

(d) Control of documents and records;

(e) Control of work processes;

(f) Compliance of the security programme with applicable regulatory provisions;

(g) Evaluation, including performance testing, by management of the security programme to assess compliance with regulatory requirements, as applicable, and assess performance, including the facility's process for identifying and tracking deficiencies, including performance testing, determining the cause of problems and implementing effective corrective actions to minimize vulnerabilities.

3.6. Information protection

Describe the facility's procedures for ensuring that all correspondence and documentation dealing with security matters is identified and protected accordingly.

3.7. Qualification and training

Describe how the facility ensures that:

(a) All personnel on whom security depends are appropriately trained and qualified;

(b) All employees are informed at least annually of the importance of effective security measures and be trained in their implementation;

(c) Training programmes are routinely evaluated and updated, as necessary.

4. Physical protection measures

4.1. Minimum physical protection measures

Describe the implementation of minimum physical protection measures for uranium at the solution (extraction and concentration process up to the point of precipitation), precipitate (precipitation, concentration and purification) and powder (concentrated material in storage) phases of processing and storage.

4.2. Supplemental physical protection measures: Attractiveness and vulnerability

Describe the implementation of supplemental physical protection measures for uranium at the precipitate (precipitation, concentration and purification) and powder (concentrated material in storage) phases of processing and storage, based on the attractiveness and vulnerability of uranium at those phases.

4.3. Supplemental physical protection measures: Increased threat

Describe the implementation of supplemental physical protection measures for uranium at the precipitate (precipitation, concentration and purification) and powder (concentrated material in storage) phases of processing and storage, based on credible information that the threat to the facility has increased.

5. Inventory control measures

5.1. Minimum inventory control measures

Describe the implementation of minimum inventory control measures for uranium at the solution (extraction and concentration process up to the point of precipitation), precipitate (precipitation, concentration and purification) and powder (concentrated material in storage) phases of processing and storage.

5.2. Supplemental inventory control measures

Describe the implementation of supplemental inventory control measures for uranium at the solution (extraction and concentration process up to the point of precipitation), precipitate (precipitation, concentration and purification) and powder (concentrated material in storage) phases of processing and storage.

6. Contingency plan

Describe the facility's plan for responding to, and countering, unauthorized acts during normal operation, as well as during anticipated security events and other emergency situations that could affect security.

APPENDIX II:

WRITING A TRANSPORT SECURITY PLAN

All transporters (shippers, carriers and consignees) engaged in the transport of UOC requiring the enhanced security level would develop, adopt, implement, periodically review, as necessary, and comply with the provisions of a security plan. The security plan would include at least the following measures and would be modified as needed to reflect the threat level at the time of its application and any changes to the transport programme:

- Specific allocation of responsibilities for security to regulatory and qualified persons with appropriate authority to carry out their responsibilities.
- Provision for keeping records of UOC transported.
- Review of current operations and assessment of vulnerability, including intermodal transfer, storage in transit, handling and distribution, as appropriate.
- Clear statements of measures, including:
    - Training and policies, including response to changes in threat conditions;
    - Verification of new employees and employment;
    - Operating practices (e.g. choice and use of routes where known, use of guards, access to UOC requiring the enhanced security level in temporary storage, proximity to vulnerable infrastructure);
    - Equipment and resources that are to be used to reduce security related risks.
- Effective procedures and equipment for timely reporting and dealing with security related threats or security related incidents.
- Procedures for evaluating and testing security plans and procedures for their periodic review and update.
- Measures to ensure the security of transport information contained in the security plan.
- Measures to ensure that the distribution of sensitive transport information is limited, to maintain security of the information. Such measures would not preclude the provision of transport documents and the consignor's declaration as required by IAEA Safety Standards Series No. TS-R-1.
- Measures to monitor the current location of the shipment at any time.
- Where appropriate, details concerning agreements on the point of transfer of responsibility for security.

It is necessary that responsibility for, and ownership of, the security plan be clearly established. In the event that transports are subcontracted, it may be appropriate to ensure that contractual arrangements exist to develop and comply with a security plan.

Information required in a security plan under these provisions may be incorporated into plans developed for other purposes. However, security plans will, almost invariably, contain information that would be restricted to those who need to know it for the performance of their duties. Such information would not be included in plans that are developed for other purposes and that may be disseminated more widely. When developing security plans, operators and transporters need to ensure that they are coordinated and integrated with emergency response plans (IAEA Safety Standards Series No. GSR Part 7).

APPENDIX III:

DESCRIPTION OF PHYSICAL PROTECTION MEASURES

III.1. ACCESS CONTROL

Facility management and security personnel can implement access control through entry checkpoints, the use of electronic readers or key control measures. Technology, in the form of automatic access control systems (AACSs), is available in various forms, from simple pushbutton mechanical devices to more sophisticated readers that respond to proximity tokens or individual biometric characteristics. Used with a turnstile, an AACS can also incorporate controls to inhibit such practices as 'pass back' and 'tailgating'. In most cases, the use of a card would be verified by a PIN keyed into the reader and in high security situations an AACS entry point would be supervised by a guard positioned within view. The essential factor for prospective operators is to specify a viable AACS that is appropriate to the requirement and that can be supported locally by a manufacturer or installer. It is also important to limit access to the AACS management computers and software to prevent unauthorized interference with the system database. Where conventional lock and key is used as a means of control, locks would be of good quality and key management procedures would be designed to prevent unauthorized access or compromise [5].

III.2. CLOSED CIRCUIT TELEVISION SURVEILLANCE

Closed circuit television is a useful aid that allows security staff to monitor outer approaches and areas where UOC is stored. Cameras can be combined with an intrusion detection system to provide event activated camera views. However, to be fully effective, the performance of closed circuit television cameras and monitors would be regularly assessed to ensure that they continue to display imagery of good quality. Systems would also be supported by a response so that alarm events and indications activated by technology can be investigated.

III.3. COMMUNICATION

Security personnel at all levels would be provided with effective and reliable forms of communication. This includes communication between patrols, fixed posts and the local reporting or control centre and the communication to external agencies responsible for providing rapid response to security events. Carriers would be able to communicate with the shipper and/or operator and to any response agencies. Consideration needs to be given as to whether diverse and redundant communications capability is required. Consideration would be given to special forms of communication when UOC is transported through remote areas.

III.4. FENCES AND GATES

The type of fence used on a perimeter would be appropriate to the threat, the nature of the material being protected and the category of the site overall. There are various types of fence ranging from those that are little more than a demarcation to those that are more robust and can be combined with a fence mounted perimeter intrusion detection and assessment system or electrified panels. Fence lines need to be checked regularly to ensure that the fabric is in good order and free from interference or damage. Gates within a fence would be constructed to a standard comparable to that of the fence and secured with good quality locks.

III.5. INTRUSION DETECTION SYSTEMS

These systems are a useful means of monitoring the security of an unoccupied area. Where appropriate, the technology can be extended to the outer area of an establishment by use of a perimeter intrusion detection and assessment system. All intrusion detection systems would be supported by a response to investigate alarm events or conditions. Alarms can sound remotely at a security control point or locally through a high volume sounder. Closed circuit television can be a

useful aid in providing initial assessment of events within an alarmed zone or area but would normally be backed up by a patrol making a visual check or investigation.

