IAEA NUCLEAR SECURITY SERIES No. XX

STEP 8 Soliciting comments by Member States (revision of Implementing Guide NSS 23-G)

Information Security for Nuclear Security

DRAFT IMPLEMENTING GUIDE

INTERNATIONAL ATOMIC ENERGY AGENCY
VIENNA, 20XX

CONTENTS

1. INTRODUCTION

BACKGROUND

1.1. Paragraph 3.3 of IAEA Nuclear Security Series No. 20, Objective and Essential Elements of a States' Nuclear Security Regime [1] states that:

> "The legislative and regulatory framework, and associated administrative measures, to govern the nuclear security regime:
>
> (g) Provide for the establishment of regulations and requirements for protecting the confidentiality of sensitive information and for protecting sensitive information assets.
>
> (h) Ensure that prime responsibility for the security of nuclear material, other radioactive material, associated facilities, associated activities, sensitive information and sensitive information assets rests with the authorized persons."

1.2. Paragraph 3.9 of Ref. [1] states that:

> "A nuclear security regime uses risk informed approaches, including in the allocation of resources for nuclear security systems and nuclear security measures and in the conduct of nuclear security related activities that are based on a graded approach and defence in depth, which take into account the following:
>
> (d) Potential harmful consequences from criminal or intentional unauthorized acts involving or directed at nuclear material, other radioactive material, associated facilities, associated activities, sensitive information or sensitive information assets, and other acts determined by the State to have an adverse impact on nuclear security."

1.3. With regard to international cooperation and assistance, para. 3.6 of Ref. [1] states that:

> "A nuclear security regime provides for cooperation and assistance between and among States, either directly or through the IAEA or other international organizations, by:
>
> (e) Ensuring through appropriate arrangements that sensitive information or other information exchanged in confidence is adequately and appropriately protected."

1.4. IAEA Nuclear Security Series Nos 13, Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5) [3]; 14, Nuclear Security Recommendations on Radioactive Material and Associated Facilities [4]. and 15, Nuclear Security Recommendations on Nuclear and Other Radioactive Material out of Regulatory Control [5] provide recommendations on the protection of sensitive information.

1.5. Groups or individuals wishing to plan or commit a criminal or other intentional unauthorized act involving nuclear material or other radioactive material or associated facilities could benefit from acquiring, modifying or denying access to sensitive information. Sensitive information is "information, in whatever form, including software, the unauthorized disclosure, modification, alteration, destruction, or denial of use of which could compromise nuclear security" [2].

1.6. This Implementing Guide provides guidance on information security for nuclear security and its interfaces with nuclear safety.

1.7. Some sensitive information is controlled, stored, processed or communicated through computer based systems (i.e. sensitive digital assets). IAEA Nuclear Security Series No. 42-

G, Computer Security for Nuclear Security [6], provides further guidance on addressing computer security utilizing a graded approach based on the severity of potential consequences for protecting the confidentiality, integrity, and availability of computer based systems, the compromise of which could adversely affect nuclear security or nuclear safety.

1.8. The terms used in this publication are to be understood as explained in the IAEA Safety and Security Glossary [2], unless otherwise stated in the text.

1.9. This publication supersedes IAEA Nuclear Security Series No. 23-G, Security of Nuclear Information[1].

OBJECTIVE

1.10. This publication provides guidance on applying the principles of information security to support a State's nuclear security regime.

1.11. This publication provides guidance on:

(a) Establishing effective state legislative, policy and regulatory frameworks for maintaining the confidentiality, integrity and availability of sensitive information;
(b) Identifying and classifying sensitive information and related information assets;
(c) Information security measures for the life cycle of sensitive information;
(d) Establishing and managing an organization's information security programme.

1.12. A considerable amount of national and international guidance exists concerning the establishment and management of information security measures for various types of information. This publication does not intend to replace either high level guidance or detailed standards. This publication complements existing regulations, guidance and standards on information security by providing States with detailed information on concepts and considerations that apply to nuclear security, and by outlining the particular provisions and conditions for information security within a nuclear security regime.

SCOPE

1.13. This Implementing Guide provides guidance on information security for nuclear security, and its interfaces with nuclear safety, and with other elements of a State's nuclear security regime, such as the physical protection of nuclear material and nuclear facilities, the security of radioactive material and associated facilities and activities, and the detection of and response to nuclear security events.

1.14. This publication addresses the security of sensitive information for civil uses of nuclear material, other radioactive material, and associated facilities and activities. It focuses on sensitive information relating to the nuclear security of material and facilities that are under regulatory control. Information within a nuclear security regime that is considered valuable for the operations of the entity holding such information or for its finances, but that is not considered sensitive in terms of nuclear security or its interfaces with nuclear safety, is outside the scope of this publication.

1.15. The general guidance provided in this publication can be used, as applicable, to sensitive information relating to nuclear and other radioactive material out of regulatory control.

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

1.16. The intended audience for this publication is all those who are responsible for the security of sensitive information, for example, competent authorities, including regulatory bodies; management in facilities, companies or organizations involved in the use, storage or transport of nuclear material or other radioactive material; response organizations for nuclear or radiological emergencies, facility operators and personnel, designers, vendors and in particular security personnel; contractors or other third parties working for competent authorities, organizations or facility operators; or any other entities that have been given legitimate access to sensitive information.

STRUCTURE

1.17. Section 2 introduces key terms and concepts for information security. Section 3 describes the elements necessary to build a framework for the security of sensitive information within a State. Section 4 presents considerations for determining which information can be considered sensitive information and would therefore need to be managed as such. Section 5 contains considerations for the sharing and disclosure of sensitive information. Section 6 describes the necessary actions at the regulated entity or competent authority for managing and operating measures to secure sensitive information. Annex I provides an example of a classification system for sensitive information. Annex II provides examples of sensitive information in a nuclear security context. Annex III presents an example of an information security training programme.

2. INFORMATION SECURITY CONCEPTS

2.1. This section clarifies the meaning of important terms that are used in this publication. It also indicates how the key concepts of information security are to be applied to the context of nuclear security.

2.2. Information security is the preservation of the confidentiality[2], integrity[3] and availability[4] of information in any form.

2.3. Protection against adversary actions that could affect the confidentiality, integrity, or availability of sensitive information should be ensured to maintain nuclear security and its interfaces with nuclear safety, such as protection of sensitive information relied on by nuclear safety systems and measures for the correct performance of a nuclear safety function.

2.4. A State's legislative and policy frameworks and the information security management system of a competent authority or regulated entity should reflect the information security measures and activities necessary to support the nuclear security regime, as some functions (e.g. the safe operation of nuclear facilities) directly relevant to the State's nuclear security objectives rely upon the confidentiality, integrity and availability of sensitive information, as illustrated in Figure 1.

[2] The property that information is not made available or disclosed to unauthorized individuals, entities or processes [2].

[3] The property of accuracy and completeness of information [2].

[4] The property of being accessible and usable upon demand by an authorized entity [2].

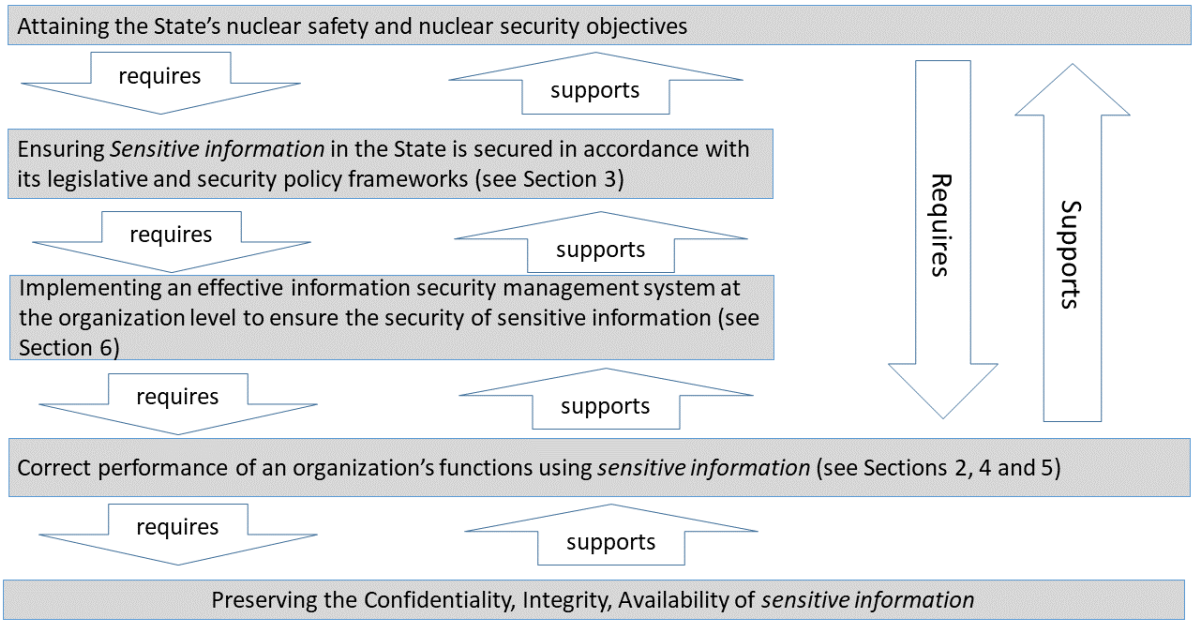

FIG. 1. Relationship between the State's nuclear security objectives, information security governance structures and the confidentiality, integrity and availability of information (adapted from Ref. [6]).

INFORMATION, INFORMATION OBJECTS AND INFORMATION ASSETS

2.5. An information object is "knowledge or data that have value to the organization" [2]. Information objects can be tangible physical or digital collections of information on paper, on film, on magnetic or optical media, in charts, in documents, in software executables, and in other forms and channels for transferring information.

2.6. For security purposes, effective management of information and convenience to the users and handlers of information, information can be grouped into information objects. Information objects share the following characteristics:

(a) The information within an information object shares a common usage, purpose, associated risk and form of storage or transmission;
(b) The information object has context (i.e. information that supports identifying it's use and value) that is sufficient to allow the associated information to be assessed;
(c) The information object can be labelled, enabling the application of targeted security controls applied to protect it proportionately.

2.7. The distinction between 'information' and 'information objects' is important because it might be difficult or less cost effective to manage information in a form in which it lacks clear context and meaning. It is only when the information can be treated as an information object (i.e. is tangible, can be labelled and is in the appropriate context, can be viewed) that practical measures for information management can be used. Information security risks can arise when sensitive information without labels and without sufficient context is shared by individuals who do not understand its potential value, for example when the information is exchanged through casual conversations. In some cases, context can be inferred when enough information is shared or obtained, even if the context is not explicitly provided.

2.8. Information assets are any equipment or components that are used to store, process, control or transmit information. Information assets might contain one or more information

objects, and/or multiple pieces of information and perform a function or contribute to a function utilizing information or information objects.

2.9. Information assets, which include control systems, networks, and information systems, actively facilitate the handling, management, and utilization of information objects through various operations such as storing, processing, controlling, or transmitting information, and while many use digital technology, some information assets perform these actions without digital technology (e.g. safes with mechanical locks).

2.10. Individuals can perform actions relating to the storage, control, transmission or processing and subsequent utilization of information contained in its abstract form, utilizing information objects or information assets. Individuals and information assets can also interact in order to act on, modify or create new information or represent information in information objects.

2.11. Decisions made and actions taken by individuals, on the basis of information in whatever form, can have some significance for the functions performed relevant to nuclear security. Raw signal information from sensors, information objects containing procedures and set points, and information assets displaying this information will all contribute to decisions made by individuals.

2.12. Figure 2 illustrates a conceptual model that begins with information on the left and demonstrates its relationship to information objects, information assets, individuals and the functions performed. The diagram should be read from left to right, following the arrows to indicate that information can be represented in information objects which are used or processed by individuals and information assets, who or which can take action to affect the functions performed or other information.