III.6. MAINTENANCE AND TESTING OF SECURITY TECHNOLOGY

Considerable reliance is often placed upon security technology to provide early warning of the entry of an adversary to the site or the secured area. Intruder detection systems used for the protection of radioactive sources would therefore not only be properly specified but also tested for performance upon installation, maintained at regular intervals by regulatory persons and tested at intervals specified by the regulatory body.

III.7. KEY CONTROL PROCEDURES

Keys which allow access to enclosures would be controlled and secured against unauthorized use or duplication. These may be keys to cages, doors, storage containers or shielded units within which sources are used. Similar levels of control would be applied to duplicate and spare keys.

III.8. LOCKS, HINGES AND INTERLOCKS FOR DOORS

Locks used for the protection of enclosures would be of good quality, incorporating features that will offer some resistance to forcible attack. The same applies to hinges on doors. Keys would be safeguarded in the manner outlined above under procedural measures. Within premises, interlock doors that meet safety requirements can serve the interests of security by controlling the movement of personnel and allowing staff to monitor access to the facility.

III.9. PASS SYSTEMS

A pass system is an efficient and cost effective means of providing a first level indication of individual authority to be within a premises or a secured area. Nevertheless, passes would be checked on entry to the facility and worn visibly by holders to confirm authority and aid identification. Embedded technology can also allow passes to be combined for use in AACSs.

III.10. QUALITY ASSURANCE

Security arrangements and procedures would be prepared, documented and maintained in line with recommended quality assurance standards such as: recording of formal approval; version control; periodic, planned review; testing of arrangements and procedures and incorporation of lessons learned into procedures.

III.11. SECURITY AND AREA LIGHTING

Effective illumination of areas can make an important contribution to physical protection. In high security situations, special lighting configurations may be necessary. However, areas that may be in place for other purposes can often provide illumination to deter intruders and assist patrolling response personnel.

III.12. SPECIALIST SECURITY DOORS AND DOOR SETS

Within certain facilities, it may be appropriate to fit storage areas with special security doors and door surrounds that offer resistance to forcible attack. This would be relevant in areas that are regularly left unattended.

III.13. STANDBY POWER

Security control rooms and security systems would be able to cope with power dips or outright loss of a main electricity supply. This can be ensured through an uninterruptible power supply and a standby

generator that automatically starts when a fluctuation in power levels is detected. Battery backup has only limited duration and would, therefore, be viewed as a short term source of standby power.

III.14. WALLS

Unless they are already in place, walls are an expensive way to form a perimeter boundary. Walls also have the disadvantage of preventing response personnel from looking out beyond the areas being protected.

APPENDIX IV

PRACTICAL IMPLEMENTATION OF INVENTORY CONTROL MEASURES

IV.1. THE DRUM EQUIVALENCY CONCEPT

Regulatory bodies would require, and operators would implement, inventory control in a graded approach throughout the process. Engineering and administrative controls to track UOC at the last stages of the process, during storage and during transit will increase as the uranium concentration increases and becomes more vulnerable. As mentioned previously, the advice provided in this publication focuses on a target item that is defined as a single drum of UOC. However, since uranium in process is not yet packaged into a drum, it is necessary to evaluate the application of inventory control measures that are based on an equivalent amount or 350 kg of UOC. When applying the graded approach for inventory control, the operator would take into consideration the quantity of uranium in the process equipment[4], the level of effort and raw materials required to further concentrate the uranium and the amount of time needed to produce/acquire an equivalent amount contained in a single drum. A scalability factor would also be considered if the risk scenario assumes a clandestine operation is very small when compared to the throughput of a large production facility. This type of evaluation will ensure that practical measures are applied across the process that do not place an unnecessary burden or cost on the operator. This approach is considered for the recommendations provided across the various stages of the process identified below under normal operating conditions. A detailed assessment of uranium concentrations per process stage is not required as part of this evaluation. The operator would use average uranium concentrations and equipment volumes to estimate the drum equivalency. This initial evaluation would demonstrate that no additional security measures are required for the process solutions. Supplemental measures would be identified and applied when the State notifies the operator that a credible increase in the threat or risk to a facility or shipment has been identified.

IV.2. ORE

Generally speaking, the minimum uranium concentration needed to produce UOC in an economical manner is approximately 0.3 kg of uranium per tonne of ore. This threshold will vary by facility based on capital investment costs, the costs of raw materials and labour and other economic factors. Some UOC is produced as a by-product of other mining operations. This also impacts the feasibility for recovering uranium. For an open pit mine, the mining operation begins with the removal of the overburden to expose the ore. Once exposed, the ore is drilled, blasted and loaded into a large dump truck. A typical dump truck holds 180 tonnes, or 180,000 kg, of ore. The amount of uranium contained in a single dump truck is approximately 54 kg assuming 0.3 kg of uranium per tonne of ore. The ore is considered solution material. The time and level of effort required to produce the concentrate is of the order of two weeks for a large processing facility where the crushing, milling and processing steps are carried out. The time required for a small scale clandestine operation would certainly exceed the detection goals defined in this publication. Therefore, it is not prudent to require operators to apply supplemental measures for security at this stage of the process. The measures applied to protect the workers, the public and the environment adequately address any security concern.

IV.3. MILLING

Once the ore is removed, it is transferred to the crushing, grinding and milling stages of the process. The refined ore is stored in large stockpiles and fed to the leaching and filtration stage to initiate the uranium recovery process. The uranium concentration for this stage of the process has not changed. The primary difference is that the ore is in a more suitable form for leaching. The material in this form

[4] This does not include uranium contained in tailings or equipment associated with tailings.

is not considered attractive or credible because it would take multiple large transfers for an adversary to remove an amount equivalent to 350 kg of UOC. The uranium at this stage of the process is considered to be solution material. Therefore, it is not prudent to require operators to apply supplemental measures for security at this stage of the process. The measures applied to protect the workers, the public and the environment adequately address any security concern.

IV.4. LEACHING AND FILTRATION

The refined ore in the form of sand is conveyed to the leaching and filtration stage using conveyor systems. The milled ore is leached using a chemical process to dissolve the uranium oxides. Most of the ore is waste material, which is not dissolved. The solids or 'tailings' are separated from the uranium rich, or pregnant, solution by allowing them to settle to the bottom of the leach tanks. The barren sediment from the settling tanks is transferred to the tailings piles. The quantity of uranium at this stage in the process is dependent upon the number and size of the leaching tanks. The concentration of uranium in solution at this stage of the process ranges from 0.05 to 0.2 kgs of uranium per cubic metre (m^3) of solution. A typical tank can have a volume of approximately 1500 m^3. An adversary would have to remove all solution from a single tank to obtain an equivalent quantity of uranium contained in a single drum. This scenario is not considered credible because plant personnel would notice any attempt to divert large quantities of pregnant solution thus providing for timely response to such an event. The uranium at this stage of the process is considered to be solution material. Normal process monitoring, radiological safety, environmental protection and product quality assurance measures are considered sufficient to address unauthorized removal of a drum equivalent at this stage in the process.