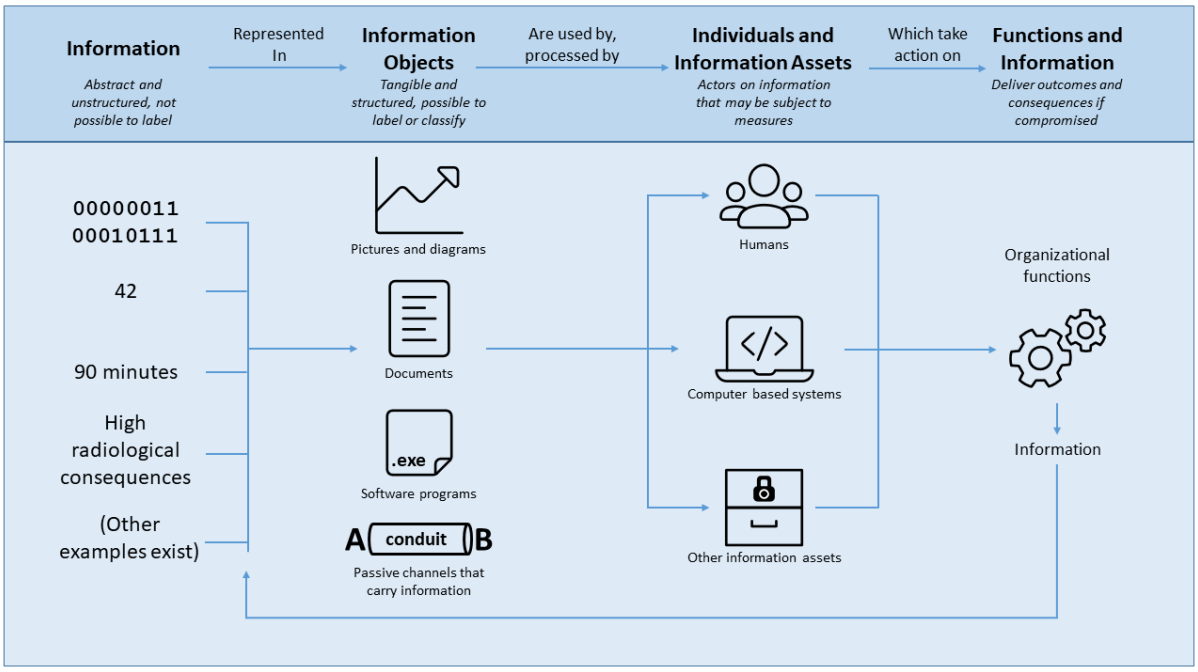

FIG. 2. Conceptual information model illustrating the relationship of information to information objects, information assets and the functions performed, with examples.

2.13. An adversary might seek to provoke a consequence by affecting the functions performed in the final column of Fig. 2. The adversary can have this effect by acting on information, information objects, information assets or individuals relating to that specific function. However, conventional information security measures can generally only be applied to

information objects, information assets, and individuals in an effort to protect the relevant functions. It is difficult to apply targeted and effective information security measures to protect information in its abstract form, without context and without the labels to convey its value.

2.14. For information security for nuclear security, any or all of the entities listed below can attribute value to information objects and information assets, when the information they contain contributes to the performance of nuclear security related functions:

(a) The State;
(b) Other States;
(c) Competent authorities and regulatory authorities with functions relevant to nuclear security;
(d) Technical support organizations;
(e) Facility operators (including third parties, such as vendors);
(f) Potential adversaries (e.g. individuals, organized entities);
(g) The media;
(h) The public.

2.15. Each entity could have a different perception of the value of information, information objects and information assets. For instance, detailed information on the configuration of a safety control system could be considered by the facility operator to be an inconsequential part of routine operations. To a potential adversary, however, it could reveal a weakness or vulnerability that could be exploited in the context of a criminal or other intentional unauthorized act.

2.16. It is important to note that an adversary could create or modify information, information objects and information assets for criminal or other intentional unauthorized purposes. The latter could include attacks that are specifically designed and executed to mislead human or machine based decision making. This type of attack should be considered when protecting information on the basis of which decisions are made.

SENSITIVE INFORMATION

2.17. Sensitive information can be used by an adversary in the conduct of criminal or intentional unauthorized acts targeting nuclear material, nuclear facilities, radioactive material, and their associated facilities and activities. Such information can also be used to undermine the detection of and response to nuclear security events, as well as to compromise the security of nuclear material or other radioactive material during transport.

2.18. The information necessary for the performance of a function important to safety, security or nuclear material accountancy and control can be considered as sensitive. Sensor values that are used to ensure the nuclear safety function to control reactivity, for example, are likely to be considered sensitive information. Sensitive information could also describe vulnerabilities that an adversary could exploit to undermine those functions. For example, the sensor values that are used to ensure the nuclear safety function to control reactivity might be converted using a calibration table, which is used in the case of multiple sensors that serve different purposes. If the calibration table is manipulated, multiple functions could be adversely affected, which means that both the sensor data the calibration table, the calibration algorithm, and any associated set points should be assessed as sensitive information.

2.19. While confidentiality is often seen as the primary concern in relation to sensitive information, loss of integrity or of availability can also have negative consequences for nuclear security. For example, if individuals or information assets do not have timely access

to the necessary sensitive information (i.e. a loss of availability), or if the sensitive information has been altered in a way that misleads individuals or information assets (i.e. a loss of integrity), it can prevent the individuals or information assets from correctly performing their functions, and potentially lead to a nuclear security event or a nuclear accident.

2.20. The following are examples of sensitive information in nuclear safety and security:

(a) Information relating to the control of important physical processes relevant to nuclear security and its interfaces with nuclear safety;
(b) Descriptions of nuclear security arrangements at a facility;
(c) Software applications or communications (e.g. network communications, process signalling) important to the performance of safety functions, security functions and of functions relating to nuclear material accounting and control;
(d) Details on the location or the transport of nuclear material or other radioactive material;
(e) Information concerning vulnerabilities in arrangements at ports and airports for the detection of material out of regulatory control;
(f) Details of an organization's personnel with authorized access to nuclear or radioactive materials;
(g) Details of essential equipment and systems;
(h) Details of a weakness in a system of minor importance that would indicate the presence of the same weakness in a system of greater importance for safety or security.

2.21. Identifying which information can be considered 'sensitive' is a key step in establishing and managing an information security management system in order to ensure the confidentiality, integrity and availability of sensitive information. Guidance on assessing and classifying sensitive information is provided in Section 4, and illustrative examples are provided in Annex II.

2.22. Maintaining the confidentiality, integrity and availability of sensitive information is crucial because having easy access to inadequately secured information, or being able to easily modify such information, can facilitate the efforts of adversaries to plan or commit criminal or other intentional unauthorized acts. If, for example, an adversary attempting the theft of nuclear material acquires the security plan of a facility, the adversary could gain knowledge of physical protection barriers, the guards and whether the guards are armed, the size of the response force and the estimated time that it would take the response force to arrive on-site. This same security plan would indicate the location of important targets within the facility and the established security measures to protect such targets.

2.23. Similarly, an adversary seeking to commit an act of sabotage could attempt to alter or deny access to information that is essential for the timely performance of a nuclear safety function, which would allow the adversary to more effectively plan the attack. Therefore, the compromise of sensitive information by an adversary increases the likelihood that the adversary can negatively impact functions important to safety, security and nuclear material accounting and control.

2.24. The conceptual information model illustrated in Figure 2 is applicable to sensitive information and supports the identification of opportunities to maintain the confidentiality, integrity and availability of sensitive information through the application of information security measures.

2.25. Access to sensitive information, sensitive information objects and sensitive information assets should be restricted to those individuals who have a genuine need for this access for the performance of their work. The dissemination of sensitive information should thus be limited to authorized individuals and sensitive information assets on a 'need to know' basis.

2.26. The ‘need to know’ and ‘least privilege’ (i.e. the minimum level of access to perform the function) principles should be used to guide management and control of access rights to sensitive information. The risks associated with information security are more enhanced when sensitive information is shared by individuals who do not understand the potential value of the information.

2.27. Maintaining the confidentiality, integrity and availability of sensitive information to protect against adversary actions relies on the application of security measures to selected sensitive information objects and sensitive information assets, with varying degrees of stringency. These measures should be tailored, using a graded approach, to the severity of the consequences resulting from the compromise of the information and be re-evaluated if a previously unknown consequence comes to light, as this could significantly amplify the impact. The greater the potential consequences of a compromise, the stronger the security measures that should be applied. Specific guidance on measures to protect against internal adversaries can be found IAEA Nuclear Security Series No. 8-G (Rev. 1), Preventive and Protective Measures against Insider Threats [7].

INFORMATION SECURITY

2.28. Information security, at a minimum, includes the following:

(a) Security of sensitive information held, processed and communicated by authorized and unauthorized individuals and sensitive information assets.

(b) Security of sensitive information objects (e.g. records of sensitive information on paper and electronic media).

(c) Security of sensitive information assets (e.g. information storage and processing equipment). Where this equipment uses computer based systems, these are specifically referred to as sensitive digital assets, as illustrated in Figure 3, and the domain is referred to as computer security. Computer security is a particular aspect of information security that is concerned the protection of computer based systems against compromise. Additional guidance on computer security for nuclear security can be found in Ref. [6].

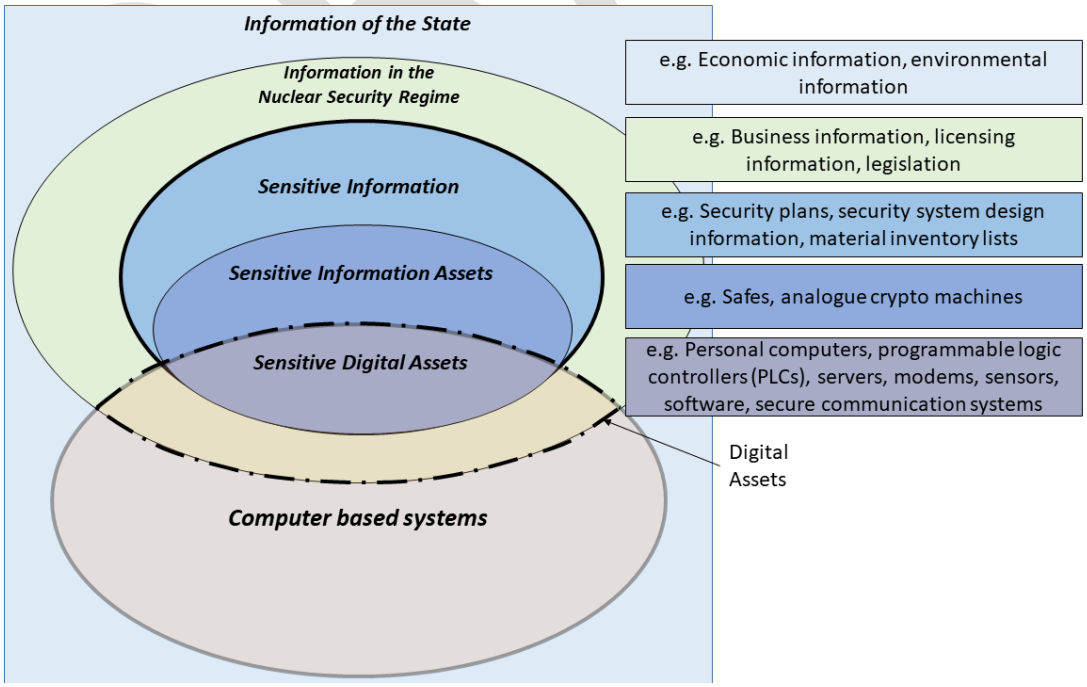

FIG. 3. Information and computer based systems in the State and in the nuclear security regime (adapted from Ref. [6]).

2.29. The choice of suitable security measures should be made on the basis of a risk analysis, with the objective of applying the necessary measures to reduce risks to an acceptable level. The State or other competent authority should ensure that the risk analysis is kept up to date through a process of periodic reviews, as part of an information security management system. This process ensures that security measures remain effective and relevant, and that such measures are adapted to changes in risk and aligned with a graded approach to protecting against the consequences of compromise.

2.30. Information security measures for confidentiality will often differ from those for integrity, as well as those for availability. Information security measures for availability can at times be in conflict with those for confidentiality, unless these measures are carefully designed to work together.

2.31. Information security activities should be conducted in accordance with the State's overall legislative and policy framework for securing sensitive information, and understood in the context of the overall nuclear security framework including other security domains, such as physical protection and personnel security since all these domains are interdependent. For example, physical protection measures can be used to protect sensitive information objects and sensitive information assets (e.g. computer based systems) that can contain sensitive information relating to other physical security measures (e.g. access control databases, site security plans).