IV.5. EXTRACTION AND STRIPPING

The pregnant solution is transferred to the extraction and stripping stage of the recovery process. This stage uses ion exchange and/or solvent extraction to increase the concentration of uranium in solution. This stage of the process uses a series of smaller tanks containing resin beads as part of the ion exchange circuit. This stage of the process increases the concentration of uranium to approximately 5 kg/m^3. The tanks are typically 40 m^3 in volume. Therefore, a single ion exchange tank contains approximately 200 kg of uranium. An adversary would have to remove the entire contents of two columns to achieve an equivalent quantity of uranium contained in a single drum. Instrumentation used to monitor the process would detect such an event resulting in response from the operator. The uranium solution at this stage of the process is considered to be solution material. Normal process monitoring, radiological safety, environmental compliance and quality assurance measures are considered sufficient to address unauthorized removal of a drum equivalent at this stage in the process.

The solvent extraction circuit further increases the concentration of uranium by a factor of three to approximately 15 kg/m^3. The volume of the mixers / settlers or columns will vary by facility. A typical volume for a single tank for this type of equipment is 60 m^3. A single tank could have approximately 700 kg of UOC, assuming 75% of the tank volume is filled. This is approximately equal to two drums of UOC. The uranium at this stage of the process is considered to be in-process pre-target material (See 5.2). It is at this stage of the process that operators and the State regulator would consider implementing recommendations provided in the inventory control tables. It would be noted, however, that many of these recommendations are already required for radiological safety, product quality assurance and environmental compliance. Supplemental measures may be applied if the threat and risk environment increases.

IV.6. PRECIPITATION, FILTRATION AND DRYING

The output from the solvent extraction stage is fed to the precipitation and thickener tanks. It is at this point in the process that the uranium is no longer in solution. Chemicals that are added to the solution cause the uranium to form small solid particles that settle, or precipitate, out of solution. The uranium concentration at this point in the process is approximately 50% solids. A typical volume for a

precipitator tank is approximately 75 m^3. A single tank will have multiple drum equivalents. The only processing required from this point is to press the water out of the slurry and dry the product in the ovens to form U_3O_8. The slurry is commonly dried at very high temperatures in enclosed process equipment. Operators need to wear respiratory protection to access material at this stage. This material is considered to be non-vulnerable, in-process target material. Operators and the State regulator would consider applying the recommendations provided in the inventory control tables, which are considered prudent for this stage. Many of these recommendations are consistent with requirements for radiological safety, worker health and safety and environmental protection measures for the central processing plant. The operator also has measures in place to sample and analyse the precipitate to estimate the quantity of uranium contained at this stage of the process. Supplemental controls to maintain continuity of knowledge for the sample analysis or to detect unauthorized access and removal of the precipitate would be considered.

The precipitated slurry is pumped from the precipitation tanks to a thickening tank. The thickening tank has a conical bottom and rake that slowly moves the thickened precipitate through a tube at the bottom of the tank to the filtration system via another pump. Thickening tanks are typically large open top tanks. The precipitated uranium is easily observed from above the tank. The tanks can be 9 m in diameter and 3 m in height, or approximately 190 m^3. This processing equipment may contain multiple drum equivalents. While access to the tanks is restricted under normal operations, the uranium precipitate is vulnerable if it is in open top tanks. This material is considered to be in-process target material. Operators and the State regulator would consider applying certain recommendations provided in the inventory control tables. Many of these recommendations are consistent with requirements for radiological safety, worker health and safety and environmental protection measures for this stage of the central processing plant. Supplemental administrative controls to detect unauthorized access and removal of the precipitate would be considered, especially for open top thickeners.

The precipitate from the thickeners is generally pumped to a series of filters to de-water, rinse and air dry the precipitate. The design of filter varies by facility. Some filters are contained within a separate room with interlocking doors and enclosed to limit the release of uranium particles into the atmosphere. This design minimizes the potential for uranium uptake by the workers. Some facilities do not place the filters in a separate room. The dewatered precipitate that is now 60% solids may be vulnerable under these operating conditions. The filter operation can have drum equivalent quantities of material that are retained within the process equipment and filters. The filtered precipitate is collected in hoppers that feed the drying circuit of the central processing plant. These hoppers can also have drum equivalent quantities of UOC at this stage. The uranium at this stage is considered to be in-process target material. Operators and the State regulator would consider applying the recommendations provided in the inventory control tables. Many of these recommendations are consistent with requirements for radiological safety, worker health and safety and environmental protection measures for this stage of the central processing plant. Supplemental administrative controls to detect unauthorized access and removal of the precipitate would be considered, especially for filter presses that are not located in a separate room. Administrative controls for containers used to collect loose precipitate would also be considered to reduce the potential for unauthorized removal of UOC prior to drying and packaging.

IV.7. CALCINING

The precipitate is typically dried using a calciner. These units have a small internal volume compared with other processing equipment. The internal volume can range from 8 to 16 m^3. Approximately half of this volume contains UOC. These units are typically designed for a throughput of between 0.5 and 1 metric tonne per day. The product is typically more than 95% U_3O_8. The density of UOC is approximately 8 kg/m^3. Therefore, a single calciner contains between 25 and 65 kg. A single calciner has less than a drum equivalent of UOC. The material at this stage of the process is considered to be in-process target material. The UOC in the calciner is not considered vulnerable because the units operate under vacuum at harmful temperatures. Material does become vulnerable if the units are taken off-line for maintenance. Supplemental administrative controls to detect unauthorized access and

removal of the UOC would be considered when maintenance is performed on the dryers. Administrative controls for containers used to collect loose UOC during the maintenance evolution would also be considered to reduce the potential for unauthorized removal.

IV.8. PACKAGING AND CONTAINERIZATION

It is this stage of the process that the UOC is most attractive and vulnerable. The dried yellowcake in the form of U_3O_8 is containerized (drummed), sampled and weighed. Weights are performed using calibrated scales. The samples are sent to the laboratory where analysis is conducted to determine the uranium concentration and impurities. This information is used to determine if the UOC meets the customers' contract specifications. The individual drums are labelled using stencils, barcodes and/or markings. The information contained on the individual drums would, as a minimum, include the name of the producer, the lot or batch number, the drum number, the tare weight of the drum, the gross weight of the drum and the date of production. The net weight of the UOC can be calculated by subtracting the tare weight of the drum from the gross weight. Radiological measurements to support shipping requirements are also performed on the drums. The drums are also washed to remove any surface contamination prior to loading the drums into the intermodal containers for shipping. Industry may use tamper indicating devices that provide continuity of knowledge after each drum is weighed if this is considered a prudent management practice for certain facilities. Access to the containers and the container contents can be controlled using commercial tamper indicating devices. The UOC at this stage of the process is considered in-process target material because it has not been transferred to the central storage area. Inventory control measures to track the number of drums being filled, cooled and temporarily stored in the drum packaging area would be implemented to ensure unauthorized removal is detected. Simple means of surveillance would also be considered at the drum packaging area. Access to this area would be restricted to employees that are authorized to be in the area. Operators and the State regulator would consider applying the recommendations provided in the inventory control tables. Many of these recommendations are consistent with requirements for radiological safety, worker health and safety and environmental protection measures for this stage of the central processing plant.

Some producers package the UOC in larger transport hoppers. These hoppers are used to transfer approximately four tonnes of UOC to other facilities within the country to further refine the product. These hoppers are weighed, sampled and labelled similar to the drums. The hoppers are also stored in a central area until enough material is accumulated to make up a single shipment. The hoppers have lids that are designed to install simple tamper indicating devices. This provides a simple means of detecting unauthorized access to the hopper contents.