2.32. Gaps or deficiencies in one security domain can affect the security of other domains, and so it is essential to adopt a comprehensive approach that considers all these domains. Legislative and policy frameworks for securing sensitive information should also consider the need to take into account other objectives, such as operational objectives, transparency and safety and provide adequate measures to do so.

3. LEGISLATIVE, REGULATORY AND POLICY FRAMEWORKS FOR SECURING SENSITIVE INFORMATION

3.1. Effective legislative and policy frameworks at the national level are necessary to ensure comprehensive, consistent and coordinated information security measures across all facilities, sites and organizations —– both governmental and non-governmental — that are handling sensitive information. Such frameworks should also ensure the criminalization of related offences. When creating security frameworks specific to the nuclear regime, the State should establish the following:

(a) Provisions for describing the responsibility of the State for information security;
(b) A legislative framework covering information security for sensitive information;
(c) An information security policy framework, including guidance and classification schemes for information security.

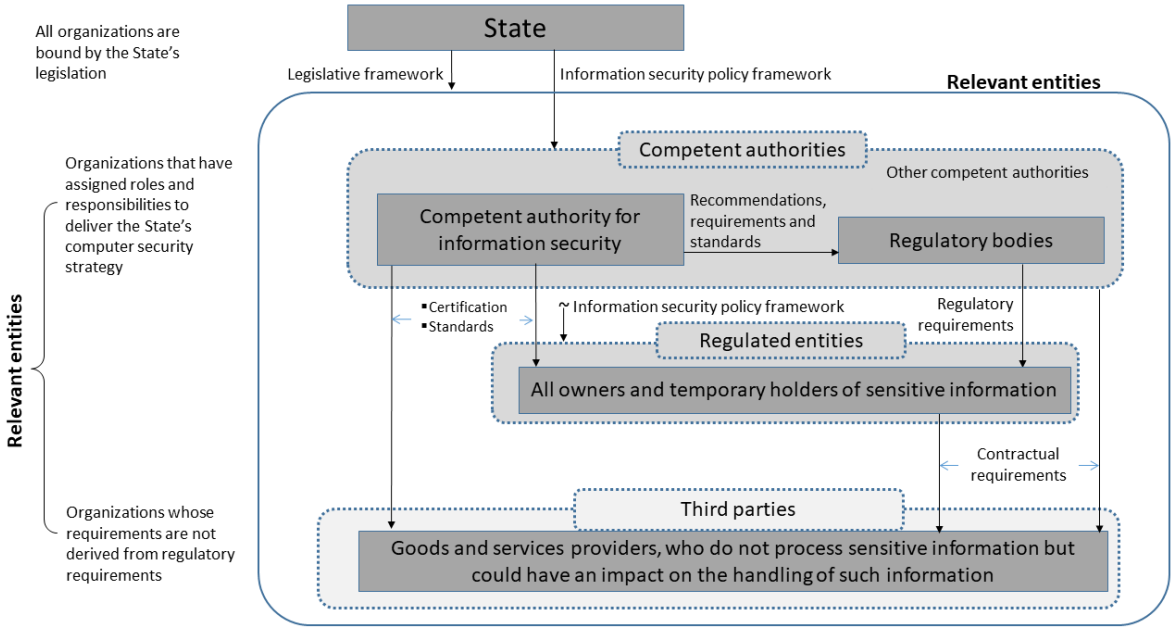

FIG. 4. The relationship between the State and entities relevant to the nuclear security regime for the purposes of information security (adapted from Ref. [6]).

3.2. Figure 4 provides an illustration of the organizations that could have an impact on the security of sensitive information in the nuclear security regime. The figure illustrates a potential relationship between the provisions of the State's legislative framework and information security policy framework and relevant entities, comprising competent authorities, regulated entities and third parties. Information security policies established within each organization should be developed in accordance with the State's legislative framework and information security policy framework.

LEGISLATIVE AND REGULATORY CONSIDERATIONS

3.3. The State should identify and ensure coordination of all organizations having a role in the nuclear security regime, described in this publication as competent authorities, regulated entities, and third parties. Competent authorities create a regulatory framework that enables oversight of the adherence to the State's legislative framework and information security policy framework within regulated entities. Regulated entities are those entities that have access to sensitive information within the nuclear security regime. They include all organizations that deal with matters identified by the State as being necessary to maintain information security within the nuclear security regime. A State could require any entity that holds and processes sensitive information, including providers of commercial goods and services, to fall within the category of regulated entities and therefore be subject to direct regulatory requirements relating to information security. Alternatively, a State could create separate information security requirements for competent authorities to follow.

3.4. Some third parties never retain sensitive information, but they could still have an impact on the security of sensitive information. These entities should be the subject of controls in order to maintain adherence to the regulations outlined in the information security policy framework. For example, third parties (e.g. equipment vendors) could provide technical equipment (e.g. document safes, computer based systems) to regulated entities (e.g. operators of nuclear power plants) that will process sensitive information. The relevant requirements for such organizations, and their products or services, could be defined directly or through contractual agreements, operating within the overall legislative framework.

3.5. The State can determine that international contractors who hold sensitive information, and who are outside of the State's legislative framework, should nevertheless be the subject of controls imposed through contracts. Alternatively, the State could demand that international contractors maintain a local presence, in which case these contractors would be constrained by the State's legislative framework.

3.6. Legislation should also be established to define competent authorities in charge of controlling information security and the sanctions or punishment that will be applied to individuals or organizations that breach information security. This legislation could have sections that define the severity of, and the corresponding sanctions for, specific types of breach, for example in relation to confidentiality, integrity, or availability of sensitive information, sensitive information objects and sensitive information assets.

3.7. The reporting of information security incidents to the competent authorities should be mandatory and laws or regulations should specify sanctions or penalties for failure to make such reports within defined timeframes.

3.8. The regulatory powers of competent authorities, established through the legislative framework, should allow the authorities to place obligations on the holders of sensitive information. Laws enacted for this purpose should mandate sanctions or punishment for unauthorized disclosure, manipulation or falsification of sensitive information. The legislation should also mandate the State ministries, departments, agencies and other organizations that are to provide the competent authorities with the necessary support, enabling the latter to fulfil the obligation of ensuring the security of sensitive information.

3.9. The State should consider examples from other laws and international legal instruments (e.g. conventions) to assist in defining and implementing information security as it relates to nuclear security. These examples could be found in the following:

(a) Laws concerning information and computer offences;
(b) Laws on terrorism;
(c) Laws on the protection of critical national infrastructure;
(d) Laws mandating the disclosure of information;
(e) Laws on privacy and the handling of personal information;
(f) International instruments (e.g. conventions, multilateral and bilateral agreements).

COMPETENT AUTHORITY FOR INFORMATION SECURITY IN THE NUCLEAR SECURITY REGIME

3.10. States typically have government organizations or agencies that are responsible for overall national security (hereafter referred to as 'national security authorities'). National security authorities have the responsibility of defining the State's information security policy framework, which includes all aspects relating to information security. The security policies and instructions issued by the national security authorities are often general in nature, covering broad applications (e.g. government information) and not specifically designed for nuclear security.

3.11. The State should therefore designate one or more competent authorities for information security (hereafter the 'competent authority for information security'), with responsibility for oversight and enforcement of information security laws and regulations as applied to the nuclear security regime. IAEA Nuclear Security Series No. 29-G, Developing Regulations and Associated Administrative Measures for Nuclear Security, provide more information on such responsibilities [10].

3.12. The State can choose to implement an information security policy framework that is not limited to the nuclear security regime, with the scope of some laws and regulations extending beyond the nuclear security regime. In such cases, the competent authority for information security should ensure that the information security policy framework is sufficient for nuclear security. If the framework does not adequately address nuclear security, the State should supplement the information security policy framework with the necessary requirements in a manner that is coherent with the nuclear security regime.

3.13. In the case that there is more than one competent authority for information security in relation to the nuclear security regime, or that the competent authority for information security differs from the competent authority responsible for nuclear security, the State should establish and maintain an appropriate coordinating body or mechanism to ensure clarity in the responsibility and accountability of these authorities, for every aspect of information security.

ROLES AND RESPONSIBILITIES FOR INFORMATION SECURITY

3.14. The State should identify all regulated entities and competent authorities with roles and responsibilities relating to information security in the nuclear security regime. The State should ensure that each identified entity has defined and assigned responsibilities, appropriate authority and falls under the oversight of the competent authority for information security in the nuclear security regime.

3.15. The State should require the identified regulated entities and competent authorities to develop and implement information security measures in accordance with the legislative framework and the information security policy framework. All personnel of regulated entities and competent authorities should be fully aware of the need for information security and should adhere to their organizations' information security policies and subordinate procedures.

3.16. The State should ensure that sufficient financial, human and technical resources are available to the competent authorities so that they can effectively fulfil their responsibilities in correctly implementing the legislative framework and the information security policy framework relating to information security in the State's nuclear security regime.

3.17. Regulated entities and competent authorities engaging third parties are responsible for developing contractual requirements for maintaining information security in adherence to the State's information security policy framework and for monitoring and evaluating the performance of the third parties to ensure compliance with the contractual requirements. In addition, the State could assign information security responsibilities and establish information security and trustworthiness requirements for third parties, in accordance with the information security policy framework, so as to ensure preservation of the confidentiality, integrity and availability of sensitive information.

3.18. Many regulated entities and competent authorities will operate within an international marketplace wherein goods and services are supplied from vendors and contractors from other States. Where the sharing of sensitive information is necessary to support contracts, it could result in sensitive information being sent outside of the jurisdiction of the originating State's legislative framework and information security policy framework. As such, enforcement actions relating to breaches of security requirements, or the control of legal authorization to access information, could be undermined. To address such issues, States can form reciprocal agreements to protect other States' classified information under their own security policy framework. The content of these agreements could differ from one State to another. Under these circumstances, it might be necessary within the State's information security policy framework to place greater emphasis on the robustness of the operator's contractual requirements, controls and assurance arrangements. Other laws or requirements, such as

requirements for data sovereignty, originating from outside the nuclear security regime, could also apply to the competent authority or regulated entity.

INTERFACES ON INFORMATION SECURITY WITH OTHER DOMAINS

3.19. The State should ensure efficient functioning/performance of interfaces between information security and other elements of a State's nuclear security regime, such as the physical protection of nuclear material and nuclear facilities, the security of radioactive material and associated facilities and activities, as well as the detection of and response to nuclear security events.. Actions could be necessary on the part of the State that are outside the scope of information security (e.g. placing requirements on information generated within other domains or accepting to apply the disclosure requirements of other domains on information security).

3.20. The State should provide for operators and other licensees requirements and guidance on the ways and methods of coordination, coincidence and adjustment of information security measures with physical protection systems (including transport), countering illicit trafficking and nuclear safety measures.

3.21. The State should ensure that the information security policy framework defines interfaces between information security and all other relevant domains to ensure that all respective competent authorities are considered, as appropriate, including regulatory authorities, coordinating bodies or mechanisms, law enforcement, response organizations for nuclear or radiological emergencies, customs and border control, intelligence and security agencies, and health and environment agencies.

IMPLEMENTATION OF THE STATE'S INFORMATION SECURITY POLICY FRAMEWORK

3.22. The State's information security policy framework should define criteria necessary to identify the information that the State wishes to protect and should indicate how information objects and information assets are to be protected. The framework generally sets out security guidance that has been compiled by the State's competent authority for information security, or by another appropriate authority. It is possible that the State's information security policy framework does not make any direct mention of sensitive information for nuclear security. The guidance should, however, specify different classes of information, indicating the information's level of sensitivity, and hence the level of protection to be applied, as well as how the information should be labelled to ensure that the level of sensitivity is evident. The State could, for example, establish a graded scale for the labelling of sensitive information in accordance with the level of protection to be provided.

3.23. Detailed policy and guidance on how to implement the requirements of the information security policy framework in the nuclear security regime should be developed by the competent authority for information security, in close liaison with national security authorities and in consultation with users of sensitive information within regulated entities of the nuclear security regime. This type of guidance should typically define what constitutes sensitive information, should divide the types of information into a series of related topics, and should indicate the importance of a particular piece of information, and thus its sensitivity and the degree of protection to be applied.

3.24. At the regulated entity and competent authority level, the importance of specific information can be indicated in an information security management system, which should also describe how sensitive information is to be protected in compliance with the information security policy framework and legislative framework (see Section 6 for additional information).

RISK MANAGEMENT

3.25. The State's information security policy framework, or the more detailed nuclear security guidance, should identify clearly the regulated entities and competent authorities within the nuclear security regime that have delegated responsibility for analyzing risks, managing risks and defining rules for the protection of sensitive information, as well as the regulated entities and competent authorities that are required to follow the defined rules. This delineation can allow some regulated entities and competent authorities more freedom to adjust the rules in accordance with local circumstances. For example, the State's competent authority for information security might operate a State-level information security management system to develop and issue detailed and mandatory information concerning security measures that are specific to the security of sensitive information in the nuclear security regime. Alternatively, the State's competent authority for information security could delegate this responsibility to regulated entities and competent authorities that demonstrate sufficient competence, along with the authority to manage certain risks locally with consideration of the national threat assessment or design basis threat. This authorization should always be in compliance with the State's legislative framework and information security policy framework, ensuring a harmonized approach to risk management across the nuclear security regime.

3.26. The competent authority for information security should also cooperate closely with the national security authorities in order to devise the national threat assessment or design basis threat. For more information on this subject, see IAEA Nuclear Security Series No. 10-G (Rev. 1), National Nuclear Threat Assessment, Design Basis Threats and Representative Threat Statements [11].

SECURITY POLICIES AND MANAGEMENT SYSTEM AT THE ORGANIZATION LEVEL

3.27. Each regulated entity and competent authority that handles sensitive information should compile its own information security policy and information security management system, on the basis of documented expectations from the competent authorities, so as to comply with the State's information security policy framework and legislative framework. The policy should be communicated to intended users in a form that is relevant, accessible and understandable. Section 6 contains additional guidance on establishing an information security management system.

3.28. The competent authority for information security could designate national or international standards that may be adopted by regulated entities and competent authorities to demonstrate compliance with elements of the State's information security policy framework and legislative framework. These standards may be used to guide the development of the regulated entities and competent authorities information security policy and information security management system.

4. IMPACT ASSESSMENT AND CLASSIFICATION OF SENSITIVE INFORMATION

4.1. Implementing information security systems and associated measures involves both resources and time. It is neither feasible nor desirable to ensure that all the information at a regulated entity or competent authority is protected in the same manner. A graded approach should therefore be used to protect sensitive information in a manner that is proportionate to the level of sensitivity. Identifying which information is sensitive information is thus important, as is determining the degree of sensitivity of this sensitive information.

4.2. The competent authority for information security should specify how to determine which information, relating to nuclear material, other radioactive material, and associated facilities

and activities, constitutes sensitive information and how this information should be classified on the basis of the following criteria:

(a) The impact of the direct compromise of the information's confidentiality, integrity or availability, which can be determined by considering the information's significance to functions that are important to safety, security and nuclear material accounting and control;
(b) The impact of of the compromise of the information's integrity or availability on the consequences of decisions made on the basis of the information, considering that the information made be targeted within an attack designed and executed to mislead human or machine based decision making.
(c) The usefulness of the information to a potential adversary seeking to compromise one or more nuclear safety or nuclear security functions.

4.3. Information can thus be classified using a graded approach. The greater the impact, on safety or security, for example, the higher the classification of the information and the more stringent the information security requirements. Some information that is not considered to be sensitive by the nuclear security regime could be considered sensitive for other reasons. Regulated entities and competent authorities might need to combine a graded approach common to the nuclear security regime and other factors used to identify sensitive information (e.g. the reliability of electricity generation by a nuclear power plant, nuclear safeguards, privacy related regulations).

SCALE OF IMPACT FOR SENSITIVE INFORMATION

4.4. The State might find it helpful to establish a common scale of impact. As shown in Fig. 5, information security requirements can then be developed using a graded approach, in proportion to the severity of the consequences of compromise of a function arising from the loss of confidentiality, integrity or availability of the information.

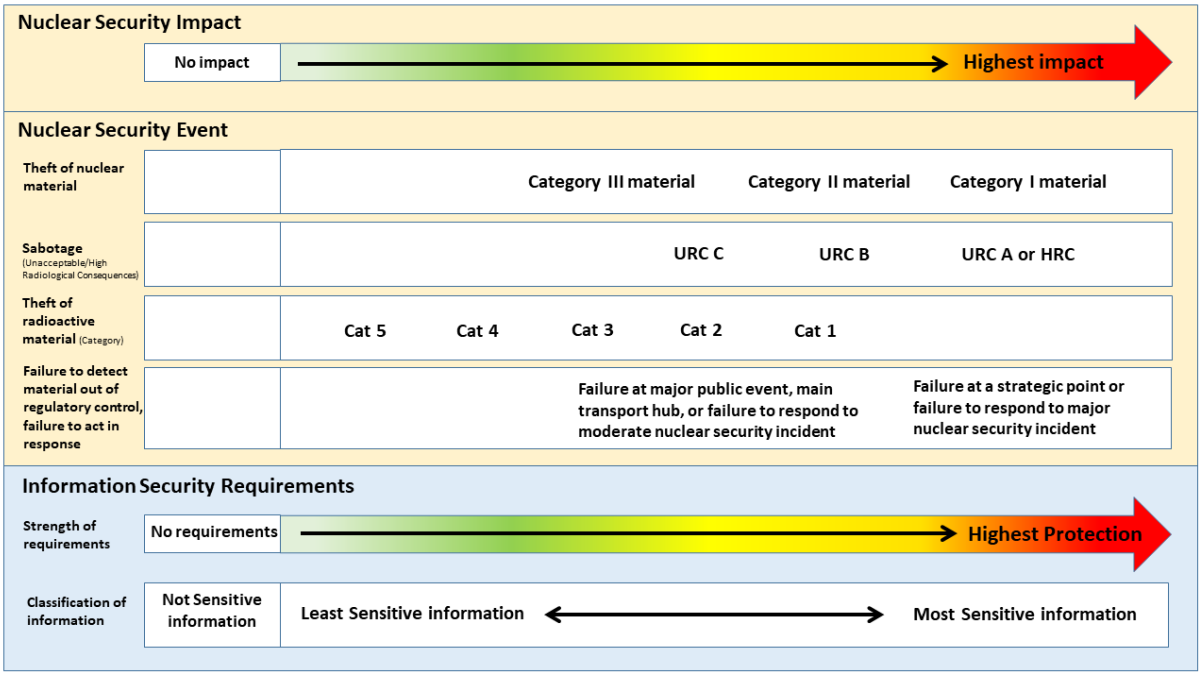

FIG. 5. Example common scale of impact and a graded approach to protecting sensitive information (adapted from Ref. [6]).

CLASSIFICATION OF SENSITIVE INFORMATION

4.5. Figure 5 shows a continuous scale for the classification of sensitive information. The State could divide this scale further into discrete levels of impact to produce a practical scheme for the classification of sensitive information. The following considerations could assist States in selecting the number of impact levels and the corresponding information security classifications:

- Very complex classification systems could contain many levels and become cumbersome, proving to be impractical.
- Very simple systems might not provide sufficiently precise classifications.
- Over-classification (i.e. requiring more stringent security than is necessary) can lead to unnecessary additional expense for regulated entities and competent authorities and conflict with policies for transparency, whereas under-classification can put sensitive information at an unacceptable risk of compromise.

4.6. When designing and implementing the classification scheme, a balance should be achieved between the need for a complex and complete scheme for information classification and the need for a practical scheme. The classification scheme should be accompanied by effective guidance that allows personnel in the nuclear security regime to easily understand and use the scheme. This guidance should consider the following factors:

(a) Specific consideration should be given to the accumulation of information and logical or physical points of aggregation (e.g. collections of non-sensitive information objects could become sensitive information objects if the relationship between the non-sensitive information objects provides additional context).
(b) Large collections of sensitive information stored in one information object or information asset could warrant a more stringent classification than when the sensitive information is classified individually.
(c) The relationship of information to functions can often be complex, and it might not always be clear to those tasked with assessing the value of the information.
(d) Individuals could have differing perceptions of the value of information. It can also be difficult to identify the most appropriate individuals to determine the classification of information.
(e) An information compromise at one regulated entity could affect other regulated entities and have broader impacts on the nuclear security regime.
(f) The usefulness of specific information to an adversary might not be clear to the individual(s) assessing the information.
(g) Labelling and classification schemes have long existed to assess the confidentiality of information, but these schemes might not consider the loss of integrity and availability of information (e.g. the classification ‘secret’ is commonly used for confidentiality schemes, and might not be recognized by some schemes as being applicable to the integrity and availability of information).
(h) The information security policy framework implementing a classification scheme should consider the practicalities of labelling information objects and processing information assets, including through computer based systems, as well as how associated requirements will be implemented in computer security measures (see Ref. [6]).
(i) As the value of sensitive information could be more readily apparent when contained in information objects or assets, they should be prioritized for classification and protection for the purposes of information security.

(j) The need for classifying certain information objects and information assets may change overtime as the understanding of threat capabilities and the consequences that could be realised evolve.

(k) Information that has not yet been classified should initially be managed using a conservative approach for the classification in order to prevent disclosure of information later proven to be sensitive.

4.7. A possible classification scheme for sensitive information, with classes that indicate the confidentiality of particular information objects, could be determined and could contain the following levels or others as defined by the State:

(a) Secret;

(b) Confidential;

(c) Restricted.

4.8. Protecting sensitive information depends on the balance between availability, integrity or confidentiality that is necessary to ensure that the function is protected from the consequences of compromise. For example, measures that provide protection in relation to the availability of information could be different from those that provide protection in relation to the confidentiality of information.

4.9. Classification schemes for sensitive information have traditionally been designed in response to the potential impacts of a loss of confidentiality. A classification scheme developed to focus on the confidentiality, integrity and availability of sensitive information could adopt one or a combination of the following options:

(a) Extending the use of established classification labels (e.g. secret) to encompass all aspects of confidentiality, integrity and availability is a simple solution, but it lacks specificity to inform the selection of information security measures.

(b) Implementing a more complex scheme, where each level separately indicates the degree of confidentiality, integrity and availability is a solution that could be overly complicated for users.

(c) Utilizing technology to manage these complex classifications is another solution that reduces the reliance on user understanding.

4.10. Some example definitions for the classification labels ‘SECRET’, ‘CONFIDENTIAL’ and ‘RESTRICTED’ are given in Annex I. These definitions can be applied to confidentiality, integrity and availability considerations.

4.11. Additional caveats[5] for information security could indicate restrictions on the distribution of sensitive information, in accordance with the nature of this sensitive information, or enhance the ‘least privilege’ or ‘need to know’ principles, which allow only users who have a legitimate need to access the information. The following is a very small set of examples that illustrate the use of caveats:

(a) No further distribution;

(b) Distribution controlled by the originator;

(c) Restricted distribution;

(d) Not releasable to foreign nationals.

[5] Caveats are additional security descriptors applied to classified information indicating specific restrictions, limitations on dissemination, or handling requirements beyond those required by the base classification level.

4.12. In the case of international activity that involves the sharing of information between States or with an organization within the jurisdiction of another State (e.g. international supply chain, international transport), the State should identify which information is sensitive and needs to be protected. Further guidance on this subject is provided in Section 5.

4.13. Examples of information that could be identified as sensitive information, classified and addressed through information security measures [12] are as follows:

(a) Details of physical protection systems and any other security measures established for nuclear material, other radioactive material, and associated facilities and activities, including information on guards and response forces;
(b) Information relating to the quantity and form of nuclear material or other radioactive material in use or storage, including nuclear material accounting information;
(c) Information relating to the quantity and form of nuclear material or other radioactive material in transport;
(d) Information related to the facility and its operations the misuse of which could compromise safety and security;
(e) Details of computer systems, including communications systems that process, handle, store or transmit information that is directly or indirectly important to safety and security;
(f) Information crucial to the correct performance of computer systems;
(g) Contingency and response plans for nuclear security events;
(h) Personal information about employees, vendors and contractors;
(i) Threat assessments and information concerning security alerts;
(j) Details of vulnerabilities or weaknesses that relate to the above topics;
(k) Historical information on any of the above topics.

4.14. Some of the information in para. 4.13 (e.g. personal information) could also be subject to specific security requirements under national laws not related to information security or could be subject to company policies.

4.15. Annex II contains examples of the specific types of information that could be encompassed in these categories, indicating whether and why they are typically considered to be sensitive information.