IV.9. CENTRAL STORAGE AREA

The drums or hoppers are moved from the packaging area to a central storage location at the facility. The information for individual drums or hoppers is entered into a facility ledger to track the total quantity of UOC at the facility. The drums are typically stored by batch or lot number. The operator conducts an inventory of all drums and hoppers at a frequency defined by management. The primary reason for taking the inventory is to ensure contractual obligations under customer contracts can be met in accordance with a delivery schedule. A drum of UOC weighing 350 kg (which will contain about 290 kg U) has a commercial value of approximately US $31 000 if the market price is US $90 per kg. A hopper containing four tonnes of UOC at 60% solids is valued at approximately US $210 000. Operators generally keep all filled drums and hoppers in an area that has restricted access. The drums are loaded into 20-foot intermodal (ISO) shipping containers when they are ready for shipment. Locks and tamper indicating devices are applied to the intermodal containers while they are stored at the facility. The UOC at this stage of the process is considered target material in storage. Inventory control measures to track the number of drums (or loaded and sealed shipping containers) in the central storage area would be implemented to ensure unauthorized removal is detected. Simple means of surveillance would also be considered. Access to this area would be restricted to employees that are authorized to be in the area. Operators and the State regulator would consider applying the recommendations provided in the inventory control tables. Many of these recommendations are

consistent with requirements for radiological safety, worker health and safety and environmental protection measures for the central storage area.

IV.10. TRANSPORT

The UOC is most vulnerable during the overland transportation process. It is during this stage that multiple targets are available to potential adversaries. The UOC is in the most attractive form and readily portable. Operators and the State regulator would consider applying the recommendations provided in the transport security tables. Many of these recommendations are consistent with requirements for transport of low specific activity radioactive material via international conveyance.

Drums containing the final product are loaded into 20-foot intermodal shipping containers. These shipping containers have a weight capacity of 21 600 kg. Therefore, the maximum number of drums that can be placed into the shipping container, assuming an average gross weight of 350 kg, is approximately 60 drums. The final product is transported overland by truck or train. Two shipping containers are typically loaded onto a flatbed trailer for transport by truck. Multiple containers can be loaded onto a railcar if the final product is transferred to the port by this means. It is not uncommon for the UOC to be transported overland using a convoy of trucks. The UOC is generally transported only during the day. This requires overnight stops at approved locations if the distance travelled cannot be accomplished in a single day. The inventory control measured listed in Table 2 and the transport security measures listed in Table 3 would be considered if material is placed in interim storage during transport.

Operators work with the port authority and State regulators to minimize the time for storing UOC in shipping containers at the port. Transfers of UOC overland would be coordinated with the arrival of the ships. This reduces the amount of time that UOC is placed into interim storage at the port.

REFERENCES

[1] 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).

[2] INTERNATIONAL ATOMIC ENERGY AGENCY, Uranium Extraction Technology, Technical Report Series No. 359 IAEA, Vienna (1993)

[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, Computer Security at Nuclear Facilities, IAEA Nuclear Security Series No. 17, IAEA, Vienna (2011).

[5] CANDIAN NUCLEAR SAFETY COMMISON, Security of Nuclear Substances: Sealed Sources, REGDOC-2.12.3: http://www.nuclearsafety.gc.ca/eng/acts-and-regulations/regulatory-documents/published/html/regdoc2-12-3/index.cfm

BIBLIOGRAPHY

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

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

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

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

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

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

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

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

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

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

GLOSSARY

competent authority. A governmental organization or institution that has been designated by a State to carry out one or more nuclear security functions. For example, competent authorities may include regulatory bodies, law enforcement, customs and border control, intelligence and security agencies, health agencies, etc.

contingency plan. Predefined sets of actions for response to unauthorized acts indicative of attempted unauthorized removal, including threats thereof, designed to effectively counter such acts.

graded approach. The application of nuclear security measures proportionate to the potential consequences of criminal or intentional unauthorized acts involving or directed at nuclear material, other radioactive material, associated facilities or associated activities or other acts determined by the State to have an adverse impact on nuclear security.

insider. An individual with authorized access to associated facilities or associated activities or to sensitive information or sensitive information assets who could commit or facilitate the commission of criminal or intentional unauthorized acts involving or directed at nuclear material, other radioactive material, associated facilities or associated activities or other acts determined by the State to have an adverse impact on nuclear security.

natural uranium. Uranium (which may be chemically separated) containing the naturally occurring distribution of uranium isotopes (approximately 99.28% uranium-238 and 0.72% uranium-235 by mass). In all cases, a very small percentage of uranium-234 is present.

nuclear security culture. The assembly of characteristics, attitudes and behaviours of individuals, organizations and institutions which serves as a means to support, enhance and sustain nuclear security.

operator. Any person, organization or government entity licensed or authorized to undertake the operation of a nuclear facility.

physical protection regime. A State's regime including:

— The legislative and regulatory framework governing the physical protection of nuclear material and nuclear facilities;

— The institutions and organizations within the State responsible for ensuring implementation of the legislative and regulatory framework;

— Facility and transport physical protection systems.

regulatory body. One or more authorities designated by the government of a State as having legal authority for conducting the regulatory process, including issuing authorizations.

threat assessment. An evaluation of the threats — based on available intelligence, law enforcement and open source information — that describes the motivations, intentions and capabilities of these threats.

two person rule. A procedure that requires at least two authorized and knowledgeable persons to be present to verify that activities involving nuclear material and nuclear facilities are authorized in order to detect access or actions that are unauthorized.