5. THE LIFE CYCLE OF SENSITIVE INFORMATION

5.1. Managing the life cycle of information, and more specifically the life cycle of sensitive information, allows regulated entities and competent authorities to use the information while at the same time protecting it. The management and protection of information are inextricably linked. This section uses the information model introduced in Section 2 to describe information management and information security activities associated with each of the four stages of the information life cycle[6], which is comprised of the following stages:

(1) Creating, collecting and classifying information;
(2) Processing, including handling, transmission and storage, of information;
(3) Using, including sharing, replication and dissemination, of information;
(4) Destroying or archiving information.

CREATING, COLLECTING AND CLASSIFYING INFORMATION

5.2. Information will generally be created in an abstract, unstructured and unlabelled form (see Fig. 2). For example, a person could calculate the number of guards on duty, or a machine could generate a stream of binary data representing observations from a sensor that is measuring temperature or pressure. Weaknesses and vulnerabilities could exist in terms of the management and security of this information, until the information is labelled and classified.

5.3. It is only when information is structured and labelled as part of an information object that it can be managed, classified and protected in proportion to its value to legitimate users and to adversaries. This process includes assessing the value to legitimate users of sensitive information (i.e. its value in relation to functions important to safety, security and nuclear material accounting and control), and the value to adversaries seeking to cause harm by subverting those functions. In order to perform the process of structuring and labelling information in a uniform and repeatable way, regulated entities and competent authorities need guidance in applying a classification scheme.

5.4. Once information has been assessed as sensitive information, regulated entities and competent authorities should implement mechanisms to manage sensitive information, such as a classified document register designed to track sensitive information. Given the widespread use of computer based systems to process information, including sensitive information, computer based information management systems should, by design, incorporate or interact with other management mechanisms for tracking sensitive information.

PROCESSING OF INFORMATION

5.5. Both the computer based systems and humans who process information can be considered information assets and individuals (see Fig. 2) and, in general, only they have the necessary ability to apply information security controls to the information objects containing sensitive information. A computer based system that processes information could, for example, be an IT system that processes documents, a control system in a nuclear power plant or an information management system. Computer based systems or humans can implement a classification guidance to apply the level of protection necessary for a specific information object (e.g. a document or a computer program).

5.6. Suitable physical containers, such as safes and locked cabinets, can also be considered information assets since they can reduce the burden of security controls needed to protect

[6] There is no single, universally recognized information life cycle, but most have between four and seven stages. The different elements in these stages are reflected in the four stage cycle provided above.

sensitive information. The concept of a security container can also be implemented in the case of a computer based system, for example by using the appropriate cryptography. Locked cabinets are another suitable measure to protect the confidentiality and integrity of information (e.g. documents, physical media), but both locked cabinets and cryptography can have a negative impact on the availability of information for authorized users.

5.7. Secure transmission protocols should be established to protect sensitive information from compromise. For instance, secure network channels or communication methods utilizing cryptography can be employed to ensure that information remains protected during digital transmission. Similarly, protocols for the transfer of information among humans should be established, and could include secure audio-isolated rooms for briefings or secure containers for the transfer of documents in public spaces or during transportation.

USING INFORMATION

5.8. The access of individuals to sensitive information should be controlled by a process or procedure that grants access on the basis of the need to know principle and rescinds this access when this need no longer exists. The need to know principle could nevertheless be perceived as incompatible with the overall need to share information in order to support the performance of functions across a regulated entity or competent authority, provide resilience and allow for innovation. This incompatibility can be managed through an information security management system to anticipate and balance the risks to the nuclear security regime (see Section 6).

5.9. For example, sharing timely information on a nuclear security incident might elevate the risk of a data breach while concurrently reducing the risk of more significant harm. Similarly, the act of withholding crucial design information for security reasons relating to confidentiality can inadvertently introduce engineering or operability risks since essential knowledge is not being fully disseminated to those needing it for safe and effective system design and operation.

5.10. An assessment to determine the authorized individuals who need access to sensitive information should be made taking into account other factors (e.g. safety considerations) that might introduce risks for the State. For example, individuals who are responsible for elements of the design and safe operation of a facility should be made aware of all sensitive information relevant to their tasking if this would reduce the risk to the State of a nuclear security event occurring.

5.11. With the widespread use of computer based systems to process information, the concept of ‘replication’ has now changed. It is no longer possible to control sensitive information by controlling the number of copies of physical documents that exist, for example by focusing information security measures on the means of replication (e.g. photocopiers). The regulated entity or competent authority’s computer based information management system should have information security measures — incorporated as part of its design and operation — for all aspects relating to the creation, processing and storing of sensitive information.

5.12. Traditional information security measures are at times impractical for information whose sensitivity has a brief lifespan, for instance during the transport of nuclear material. In such cases, employing code words (including gestures or signs) may reduce requirements for protection. This method involves substituting sensitive details with unrelated terms, or in essence creating a rudimentary form of encryption. It is nonetheless crucial to treat the context of these code words as sensitive information, to understand that the context can be quickly inferred and to use this strategy only when other security measures are not feasible. Authorized users should be pre-informed about the context and meaning of the code words so as to ensure that they are used effectively. This approach should be strictly controlled and limited to scenarios in which the information's sensitive nature is transient.

Disseminating information outside the regulated entity or competent authority

5.13. Since nuclear security responsibilities are not typically confined to an entity it is often necessary for information to be shared among entities that share security responsibilities and have a legitimate need to know the information on an ongoing basis. A legitimate need to share sensitive information outside of the regulated entity or competent authority could also arise, for example among State agencies, between regulated entities handling nuclear or other radioactive material and the relevant competent authorities, or among different States. Sharing of information might also be needed for effective security by design approaches.

5.14. Similarly, the need to disclose sensitive information to other regulated entities or competent authorities or to the public in a manner that was unanticipated and therefore not specifically planned could also occur. Timely communication of updates in relation to threat assessments or information on nuclear security events to relevant parties enables the adjustment of security measures and the exchange of operational experiences, which generally fosters continuous improvements. In addition to security concerns, information sharing could be necessary to support other objectives, such as safety assessments, operational needs and commercial demands. In all cases, information sharing should be performed while maintaining the confidentiality, integrity and availability of the shared data.

5.15. Both sharing and disclosure should be managed in a way that ensures that sensitive information is not inadvertently shared with, or disclosed to, individuals who do not have a need to know the information. The integrity and availability of the information should be maintained for those who do have a need to know.

5.16. The nature and extent of sharing such information should be based firstly on compliance with national laws or regulations and then on a balance between the benefits obtained from sharing the information and the associated risks. Rules concerning the dissemination of information between authorities should be governed by the State's security procedures. The dissemination of information between authorities should be performed in a manner that provides mutual assurances of information security at the appropriate levels and between all parties. Establishing a common approach throughout the nuclear security regime can maintain equivalent protection of sensitive information from compromise.

5.17. It is often necessary to share specific information with other States or relevant international organizations. In such cases, an agreement should be established to guarantee that sensitive information is secured by the recipient in a manner consistent with the requirements of the State from which the information originates. The security of information could be ensured through a bilateral or multilateral treaty or agreement that defines how information will be protected from disclosure. Such agreements would typically describe the necessary protection measures to be applied to sensitive information for the different classification levels in each State. These agreements should also consider how particular requirements (e.g. freedom of information legislation) in any one State might affect the handling of the other States' sensitive information.

5.18. In practice, most information will be shared using computer based systems, meaning that computer security controls will be needed to avoid any compromise to the confidentiality, integrity or availability of sensitive information as it passes between jurisdictions. Further guidance on computer security controls can be found in Ref. [6].

Need for disclosure of sensitive information

5.19. Most States have established laws to address the security of information that is of importance to national interest. Such laws specify sanctions that will be imposed if a person, either a national of that State or otherwise, breaches the information security laws governing

such information. There are also usually laws that regulate an individual's access to official government information.

5.20. Some States have freedom of information legislation or laws that allow members of the public to request access to information held by the authorities. The only information that can typically be withheld by the authorities is information that is covered by specified exemptions, such as information associated with national defence, security systems and measures or private and personal information. In a number of States, an item bearing a classification mark is not automatically exempted from disclosure. Mechanisms could be set up to resolve disagreements between the government and other parties regarding which information can be withheld to protect national security.

5.21. Other laws and regulations could require that certain types of information, which might include sensitive information, be disclosed upon request. One example is environmental legislation that requires public reporting of specified information. States should determine when such laws can allow the exemption of information that might affect nuclear security or the security of sensitive information from third parties.

Preparing guidance on disclosure

5.22. The State should develop specific guidance to assist regulated entities or competent authorities in deciding which sensitive information can be disclosed. When compiling such guidance, the responsible entity will typically consult government departments and relevant organizations. The guidance should aim to prevent unauthorized disclosure of sensitive information (see Annex II) by identifying the characteristics of information that is considered to be unsuitable for disclosure.

5.23. States should consider the need to provide specific guidance on the following:

(a) The level of sensitivity of certain types of information based on the consequences of compromise;
(b) The types of information that can be disclosed, under which circumstances information can be disclosed, to whom information can be disclosed and by which methods information can be disclosed;
(c) Conditions for the disclosure of information;
(d) The processes to review information for its potential sensitivity before presentation to the public (e.g. information destined for conference presentations, web postings or technical specifications);
(e) The actions that should be taken in the case of unauthorized disclosure of sensitive information, whether intentional or unintentional, or in the case of other breaches of information security requirements.

5.24. Given that circumstances evolve and information that might be considered sensitive and unsuitable for disclosure at one time might be significantly less sensitive and suitable for disclosure at a later time (or vice versa), guidance will be subject to change. All guidance should therefore be reviewed and updated periodically and in the event of significant changes in policies or circumstances.

5.25. It is generally feasible to reduce the level of security applied to specific information, where appropriate. The reclassification of information to a more restricted class could, however, be impossible or ineffective if it has already been widely disclosed. It is therefore important that difficulties in reclassification be considered in the original classification, and consideration be given to the appropriate balance between confidentiality and caution, and between availability and transparency. A default time frame for periodic review of

classifications should be established, but changes should also be made when needed, for example if the circumstances change significantly.

5.26. All requests to a regulated entity or competent authority for disclosure of sensitive information should be considered against this same guidance or criteria, and if possible, all such requests should be processed through a single, central office of the regulated entity or competent authority. A technique commonly used to gain inappropriate access to sensitive information is to make multiple requests to different individuals or units within the same regulated entity or competent authority. If these requests are addressed separately, without coordination, different responses could be given and sensitive information might be disclosed that otherwise would not have been.

DESTROYING OR ARCHIVING INFORMATION

5.27. The State's legislative and policy frameworks should define the rules for the retention, archiving, downgrading or declassification and destruction of sensitive information. In general, sensitive information should be kept only as long as needed, with sufficient information retained for the State's public record.

5.28. The destruction of sensitive information should transform the information beyond recognition and recovery, by any means available within the lifetime of the sensitive information. For example, if the information is expected to be sensitive information for many decades, the means of transformation and destruction (e.g. cryptographic methods) should be judged by experts to be irreversible for many decades.

6. IMPLEMENTATION AND SUSTAINABILITY OF INFORMATION SECURITY MANAGEMENT SYSTEMS

6.1. This section describes how a State's legislative and policy frameworks should be implemented and sustained within a regulated entity or competent authority, using an information security management system[7].

6.2. Regulated entities and competent authorities within the state's nuclear security regime should develop their own information security policies in collaboration with the State's competent authority. The policy should articulate high level goals, objectives and requirements for information security and represent management commitment. It should also reflect the extent of autonomy granted to the regulated entity or competent authority in managing information security risks. For instance, smaller entities with simple nuclear security responsibilities could adhere to a strict set of obligatory rules without much flexibility. In contrast, larger entities, such as nuclear power plants that face unique and complex security challenges, could possess more autonomy in tailoring their information security policy to adhere to a number of regulatory systems.

6.3. The resource allocation that is necessary for managing and monitoring information security will vary, depending on the complexity of the regulated entity or competent authority.

6.4. The establishment of goals, objectives and requirements should be effectively managed and subsequently maintained through the management system. The system should also be subject to continuous evaluation, modification and enhancement, which could be achieved by incorporating a continuous improvement or a 'plan, do, check, act' cycle. Such a cycle for an information security management system is depicted in Fig. 6. This management system

[7] The International Standard for Information Security, ISO-27000, uses the term 'information security management system'. Some States also use the term 'information security programme'.

should be integrated with the regulated entity or competent authority's other management systems (e.g. safety, quality, physical security and computer security) in a coherent manner to ensure a holistic approach to overall management, such as an integrated management system.