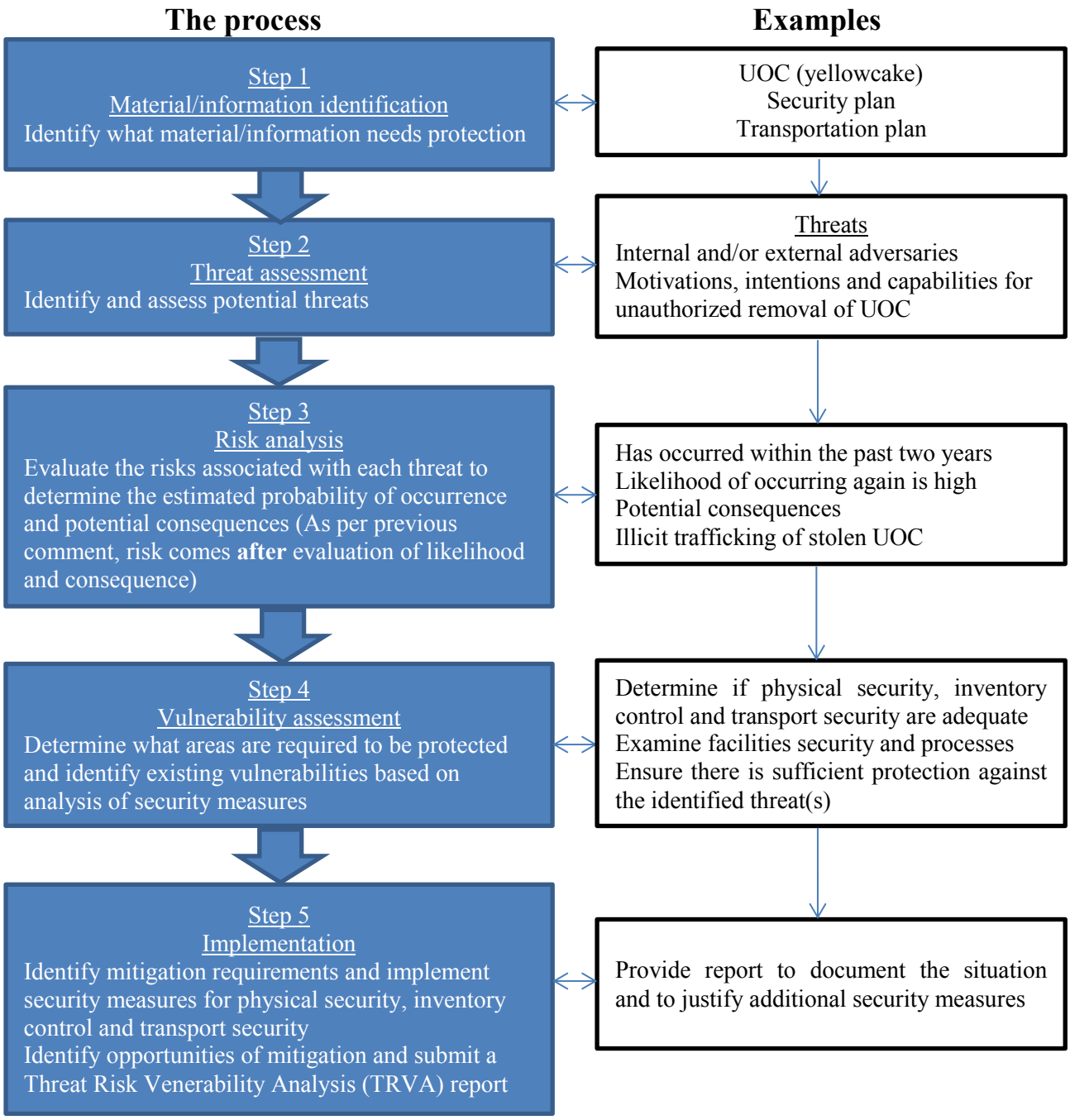
unauthorized removal. The theft or other unlawful taking of radioactive material.

uranium ore concentrate (UOC). Natural uranium occurring in a chemical form derived from uranium extraction, concentration and purification.

ANNEX I

PROCESS STEPS FOR DEVELOPING A RISK BASED APPROACH

The following table outlines the basic steps involved in completing threat, risk and vulnerability assessments, and provides examples for the processing, storage and transportation of UOC.



ANNEX II

REGULATORY PROVISIONS FOR NUCLEAR SECURITY IN THE URANIUM INDUSTRY

II–1. INTRODUCTION

These Regulatory Provisions illustrate a way to implement the IAEA's advice on Nuclear Security in the Uranium Industry.

These Regulatory Provisions are not the only way to implement the advice in this document, but they were chosen to be as clear and simple as possible in view of the particular needs of the States that may wish to use them as a reference in developing their own provisions.

The Regulatory Provisions are designed to help States protect UOC in accordance with prudent management practice by operators, shippers and carriers, through a combination of physical protection measures and inventory control measures.

II–2. SCOPE

As with the underlying advice, the Model Regulatory Provisions apply to processing and storage associated with the concentration of natural uranium into UOC and its subsequent transport. The Model Regulatory Provisions do not apply to exploration, mining, milling, conversion or transport incidental to these activities. The Model Regulatory Provisions are intended to protect UOC against unauthorized removal; they do not address sabotage. Further, these Model Regulatory Provisions do not address inspection against the provisions; States may wish to consider developing guidance for inspectors. Some States may have already implemented some of the content of the Model Regulatory Provisions for safety or for environmental purposes.

The Model Regulatory Provisions incorporate all of the advice in the document that involves implementation by operators, shippers and carriers. The Model Regulatory Provisions do not include advice directed solely at the regulatory body or other competent authorities.

II–3. ASSUMPTIONS

These Regulatory Provisions are predicated on the assumption that the State has established, and is implementing and maintaining, an effective national legislative and regulatory framework for nuclear materials. In short, the assumption is that UOC is already subject to regulatory control for safety, environmental and other purposes and that the State wishes to consider application of additional provisions in order to help protect UOC from unauthorized removal.

II–4. SECURITY CULTURE

A dynamic and effective nuclear security culture would exist and be integrated with the safety culture throughout the natural uranium industry. The characteristics of a nuclear security culture are the beliefs, attitudes, behaviour and management systems, the proper assembly of which lead to more effective security. The foundation of a nuclear security culture is recognition — by those that have a role in regulating, managing or operating facilities or activities involving natural uranium — that a credible threat exists and that security is important.

Safety measures and security measures have in common the aim of protecting human life and health and the environment. Safety measures and security measures would be designed and implemented in an integrated manner so that security measures do not compromise safety and safety measures do not compromise security. In implementing the Model Regulatory Provisions, the designers of security systems would consult with qualified safety experts to ensure that security measures do not compromise the safety of individuals or the protection of the environment.

MODEL REGULATORY PROVISIONS

II–5. GENERAL PROVISIONS

Article 1. Effective date

These provisions shall be effective as of [*date*].

Article 2. Purpose

(1) These provisions specify the means by which operators, shippers and carriers would protect uranium ore concentrate (UOC) from unauthorized removal in processing, storage and transport.

(2) These provisions are intended to complement such other measures as may be appropriate and necessary for health, safety and environmental protection.

Article 3. Scope

(1) These provisions apply to processing and storage of natural uranium associated with the concentration of natural uranium into UOC and its subsequent domestic and international transport.

(2) These provisions do not apply to processing or storage of natural uranium associated with exploration, mining, milling or conversion or to transport incidental to these activities.

(3) These provisions are not intended to protect UOC against sabotage.

Article 4. Fundamental obligation

No person shall engage in the processing or storage of UOC and/or the transport of UOC except in conformance with these provisions.

Article 5. Definitions

Where noted, the definitions have been adjusted from the original source document to be consistent with the scope of these provisions. They may need to be further modified to reflect the terminology and national practice of the State.

Carrier: Any person, organization or government undertaking the carriage of UOC by any means of transport.

Contingency plan: Predefined sets of actions for response to unauthorized acts indicative of attempted unauthorized removal, including threats thereof, designed to effectively counter such acts.

Delay: The element of a physical protection system designed to increase the time required for an adversary to gain unauthorized access to, or to remove UOC, generally through barriers or other physical means.

Detection: A process in a physical protection system that begins with sensing a potentially malicious or other unauthorized act and that is completed with the assessment of the cause of the alarm.

Graded approach: The application of security measures which are proportional to the consequences of a malicious act.

Guard: A person who is entrusted with responsibility for patrolling, monitoring, assessing, escorting individuals or transports, controlling access and/or providing initial response.

Malicious act: An act or attempt of unauthorized removal of UOC

Nuclear security culture: The assembly of characteristics, attitudes and behaviours of individuals, organizations and institutions, which serve as means to support, enhance and sustain nuclear security.

Operator: Any person, organization or government entity licensed or authorized to undertake the operation of a facility where natural uranium is processed or stored.

Security event: An event that is assessed as having implications for nuclear security that would be addressed.

Shipper: Any person, organization or government entity that prepares or offers a consignment of UOC for transport (i.e. the consignor).

Threat: A person or group of persons with motivation, intention and capability to commit a malicious act.

Unauthorized removal: The theft or other unlawful taking of UOC.

Article 6. Regulatory inspection of premises and information

Operators, shippers and carriers shall provide representatives of [*regulatory body*] with immediate access to premises, facilities and vehicles in order to obtain information about the status of security and verify compliance with these provisions. Upon request, each operator, shipper and carrier shall make available to [*regulatory body*] information and records regarding security.

Article 7. Reporting of events

(1) In the event of any failure to comply with any of these provisions, operators, shippers and carriers shall:

(a) Report to [*regulatory body*] within 24 hours;

(b) Take appropriate action to remedy the circumstances and to prevent a recurrence of similar situations;

(c) Investigate the failure and its causes, circumstances and consequences;

(d) Within 30 days, or as required, provide [*regulatory body*] with a report on the causes of the failure, its circumstances and consequences, and on the corrective or preventative actions taken or to be taken.

(2) Whenever a situation involving the loss of control of, unauthorized access to, or actual or attempted unauthorized removal of, UOC has occurred or is occurring, operators, shippers and carriers shall:

(a) Immediately inform [*regulatory body*] and local law enforcement bodies;

(b) Take appropriate action to remedy the circumstances and to prevent a recurrence of similar situations;

(c) Investigate the event and its causes, circumstances and consequences;

(d) Within 30 days, or as required, provide [*regulatory body*] with a report on the causes of the event, its circumstances and consequences, and on the corrective or preventative actions taken or to be taken.

(3) Failure to take corrective or preventative actions within a reasonable time in accordance with these provisions shall be grounds for enforcement in accordance with Article 8.

Article 8. Enforcement

A licence may be revoked, suspended or modified, or the possession or transport of UOC may be prohibited, upon finding by [*regulatory body*] of non-compliance with these provisions. Operators, shippers and carriers are subject to fines for non-compliance with applicable provisions commensurate with the nature of the infraction. Wilful violations or attempted violations of the provisions may be referred to [*national justice authority*] for prosecution under national criminal statutes and codes.

Note: Sanctions may be included in this Article 8 if provided for in applicable legislation and consistent with national practice.

II–6. SECURITY PROGRAMME

Article 9. Responsibilities of operators, shippers and carriers

(1) Operators, shippers and carriers shall bear the responsibility for establishing and implementing a programme for ensuring the security of UOC for which they are responsible and for complying with these provisions. They may appoint and shall specifically identify other persons to carry out actions and tasks related to this responsibility, but operators, shippers and carriers shall themselves retain the responsibility for the actions and tasks.

(2) Operators, shippers and carriers shall notify [*regulatory body*] of their intention to introduce any modification to facilities or activities affecting the security of UOC for which they are responsible, and shall not carry out any such modification unless specifically authorized by [*regulatory body*].

Article 10. Security policy

Operators, shippers and carriers shall develop a policy statement that demonstrates their commitment to comply with these provisions.

Article 11. Security management

Operators, shippers and carriers shall establish a nuclear security management system that includes provision for:

(1) Clearly identifying the responsibilities of each individual for security and ensuring that each individual is suitably trained and qualified;

(2) Defining clear lines of authority for decisions on security;

(3) Ensuring adequate resources (personnel and funding) for the security programme;

(4) Developing procedures, policies, records and plans for the security programme and for an effective nuclear security culture;

(5) Developing procedures for the proper handling of sensitive information and protecting it against unauthorized disclosure.

Article 12. Security functions

Operators, shippers and carriers shall employ the defence in depth principle in the design of a security system that conforms to Articles 19–31 of these provisions, as applicable, and performs the basic security functions of detection, delay and response.

Article 13. Nuclear security culture

Operators, shippers and carriers shall promote an effective nuclear security culture by ensuring that:

(1) Policies and procedures are established that identify security as being of the highest priority.

(2) Problems affecting security are promptly identified and corrected in a manner commensurate with their importance.

(3) Organizational arrangements and lines of communications are established that result in an appropriate flow of information on security at and between the various levels in the entire organization of the operator, shipper or carrier.

Article 14. Security plans: Administrative controls and procedures

(1) Operators and shippers shall develop and implement security plans for the management of UOC in processing, storage and transport, as applicable.

(2) The security plan shall include a contingency plan.

(3) The security plan shall form part of the operator’s or shipper’s overall business management system and shall cover normal operational activities as well as anticipated security events.

(4) Each operator and shipper shall identify an individual who is responsible for the implementation and periodic exercise, review and revision of their respective security plans.

(5) Operators and shippers shall develop administrative controls and procedures to identify the roles and responsibilities of key personnel for the physical protection measures, inventory control measures and transport security measures, as applicable, and to respond to and report such nuclear security events, including reporting to off-site first responders. Procedures shall also provide specific security related instructions to all personnel involved in processing, storage and transport of UOC.

Article 15. Quality assurance

Operators and shippers shall implement an independent quality assurance programme which verifies and ensures that all aspects of the operator's or shipper's security programme is functioning in accordance with the security plan and in compliance with all applicable regulatory provisions. The quality assurance programme shall address the following areas:

(1) Security management and functions;

(2) Personnel training and qualifications;

(3) Quality improvement;

(4) Control of documents and records;

(5) Control of work processes;

(6) Compliance of the security programme with applicable regulatory provisions;

(7) Evaluation, including performance testing, by management of the security programme, as further provided in Article 16.

Article 16. Evaluations

(1) Operators and shippers shall conduct regular evaluations of their security programmes to assess and sustain conformance with these provisions and to assess its effectiveness.

(2) The evaluations shall be coordinated through the operator's or shipper's quality assurance organization, and shall include a process for identifying and tracking deficiencies, including performance testing, determining the cause of problems and implementing effective corrective actions to minimize vulnerabilities.

(3) The evaluation process shall be documented in the security plan.

Article 17. Information protection

(1) Operators and shippers shall protect all sensitive information pertaining to security matters pursuant to applicable State regulations through:

   (a) Procedures to ensure that such information is reliably identified;

   (b) A requirement that access to such information be limited to personnel with a need to know, whose trustworthiness has been verified;

   (c) Measures for the handling and control of such information, addressing document and information storage, transmission, reproduction and destruction.

(2) The security plan shall document compliance with these requirements.

Article 18. Qualification and training

(1) Operators, shippers and carriers shall ensure that all personnel on whom security depends are appropriately trained and qualified so that they understand their responsibilities and can perform their duties by exercising appropriate judgement and according to defined procedures. Such personnel shall be periodically retrained or re-qualified, as necessary.

(2) All employees shall be informed at least annually of the importance of effective security measures and be trained in their implementation.

(3) Training programmes shall be routinely evaluated and updated as necessary.