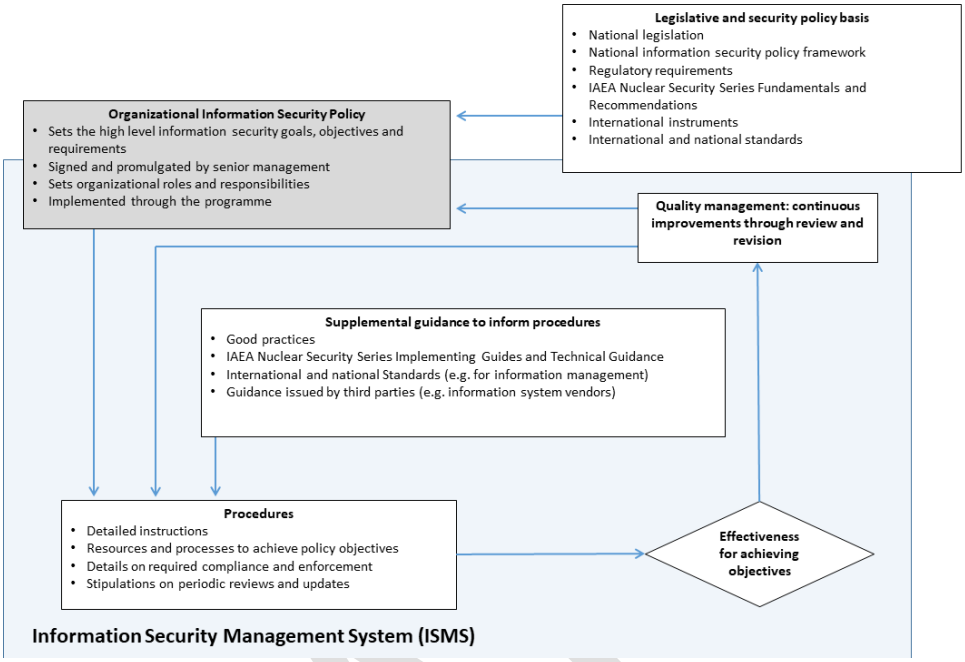

FIG 6. A continuous improvement cycle for the information security management system (adapted from Ref. [6]).

ELEMENTS OF AN INFORMATION SECURITY MANAGEMENT SYSTEM

6.5. An information security management system is a regulated entity or competent authority's means of implementing systematic, structured information security measures and subordinate systems with the objective of preserving the confidentiality, integrity, and availability of sensitive information. The system encompasses a comprehensive set of subordinate procedures and processes (e.g. technical, administrative, physical or other interconnected security measures) designed to provide for the security of sensitive information, sensitive information objects and sensitive information assets.

6.6. An overall organization level information security policy should be developed and endorsed by management at the highest levels. It should include a statement of overall objectives, scope and importance. The policy is binding on all personnel, and therefore measures should be taken to inform personnel of their obligations in relation to the information security policy, both during and after ceasing their term of employment as appropriate.

6.7. The objectives of the information security management system should be clearly documented in the organization level policy, reflecting the commitment to meet the State's legislative and policy frameworks. These objectives should be reviewed and updated on a regular basis to drive continuous improvement and to adapt to the changing information security situation.

6.8. The information security management system should take into consideration the risks identified within its scope to support the regulated entity or competent authority in addressing the design basis threat or threat statement and fulfilling regulatory requirements in accordance with the State's information security policy framework. Risk management objectives are to

reduce risks to an acceptable level through the application of adequate information security systems and measures.

6.9. The information security management system should be integrated at all levels of the regulated entity or competent authority, recognizing and leveraging interdependencies with other processes and management systems. This integration should also extend beyond the regulated entity or competent authority's boundaries to encompass third parties with information security responsibilities, where necessary. The integration of external parties can ensure a comprehensive approach to information security.

6.10. The information security management system, including all subordinate policies, procedures and processes, should be formally documented. Documentation serves as a foundation to maintain an up to date, auditable and effective information security posture. This documentation should be periodically reviewed to ensure that it adequately meets the State's legislative and policy frameworks and is up to date with the threat statement and the design basis threat.

6.11. The information security management system should also be updated in accordance with changes to the risk environment. Where the risk environment is assumed to be static, the risk management process should nevertheless continue to be reviewed at regular intervals. Any changes to the risk management process will necessitate commensurate changes in security systems and measures so as to ensure continued information security.

6.12. The regulated entity or competent authority should ensure that the necessary resources are available for the implementation of information security. Such resources would encompass the allocation of the appropriate information resources, financial investments and the personnel necessary to maintain and enhance the regulated entity or competent authority's information security posture.

6.13. A regulated entity or competent authority's senior management should visibly demonstrate their commitment to information security. This includes designating a senior manager with the responsibility to direct and manage information security functions. The designated manager should oversee assurance activities for information security and should manage the implementation of corrective actions resulting from these assurance activities.

Security culture for information security

6.14. A robust nuclear security culture is particularly important for information security in the nuclear sector because of the broader set of personal responsibilities involved. People and processes are a key factor in securing information, complementing the use of technology.

6.15. All personnel within the regulated entity or competent authority should recognize the importance of information security as an integral part of the broader nuclear security framework that also supports nuclear safety. To reinforce this, the regulated entity or competent authority should undertake to develop and implement an information security awareness programme that does the following:

(a) Contextualizes information security principles, highlighting their relationship to nuclear security and nuclear safety;
(b) Highlights the responsibility of personnel to adhere to the information security policy and processes implemented in the context of the information security management system;
(c) Fosters a culture that encourages the reporting of any information security issues, including incidents and vulnerabilities.

6.16. All personnel should fulfil their security responsibilities, with the regulated entity or competent authority providing appropriate education and training to ensure their competence and accountability in these roles. Individual performance reviews should also reflect the information security objectives so as to embed a culture of security awareness at all levels of the organization.

6.17. The regulated entity or competent authority should provide personnel with specific, security related responsibilities, or personnel with access to sensitive information, as well as information owners and management accountable for information security at all levels of the organization, specific training and briefings regarding their responsibilities. This training should encompass the procedural aspects involved in the management of sensitive information (see Section 5), and should focus on how to expand the capacity of personnel to recognize and respond to potential information security incidents. By enhancing these attributes, personnel are better equipped to effectively identify, report, assess and mitigate risks, ensuring a more robust information security management system.

6.18. Information security training events that are limited to one single event might not adequately reinforce training, and over the long term could allow personnel to become complacent. All those who handle sensitive information, including management, personnel and contractors, should receive continual on the job training and be required to attend periodic refresher courses. Personnel who handle sensitive information without necessarily being aware of its content should also receive security training specific to their responsibilities. Records should be maintained of formal training provided and completed by all personnel and contractors. Any changes in security rules and procedures should be made known by the management to all relevant personnel and contractors as soon as practicable. A suggested format and content for training and awareness programmes is provided in Annex III.

Security measures and information security system

6.19. The handling of sensitive information should be governed by procedures, in accordance with the regulated entity or competent authority's information security policy and as agreed with the competent authority, operating within the State's overall information security policy framework. The minimum information security requirements for the various security levels in the graded approach should be described in the information security management system procedures. An example would be the minimum encryption security lifetime used for the electronic transmission of information.

6.20. Effective management of the risks relating to the confidentiality, integrity and availability of sensitive information should involve developing effective security measures to protect against threats and meet the requirements. This process should result in a combination of security measures drawn from information security, physical protection and personnel security.

6.21. Security measures should protect the confidentiality, integrity and availability of information throughout the entire information life cycle, as described in Section 5.

6.22. The following security measures should be considered in the context of sensitive information:

(a) Access control should be utilized to ensure that access to sensitive information and sensitive information assets is limited to those who need such access to perform their duties.
(b) Personnel security, including trustworthiness determinations, should be used so that those who have access to sensitive information are deemed to be suitably trustworthy to a level established by the State in the information security policy framework. For information

with a low classification, the regulated entity or competent authority should decide whether any determinations are necessary for personnel that need access; if deemed necessary, a limited check of an individual's background could be sufficient. For access to information with a higher classification, a more comprehensive set of background checks will be needed to determine trustworthiness. The personnel security process could also include the signing of a non-disclosure agreement between the member of personnel and the competent authority for information security or the respective regulated entity or competent authority, the obligations under such an agreement should be reinforced during activities associated with the cessation of employment.

(c) Physical protection measures should combine a degree of strictly managed access through a secure perimeter with one or more layers of other physical protection measures closer to the information objects and information assets (e.g. vaults or other secure locations) that are being protected.

(d) The transmission of sensitive information, including as information objects, should be undertaken in a manner that reduces any risk of compromise, unauthorized interception, modification or denial of use to an acceptable level.

(e) Interfaces with a subordinate computer security programme should address computer security aspects of sensitive information assets, objects and digital collections of sensitive information [6].

6.23. Other considerations could affect the security measures used to protect sensitive information. For example, privacy requirements are typically not within the scope of the nuclear security regime, but these requirements could influence the implementation of the security measures used for information security within the nuclear security regime.

Arrangements with third parties

6.24. Third parties can provide goods and services to a competent authority or a regulated entity, which could have an impact on the security of sensitive information. Information security arrangements with third parties thus necessitate special consideration.

6.25. Information security arrangements for third parties should be established through legal agreements, such as a licence or contract, and should include a non-disclosure agreement. Such agreements could involve sensitive information being placed in the care of the third party. Contracting regulated entities and competent authorities should adhere to any national policies or legislation covering such agreements.

6.26. It is the responsibility of the contracting regulated entity or competent authority, when negotiating such a relationship with third parties, to ensure that any sensitive information entrusted to the third parties is protected in a satisfactory manner. The security measures that are established to protect sensitive information should be commensurate with the risks, and in accordance with the information security policy. As a design principle, the information security arrangements of third parties should be broadly equivalent to those of contracting regulated entities or competent authorities, although not necessarily identical in terms of the measures.

6.27. Regulated entities and competent authorities should require, and confirm, that third parties having access to sensitive information operate an information security management system. In addition, third parties should ensure the following:

(a) A contact point is established to direct and manage security in coordination with the contracting regulated entity or competent authority;

(b) Security arrangements at the third party's premises can be regularly inspected by the regulated entities or competent authorities, in accordance with the provisions of the agreement.

Managing access to sensitive information

6.28. A system should be in place to control why, when, to what extent and how specific individuals and information assets are authorized to have access to, or the ability to modify, sensitive information and sensitive information assets. Such a system should typically include the following:

(a) Defined responsibilities regarding the management of authorization of access to sensitive information;
(b) Defined processes concerning who has the right to access and modify sensitive information and sensitive information assets, and who has the right to grant further access;
(c) Defined processes concerning how to verify, control and supervise the function of assigning access;
(d) Defined processes to determine the duration of an authorization to access sensitive information and sensitive information assets;
(e) Defined processes to revoke authorization to access sensitive information and sensitive information assets due to an incident, employee turnover, and changes in job functions;
(f) Defined processes to maintain full traceability with regard to the management of rights during all of the steps involved in the management of authorizations to access sensitive information and sensitive information assets.

Information security management system activities for insider threat mitigation

6.29. The information security management system should interface directly with the regulated entity or competent authority's insider threat programme.

6.30. Reference [7] addresses information security systems and security measures, and underlines the possibility that information security could be compromised by an insider, namely by personnel "with authorized access to [nuclear material,] associated facilities or associated activities or to sensitive information or sensitive information assets".

6.31. Independent, non-repudiable logging and alert systems should be used to detect and alert on insider activities. Such systems should be capable of identifying unauthorized sensitive information transfers (i.e. a data loss prevention).

6.32. Paragraph 4.10 of Ref. [7] states that a key mitigation aspect of information security is "to minimize opportunities for malicious acts by limiting access, authority and knowledge of insiders". Such limitations can be accomplished, for example, by dividing critical functions into two parts that necessitate separate authorizations (e.g. the 'two person rule').

Assurance activities for the management system

6.33. The regulated entity or competent authority should establish metrics to provide an indication of the health of the information security management system and to identify trends that could be of concern.

6.34. Drills and exercises should be conducted on a regular basis to test all aspects of the information security management system. Drills and exercises provide assurance that the information security procedures are operating as intended. Lessons identified from drills and exercises should be considered in the regulated entity or competent authority's corrective actions.