II–7. PHYSICAL PROTECTION MEASURES

Article 19. Minimum physical protection measures for solution, precipitate and powder

Except as otherwise indicated, operators shall establish and implement the following minimum physical protection measures for UOC at the solution (extraction and concentration process up to the point of precipitation), precipitate (precipitation, concentration and purification) and powder (concentrated material in storage) phases of processing and storage:

(1) Administrative controls that restrict access to authorized personnel at the site boundary, including procedures for identifying and controlling visitor access;

(2) Administrative controls to ensure that process monitoring systems that are also used for security purposes are not compromised by any changes in facility design (solution and precipitate only);

(3) Signs and postings that provide notification that access to the area is restricted to authorized personnel and that access to the area could expose individuals to chemical and radiological hazards;

(4) Manned or unmanned barriers such as fences, gates and entry control points that identify a defined exterior boundary for the facility or critical areas within the facility;

(5) Visual inspections of the process and storage areas to detect access by unauthorized personnel, unauthorized access to the process systems or storage areas and components or other anomalous conditions;

(6) Detection assessment procedures and response arrangements.

Article 20. Supplemental physical protection measures for precipitate and powder

Operators shall establish and implement the following supplemental physical protection measures for UOC at the precipitate (precipitation, concentration and purification) and powder (concentrated material in storage) phases of processing and storage when the appropriate State competent authority has indentified that UOC is at increased risk of unauthorized removal and has communicated such to the operator:

(1) Administrative controls that restrict access to process components containing UOC, covering both normal operation and maintenance activities.

(2) Administrative controls that require the use of approved vehicles to move UOC within the defined boundary of the site.

(3) Administrative controls that require the use of approved containers for storage and transport of UOC and which prohibit the use of these containers for any other purpose.

(4) Industrial surveillance cameras to monitor process components containing concentrated cakes or powders and drums in the packaging and storage areas.

(5) Independent verification of access authorization to the drum packaging area, drum storage area and the transport container storage area.

(6) Detailed procedures for additional measures which can be quickly implemented in a structured manner when [*regulatory body or other competent authority*] provides notice of an increased threat level or a specific threat. Such measures may include:

   (a) Radiological surveys of all equipment and personnel exiting the facility;

   (b) Administrative requirement to have two people in the drum packaging and storage areas;

   (c) Restriction of access to essential personnel and vehicles;

   (d) Notification and coordination with local law enforcement;

(e) Increased surveillance measures.

Article 21. Supplemental physical protection measures for solution and precipitate

Operators shall establish and implement the following supplemental physical protection measures for UOC at the solution (extraction and concentration process up to the point of precipitation) and precipitate (precipitation, concentration and purification) phases of processing and storage when the appropriate State competent authority has indentified that UOC is at increased risk of unauthorized removal and has communicated such to the operator:

(1) Performance testing with documentation which verifies that process monitoring equipment used for security purposes is properly maintained and tested to meet its design specifications;

(2) A tamper indicating device to detect unauthorized access to process equipment and drums (precipitate only).

Article 22. Supplemental physical protection measures for powder

Operators shall establish and implement the following supplemental physical protection measures for UOC at the powder (concentrated material in storage) phase of processing and storage when the applicable State competent authority has indentified that UOC is at increased risk of unauthorized removal and has communicated such to the operator:

(1) Administrative controls that limit the number of full drums in the product packaging area;

(2) Physical barriers that restrict access to the drum and transport container storage area to authorized personnel, such as robust fencing, lockable doors, gates and block walls;

(3) A tamper indicating device to detect unauthorized access to UOC in storage and during transport.

II–8. INVENTORY CONTROL MEASURES

Article 23. Minimum inventory control measures for solution, precipitate and powder

Except as otherwise indicated, operators shall establish and implement the following minimum inventory control measures for UOC at the solution (extraction and concentration process up to the point of precipitation), precipitate (precipitation, concentration and purification) and powder (concentrated material in storage) phases of processing and storage:

(1) Methods and procedures to evaluate the inventory control programme to sustain effective performance;

(2) Quality assurance procedures which demonstrate that the facility process monitoring equipment is maintained and is capable of detecting unauthorized removal (precipitate only);

(3) A qualified sampling and analysis programme to accurately determine UOC inventory and throughput (solution and precipitate only);

(4) Use of calibrated scales, which are regularly recalibrated, to determine accurately the mass of UOC in drums (powder only);

(5) Methods and procedures to estimate the bulk process inventory (precipitate and powder only);

(6) Administrative controls to balance raw material consumption against the number of drums produced over a defined period of time (precipitate and powder only);

(7) Information management systems that track the location and quantity of UOC in process and storage, such information to be protected in accordance with information protection procedures;

(8) Administrative controls to investigate and resolve indications of unauthorized removal of UOC (precipitate and target storage only);

(9) Duplicate samples of the final product for independent analysis to resolve inconsistencies between the shipper and receiver (precipitate and powder only);

(10) Unique identification of each drum and shipping container of UOC with a durable form of marking (precipitate and powder only).

Article 24. Supplemental inventory control measures for precipitate and powder

Operators shall establish and implement the following supplemental inventory control measures for UOC at the precipitate (precipitation, concentration and purification) and powder (concentrated material in storage) phases of processing and storage when the appropriate State competent authority has indentified that UOC is at increased risk of unauthorized removal and has communicated such to the operator:

(1) Independent assessment of the sampling and analysis programme by an organization external to the facility;

(2) An inventory control plan that clearly defines control measures to detect and resolve indicators of unauthorized removal;

(3) Administrative controls to restrict removal of UOC using unauthorized pathways (e.g. sanitary waste containers, construction debris).

Article 25. Supplemental inventory control measures for precipitate

Operators shall establish and implement the following supplemental inventory control measures for UOC at the precipitate (precipitation, concentration and purification) phase of processing and storage when the appropriate State competent authority has indentified that UOC is at increased risk of unauthorized removal and has communicated such to the operator:

(1) Administrative controls to prevent unauthorized removal of UOC during maintenance activities where UOC is directly accessible;

(2) Administrative or technical controls that independently verify the number of drums filled over a defined period of time, such as a shift.

Article 26. Supplemental inventory control measures for powder

Operators shall establish and implement the following supplemental inventory control measures for UOC at the powder (concentrated material in storage) phase of processing and storage when the appropriate State competent authority has indentified that UOC is at increased risk of unauthorized removal and has communicated such to the operator:

(1) Administrative controls to track movement of drums between the process packaging area and the drum storage area and to document transfers of drums from the facility to the transporter;

(2) Routine drum inventories to detect unauthorized removal from the storage area;

(3) Administrative procedures to receive, distribute and track tamper indicating devices.

II–9. TRANSPORT SECURITY MEASURES

Article 27. Minimum transport security measures for material in transit or intermediate storage

Operators, shippers and carriers shall establish and implement the following minimum transport security measures for UOC in transit and in intermediate storage during transport:

(1) Restriction of access to shipping information to individuals that have a need to know;

(2) Contingency plans for transport and interim storage locations developed in coordination with [*the regulatory body and other applicable competent authorities*] to address unexpected delays due to accidents, natural disasters, social unrest or other occurrences;

(3) Industrial packages, shipping containers and labelling in compliance with all international standards for transport of UOC, including IAEA Safety Standards Series No. TS-R-1, Regulations for the Safe Transport of Radioactive Material;

(4) Trustworthiness determinations for all personnel involved in the transport and intermediate storage of UOC;

(5) Application of tamper indicating devices to all shipping containers, each with a unique identification, and procedures to control and track tamper indicating devices for each shipping container;

(6) Administrative controls to investigate and resolve indications of unauthorized removal of UOC.

Article 28. Minimum transport security measures for material in transit

Operators, shippers and carriers shall establish and implement the following minimum transport security measures for UOC in transit:

(1) Administrative controls and transport personnel training on reporting procedures associated with accidents and/or transport delays;

(2) Use of primary, and alternative if available, transport routes approved by [*regulatory body or other competent authority*];

(3) Administrative controls that prohibit transportation of other cargo with UOC in the same shipping container or on the same conveyance;

(4) Determination of the gross weight of each container and verification of this weight, when possible, during transport and upon receipt;

(5) Transport vehicle and transport personnel communications capabilities to facilitate immediate reporting of activities that put UOC at increased risk;

(6) Evaluation of the contents of each shipping container by the receiver within [*specify time period*] following receipt to identify any shipper–receiver differences;

(7) Procedures to address identified shipper–receiver differences, including immediate notification by the receiver to the shipper and the [*regulatory body or other competent authority*] of any differences;

(8) Pre-shipment inspection of all transport security measures in accordance with the transport security plan.

Article 29. Minimum transport security measures for material in intermediate storage

Operators, shippers and carriers shall establish and implement the following minimum transport security measures for UOC in intermediate storage during transport:

(1) Administrative controls which require drums and shipping containers of UOC to be physically segregated from other cargo when in interim storage;

(2) Administrative controls to verify the serial number and tamper indicating device number for each shipping container at interim storage locations.

Article 30. Supplemental transport security measures for material in transit

When [*regulatory body or other competent authority*] indicates that a targeted, credible increased threat is identified, operators, shippers and carriers shall establish and implement the following supplemental transport security measures for UOC in transit:

(1) Joint exercise of contingency plans on a periodic basis to ensure that the operator, shipper, transport company, response force and [*regulatory body and/or other competent authorities*] can respond in a timely and effective manner to a security event during transit;

(2) Implementation of compensatory security measures when UOC is placed in temporary storage for extended periods of time owing to transit disruptions;

(3) Monitoring of progress of transport by road using periodic communication, such as radio or mobile phone, or electronic tracking, such as global positioning systems, as defined in the transport security plan;

(4) Implementation of a two person rule for transport of UOC by road, as defined in the transport security plan;

(5) Consideration of security escorts to address specific threats as prescribed in the transport security plan.

Article 31. Supplemental transport security measures for material in intermediate storage

When [*regulatory body or other competent authority*] indicates that a targeted, credible increased threat is identified, operators, shippers and carriers shall establish and implement the following additional transport security measures for UOC in intermediate storage:

(1) Levels of protection for interim storage facilities used to store UOC to be equivalent to the levels of protection for UOC in storage at the producer, adjusted to address local threat conditions;

(2) Periodic inspections by the owner/operator of the interim storage facility to ensure security measures are in place for receipt of UOC;

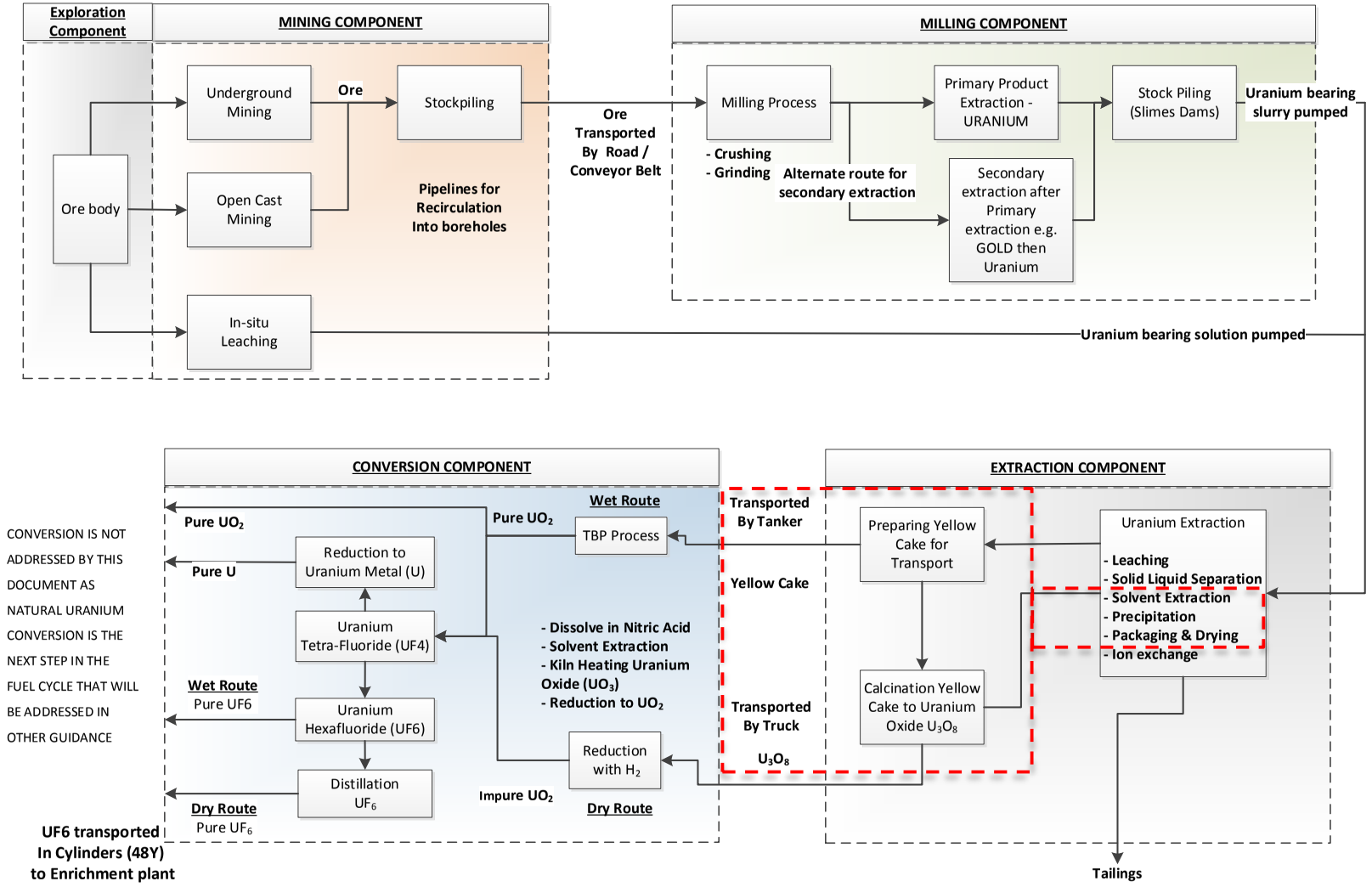
(3) Joint exercise of contingency plans on a periodic basis to ensure that the operator, shipper, transport company, response force and [*regulatory body and/or other competent authorities*] can respond in a timely and effective manner to a security event during intermediate storage;

(4) Implementation of compensatory security measures when UOC is placed in temporary storage for extended periods of time owing to transit disruptions;

(5) Security patrols at interim storage areas to monitor for unauthorized access and/or unauthorized removal of UOC.

ANNEX III:

OVERVIEW OF PROCESS FLOWS FOR THE FRONT END OF THE NUCLEAR FUEL CYCLE AND APPLICABILITY OF THIS DOCUMENT TO THIS PORTION OF THE FUEL CYCLE



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

15-37541

International Atomic Energy Agency
Vienna
ISBN 978–92–0–110815–9