6.35. The regulated entity or competent authority should also establish internal resources and a process to conduct internal inspections and audits. These inspections and audits should be performed to determine whether the practiced approach to information security complies with

the regulated entity or competent authority's information security policy and whether it remains in compliance with the State's regulatory and policy frameworks. Through such inspections, the regulated entity or competent authority will be able to check compliance more frequently than they would in the case of having to undergo external inspections. Moreover, the regulated entity or competent authority may establish training and procedures for inspections and audits, to enable conduct by trained personnel who are familiar with the internal requirements, procedures and systems allowing the identification of opportunities for improvement that differ from those discovered through external inspection.

6.36. External inspections are conducted by the competent authority for information security or other external organizations authorized to conduct inspections for information security within the nuclear security regime. The aim of external inspections is primarily to assess the level of compliance with the State's regulatory and policy frameworks in an independent manner. When using external auditors, issues of confidentiality and trustworthiness should be addressed in relation to the exchange of sensitive information with these external auditors.

6.37. Inspection and audit results should highlight specific areas for action or improvement. Preventive and corrective actions should be identified and specific time frames for the rectification or implementation of actions should be assigned. Organizations should also ensure follow up of rectification and implementation actions, verifying the overall effectiveness of these actions.

Continuous improvement of the information security management system

6.38. The regulated entity or competent authority's information security management system relies on the 'plan, do, check, act' cycle for continuous assessment and improvement (see Fig. 6). Additionally, this cycle should build on operating experience relating to information security from available sources, including government agencies, open sources and commercial information feeds, as well as threat statements and revisions to the design basis threat.

Detection of and response to information security incidents

6.39. Information security incidents, and particularly those stemming from criminal or other intentional unauthorized acts, necessitate an adaptable response strategy. These incidents can range from unauthorized access to sensitive information to those that immediately disrupt the correct performance of functions reliant on information. Incident response is necessary for both digital and physical collections of sensitive information (i.e. sensitive information objects and sensitive information assets).

6.40. Sudden incidents, such as the breach of highly classified information or a sophisticated cyber-attack against an instrumentation and control system, can occur without any prior indication, and necessitate immediate response measures to mitigate their impact. Other incidents could evolve slowly through a series of minor breaches or vulnerabilities that initially go unnoticed, but that accumulate over time to pose significant risks. The longer time frames in the case of these latter incidents could offer an opportunity for early detection and prevention, but such incidents can be damaging if left unaddressed.

6.41. The regulated entity or competent authority should identify an incident response team with diverse expertise in areas that include information security, computer security, physical protection, law, and operational management. The team should be trained and equipped to handle various types of information security incident (i.e. loss of confidentiality, integrity and/or availability).

6.42. A designated team within the regulated entity or competent authority should prepare an incident response plan. This plan should do the following:

(a) Define the roles and responsibilities of the incident response team members, including the scope of their authority during the investigation and any temporary investigative powers they might be accorded, within the limits of privacy and legal boundaries.

(b) Establish procedures for registering, recording, and tracking information security incidents, including the details associated with each incident and the response actions taken;

(c) Provide details of procedures for preserving evidence in relation to the incident in order to support criminal investigations of nuclear security related offences.

(d) Establish protocols for notifying and engaging internal and external stakeholders, (e.g. law enforcement and other relevant authorities). Thresholds could be determined for different levels and categories of incident, and who should be notified for each level and category of incident.

(e) Outline steps to contain the incident so as to prevent further loss of confidentiality, integrity or availability. These steps might involve mobilizing other resources in the regulated entity or competent authority, such as information owners, asset owners, engineers and specialized teams (e.g. a computer security incident response team). Any risks in relation to nuclear security within the State should be appropriately communicated to the relevant parties.

(f) Outline methods for assessing the scope and impact of an incident on nuclear security, nuclear safety, and nuclear material accountancy and control. The impact on relevant interested parties should also be assessed.

(g) Outline methods to recover information that has been lost, stolen or compromised, or otherwise mitigate the related consequences, ensuring that functions can continue to be performed within the defined levels of risk tolerance.

(h) Respect legal requirements relating to the incident, such as reporting obligations, data protection laws, and potential engagement with law enforcement or legal counsel.

(i) Outline how to communicate the incident internally and externally, ensuring that messages are accurate, timely, and aligned with legal and regulatory requirements (e.g. privacy regulations, incident disclosure laws).

(j) Plan for a post-incident review process to analyse the incident, identify root causes and integrate improvements into the response plan.

6.43. The response plan should be subject to continual improvement, through the use of drills, lessons identified in actual incidents, and operating experience from other organizations.

6.44. The information security management system should include security measures for the detection of suspicious activity, for the alerting of monitoring personnel in an expeditious manner, for ensuring effective monitoring of the incident, and for verifying on an ongoing basis the integrity and availability of backups of information and information assets. An example of a detection security measure is a system that detects unauthorized exfiltration of sensitive information.

6.45. After an incident, the chronology of the incident should be restored and its root causes identified. Lessons should be integrated into the regulated entity or competent authority's corrective actions. Such actions should include revising policies and procedures within the information security management system, enhancing information security measures, and augmenting training for personnel as needed to prevent future incidents.

6.46. The regulated entity or competent authority should report significant incidents or breaches of nuclear security, including breaches of information security, to the competent authorities in accordance with the State's laws or regulations.

6.47. Heads of regulated entities and competent authorities should establish formal reporting arrangements to ensure that all information security incidents are brought to their immediate attention in an effort to implement corrective actions, and where appropriate, to report the incident to the competent authorities. Personnel at all levels should be encouraged to promptly report all information security incidents regardless of the cause so that appropriate corrective actions can be taken and trends can be identified.

6.48. All information security incidents should be investigated by the regulated entity or competent authority. Policies and procedures governing the investigation of information security incidents should be defined by the organization within the information security management system. An investigation should aim to determine whether a security incident has a minor or major impact on information security. An example of a minor incident would be the failure to lock up or secure a document properly, with no result in terms of the loss or compromise of information. A major incident, for example, would be the theft of a highly sensitive document outlining security procedures, resulting in a significant risk for the organization.

6.49. The competent authority for information security should maintain records of the number and type of information security incident reported. Recurring incidents or trends in security failures should be identified and could underline a need for changes to the information security policy framework or for improvements in information security management systems.

REFERENCES

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

[2] INTERNATIONAL ATOMIC ENERGY AGENCY, IAEA Nuclear Safety and Security Glossary: Terminology Used in Nuclear Safety, Nuclear Security, Radiation Protection and Emergency Preparedness and Response, 2022 (Interim) Edition, IAEA, Vienna (2022).

[3] 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).

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

[5] EUROPEAN POLICE OFFICE–EUROPOL, INTERNATIONAL ATOMIC ENERGY AGENCY, INTERNATIONAL CIVIL AVIATION ORGANIZATION, INTERNATIONAL CRIMINAL POLICE ORGANIZATION–INTERPOL, UNITED NATIONS INTERREGIONAL CRIME AND JUSTICE RESEARCH INSTITUTE, UNITED NATIONS OFFICE ON DRUGS AND CRIME, WORLD CUSTOMS ORGANIZATION, Nuclear Security Recommendations on Nuclear and Other Radioactive Material out of Regulatory Control, IAEA Nuclear Security Series No. 15, IAEA, Vienna (2011).

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

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

[8] Amendment to the Convention on the Physical Protection of Nuclear Material, INFCIRC/274/Rev. 1/ Mod. 1 (Corrected), IAEA, Vienna (2021).

[9] International Convention for the Suppression of Acts of Nuclear Terrorism, United Nations, New York (2005).

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

[11] INTERNATIONAL ATOMIC ENERGY AGENCY, National Nuclear Security Threat Assessment, Design Basis Threats and Representative Threat Statements, IAEA Nuclear Security Series No. 10-G (Rev. 1), IAEA, Vienna (2021).

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

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

Annex I

EXAMPLE OF A CLASSIFICATION SYSTEM FOR SENSITIVE INFORMATION

I–1. Annex I provides an example of a classification system for sensitive information. Individual States can devise and use their own classification systems to indicate the level of sensitivity of nuclear security information. The definitions given in the following paragraphs represent a four level system similar to that used by many States. The fourth level, 'TOP SECRET' is not discussed in this annex since experience has shown that it is very unlikely that sensitive information in the civil nuclear field that might be distributed outside of national security authorities through mechanisms such as the design basis threat would attract the classification top secret[1]. The three levels used in this annex are the following:

(1) Secret;
(2) Confidential;
(3) Restricted.

I–2. While information for classification is primarily envisioned as being in the form of documents or knowledge, items of equipment or other physical objects could also be classified, more specifically in the case that classified information can be derived from equipment or physical objects through visual observation of internal or external appearance, structure, operation, testing, application or use.

I–3. The compromise of information or material classified as 'SECRET' would be likely to fulfil the following criteria:

(a) Raise international tensions;
(b) Cause serious damage to relations between governments;
(c) Threaten life directly, or seriously prejudice public order, individual security or liberty;
(d) Cause serious damage to the operational effectiveness or security of national security forces or to the continuing effectiveness of highly valuable security or intelligence operations;
(e) Cause substantial material damage in terms of national finances, or economic and commercial interests;
(f) Be of use to an adversary planning a criminal or other intentional unauthorized act that could cause grave damage to a facility with nuclear or other radioactive material, or during transport of such material.

I–4. The compromise of information or material classified as 'CONFIDENTIAL' would be likely to fulfil the following criteria:

(a) Damage diplomatic relations between States;
(b) Prejudice the security or liberty of an individual;
(c) Cause damage to the operational effectiveness or security of national security forces or to the effectiveness of valuable security or intelligence operations;
(d) Work substantially against national finances or economic and commercial interests;
(e) Substantially undermine the financial viability of major organizations;

[1] However, in exceptional cases, particularly concerning intelligence information and sources pertaining to the prevention of, or response to, a nuclear security event, a TOP SECRET classification might be warranted. This classification would typically involve highly sensitive intelligence that directly impacts national security and concerns the capabilities of specific and imminent credible threats targeting facilities or material.

(f) Impede the investigation of, or facilitate the commission of, serious crimes;
(g) Seriously impede the development or operation of major government policies;
(h) Shut down or otherwise substantially disrupt significant national operations;
(i) Be of use to an adversary group planning a criminal or other intentional unauthorized act that could cause serious damage at a facility with nuclear or other radioactive material, or during transport of such material.

I–5. The compromise of information or material classified as 'restricted' would be likely to fulfil the following criteria:

(a) Adversely affect diplomatic relations between States;
(b) Cause substantial distress to individuals;
(c) Make it more difficult to maintain the operational effectiveness or security of national security forces;
(d) Cause financial loss or loss of earnings potential to individuals or companies, or facilitate improper gains or advantages for an adversary;
(e) Prejudice the investigation of a crime;
(f) Facilitate the commission of a crime;
(g) Breach proper undertakings to maintain the confidence of information provided by third parties;
(h) Impede the effective development or operation of government policies;
(i) Breach statutory restrictions on the disclosure of information;
(j) Disadvantage the government in commercial or policy negotiations with other entities;
(k) Undermine the proper management of the public sector, as well as its operations;
(l) Be of use to an individual or group planning a criminal or other intentional unauthorized act that could cause significant damage at a facility with nuclear or other radioactive material, or during transport of such material.

I–6. The above classification levels can be applied to ensure the control of sensitive nuclear information, with consideration given to how the unauthorized disclosure of such information could assist a potential adversary in the following tasks:

(a) Selecting a target for an act of theft, or sabotage of nuclear or other radioactive material or associated facilities.
(b) Planning or committing an act of theft or sabotage of nuclear or other radioactive material or associated facilities on the basis of the following:
    (i) Design of security systems or specific vital equipment;
    (ii) Building plans;
    (iii) Methods and procedures for the transfer, accountability and handling of nuclear or other radioactive material;
    (iv) Security plans, procedures and capabilities.
(c) Measuring the success of an act of theft or sabotage of nuclear or other radioactive material or associated facilities by assessing the actual or hypothetical consequences of the sabotage of specific vital equipment or facilities.
(d) Illegally producing an improvised nuclear device, a radiological dispersal device or a radiation exposure device using the following:
    (i) Design information useful in developing a device;
    (ii) Location of material needed to manufacture a device;
    (iii) Location of a nuclear weapon.
(e) Dispersing nuclear or other radioactive material in the environment using information on

the location, form and quantity of nuclear or other radioactive material.

(f) Planning attacks to compromise the integrity and availability of information and information assets critical to nuclear security, through the following actions:

(i) Breaching the integrity of sensitive information assets, leading to misinformation or misdirection in nuclear operations, nuclear safety, nuclear security, and nuclear material accounting and control.

(ii) Disrupting the availability of sensitive information or sensitive information assets, hindering effective response or control in nuclear security events.

(iii) Compromising communication channels or computer networks that have an effect on the coordination and management of nuclear security measures, contingency operations and emergency response actions.

(iv) Altering or obstructing access to sensitive information regarding the safe and secure transport of nuclear material, its use or storage.

Annex II

EXAMPLES OF SENSITIVE INFORMATION

II–1. Annex II provides an example of what may be considered sensitive information. The State is to decide the exact level of classification to be applied to each item of information or produce guidance within the information security policy framework to delegate this to regulated entities and competent authorities. Table II–1 includes examples of sensitive information and identifies the sensitivity issues associated with this information.

II–2. The categories of information presented in Table II–1 are not intended as a comprehensive list or model, and are simply indicative of what might be considered sensitive information. The relevance of these categories and their potential inclusion in a national table are to be decided on the basis of a specific assessment by the State.

II–3. The first column of the table indicates the category of information and lists types of information that are included in each category divided by header rows representing topics relevant to nuclear security. The second column indicates whether this category is usually applicable to nuclear material and nuclear facilities (NSS 13 [II–1]), other radioactive material and associated facilities (NSS 14 [II–2]), the detection of and response to material outside of regulatory control (NSS 15 [II–3]) or a combination of these. The third column indicates whether this information could be considered sensitive (in terms of confidentiality, integrity, or availability) or not sensitive. The final column provides an explanation of the sensitivity of information and the rationale for securing it. The identification of whether an item is sensitive, the explanation, and the rationale are provided as non-exhaustive examples only.

II–4. In terms of the designation of information as sensitive and the assignment of a potential classification level, the State can give consideration to information that has already appeared in the public domain, or to any previous compromise or possible compromise of information. It might be impractical to assign and manage a classification level for such information.

II–5. Consideration could also be given to designating non-sensitive information as sensitive if it can be used to reveal sensitive information when it is combined with other non-sensitive information.

TABLE II–1. EXAMPLES OF SENSITIVE INFORMATION RELEVANT TO NUCLEAR SECURITY

Category	References	Sensitivity	Rationale for sensitivity
1. SECURITY OF MATERIAL AND FACILITIES			
1.1. Regulations and guidance			
A. National security regulations governing the use of nuclear material or other radioactive material	[II-1], [II-2], [II-3]	Not sensitive	Such information is typically published in the public domain.
B. Guidance for such regulations, issued by the competent authority or other government agency	[II-1], [II-2], [II-3]	Confidentiality	While not all such guidance is sensitive, a document of this nature could contain details of standards, types of equipment to be used, procedures and security operations at a facility. Such details could be of use to adversaries planning a criminal or other intentional unauthorized act.
1.2. National nuclear security policies			
A. General government policies on matters involving nuclear material or other radioactive material	[II-1], [II-2]	Not sensitive	Such information is typically in the public domain.
B. Detailed policy covering specific security topics	[II-1], [II-2], [II-3]	Confidentiality	The policy might give an indication of the sort of obstacles that adversaries could face, allowing them to plan the acquisition of more detailed information.

Category	References	Sensitivity	Rationale for sensitivity
1.3. Facility security plan	[II-1], [II-2]	Confidentiality	These plans typically contain detailed descriptions of the security measures in place at a site and precise details of where material is stored within the site. For nuclear facilities, such plans would also contain details of other areas essential to the operation of the site.
1.4. Security reports			
A. Reports from security surveys, inspections and assessments, and other reports on physical protection or technical security measures used at a site or facility	[II-1], [II-2]	Confidentiality	Access to these reports could provide adversaries with details on the location of material, the measures taken to protect material and any assessed vulnerabilities, thus assisting adversaries in avoiding security measures and controls.
B. Reports describing critical features and/or highlighting the need for security improvements, including at vital areas (if applicable)	[II-1], [II-2]	Confidentiality	Information of this nature could be of use to adversaries wishing to avoid security measures and could assist them in the targeting a facility.
C. Results of security investigations at a site or facility, including those into leaks and losses of sensitive information	[II-1], [II-2]	Integrity	An adversary could seek to alter such investigation data. This alteration could lead to incorrect conclusions, potentially exonerating the actual perpetrator of a security incident and allowing further undetected intrusions or data losses.
D. Reports describing vulnerabilities of the security management system and consequences of failure	[II-1], [II-2]	Confidentiality	Information of this nature could be useful to adversaries wishing to bypass security arrangements.
1.5. Construction details			

Category	References	Sensitivity	Rationale for sensitivity
A. Details concerning the construction and layout of locations in which material could be stored or processed, including drawings or plans stored on any medium (e.g. hard copy, electronic files), showing features of physical protection relevant to the prevention of criminal or other intentional unauthorized acts	[II-1], [II-2]	Confidentiality	Detailed information about the physical layout, security features, and storage locations could be leveraged by malicious actors to identify potential vulnerabilities in the facility's security system or otherwise aid in planning an attack.
B. Details of construction of vital areas at nuclear power plants and other nuclear facilities	[II-1]	Confidentiality	Information of this nature can help adversaries to avoid security arrangements and could possibly assist them in the targeting a facility for sabotage purposes.
1.6. Physical protection systems			
A. The computer program providing the correct functionality to any computer based physical protection measures in use (e.g. alarms, surveillance cameras, access controls)	[II-1], [II-2], [II-3]	Availability	If the availability of the computer code for physical protection systems is compromised, potentially through a cyber-attack or system failure, these security measures could become non-functional. The unavailability of such functions can leave sensitive areas vulnerable to unauthorized access or to criminal or other intentional unauthorized acts, since surveillance, access control and alarms would not operate as intended to detect or prevent such activities.
B. The types and locations of intrusion detection system sensors and the associated surveillance cameras, including circuit diagrams, the location of critical power supplies, cable runs, and maintenance and testing programmes for this equipment	[II-1], [II-2]	Confidentiality	Any details of this nature would be of use to adversaries who wished to defeat the security systems at a facility.

Category	References	Sensitivity	Rationale for sensitivity
1.7. Details of automated access control systems, including the location of computer servers and backup servers and their power supplies	[II-1], [II-2]	Confidentiality	Either insiders or external adversaries could use details to understand limitations in the access control systems or used in preparation of an attack against the system itself.
1.8. Detailed protocols for issuing, receiving and managing material stock; lists of personnel authorized to access key storage areas; and strategies implemented for continuous monitoring and security of these locations	[II-1], [II-2]	Integrity	An adversary might alter the protocols or the list of authorized personnel in the security procedures. Such tampering could lead to unauthorized access to sensitive material, with the changes potentially going unnoticed given the perceived legitimacy of the altered records.
1.9. General maps showing the position and limits of a facility but without detail of what is contained within the facility	[II-1], [II-2]	Not sensitive	Such maps are freely available on online mapping applications, which clearly show such information.
1.10. Other matters associated with physical protection (e.g. location, set up, manning and equipment at the central alarm station; location of the secondary alarm station; type of inner area barrier)	[II-1], [II-2]	Confidentiality	Details of this nature would be of great use to an adversary who wished to defeat the security systems at nuclear facilities.
2. INFORMATION RELATING TO THE QUANTITY AND FORM OF MATERIAL			
2.1. Information about the quantity, type and form of nuclear material and other radioactive material, (e.g. sources that have been received or are being held in specified locations including the exact locations where spent fuel is held)	[II-1]. [II-2]	Integrity	An adversary could manipulate such records, which provide specific details on the nuclear material inventory. The adversary's manipulations could misrepresent the actual quantities or types of nuclear material stored, and potentially facilitate the unauthorized removal or diversion of nuclear material.

Category	References	Sensitivity	Rationale for sensitivity
2.2. Throughput, including nominal capacity, actual throughput and historical data on the throughput of a facility under IAEA safeguards	[II-1]	Not sensitive	Such information, particularly for nuclear power plants, is often in the public domain.
2.3. Inventories, either national or local, of other radioactive material (e.g. disused material), including the quantity, type, form and exact location of this material	[II-2]	Confidentiality	This type of information could be of use to adversaries when choosing targets to attack in order to steal radioactive material. Consideration could be given to whether any of the information is publicly available concerning such inventories. Not all such information is necessarily considered sensitive. Risk informed processes will help determine whether something is to be designated as 'sensitive'.
3. MATERIAL IN TRANSPORT (INCLUDING MOVEMENT WITHIN A SITE)			
3.1. Transport security plans for nuclear material classified as Category I, II and III. These plans could include transit routes, times and security measures in place for transport.	[II-1]	Confidentiality, Availability	A disruption in the availability of accurate and up to date information on the movement of nuclear material can severely compromise security protocols. The inability to access or verify these details in real time could hinder the effective monitoring and protection of material during transit, increasing the risk of theft or sabotage.
3.2. High security vehicles			
A. Visual access to the interior of the vehicle and cargo compartment	[II-1]	Confidentiality	
B. Physical security features of vehicle design and construction	[II-1]	Confidentiality	

Category	References	Sensitivity	Rationale for sensitivity
C. Design and function of alarms, immobilization devices and key designs for special locks	[II-1]	Confidentiality	High security vehicles are vehicles specially designed to securely transport nuclear material. High security vehicles carry both the nuclear material and information of the type listed in the column to the left (see 3.2 A to E), which could be of use to an adversary planning an attempt to steal or sabotage nuclear material in transport.
D. Load compartment keys, spare keys and combination lock settings, where used	[II-1]	Confidentiality	
E. Vehicle tracking system if fitted to the high security vehicles; system performance and communications systems	[II-1]	Confidentiality	
3.3. Nuclear material transport containers			
A. Level of resistance to the attack (i.e. by various means) of transport containers	[II-1]	Confidentiality	This information can be useful to an adversary planning a sabotage attack with the aim of releasing nuclear material, or planning the theft of nuclear material during transport.
B. Specifications and design data on transport containers	[II-1]	Not sensitive	Information on the design of transport containers, without identification of construction details, is often available on the internet.
C. Information on the design of specific transport containers (specially protected containers)	[II-1]	Confidentiality	This information can be useful to an adversary planning a sabotage attack with the aim of releasing nuclear material or planning the theft of the material during transport.
3.4. Transport packages: Information on the design of transport packages	[II-1]	Not sensitive	Information on the design of transport packages, without identification of construction details, is typically in the public domain.

Category	References	Sensitivity	Rationale for sensitivity
3.5. Information on the movement of other radioactive material	[II-2]	Confidentiality	This type of information, particularly if concerned with the transport of high activity radiation sources, could be of use to adversaries in planning the theft of other radioactive material.
4. IT SYSTEMS AND COMPUTER SYSTEMS IMPORTANT TO SECURITY AND SAFETY			
4.1. Details of IT systems used to store and process sensitive information, including the systems used for security purposes and system architecture, details of computer security measures employed and location of backup media	[II-1], [II-2]	Confidentiality	This type of information could be used by an adversary to attack the regulated entity or competent authority, or could provide an adversary access to the system, allowing the adversary to compromise the sensitive information and affect the performance of functions relevant to nuclear security.
4.2. Computer based access control, intrusion detection systems, alarm monitoring systems, assessment and surveillance systems and other security functions and devices; and information on the location of backup hardware and software	[II-1], [II-2], [II-3]	Availability	If the availability of these computer based systems is disrupted, it could significantly impair nuclear security functions. Inability to access information on the location and specifics of backup hardware and software could hinder effective recovery and response in the event of a system compromise or failure.
4.3. Details of safety related IT systems or computer systems important to safety, including the locations, functions, upgrade routes, power supply and backup	[II-1], [II-2]	Integrity	Such safety related IT systems have control and operational monitoring functions. Successful compromise of these systems could enable an adversary to disrupt the operation of a facility, at a minimum, and to disrupt the systems in a way that leads to the release of radioactive material at worst.
5. GUARD FORCES AND RESPONSE FORCES			

Category	References	Sensitivity	Rationale for sensitivity
5.1. Guard force at a facility			
A. Overall establishment of the guard force and the current capabilities of the force	[II-1]	Not sensitive	Publicizing the existence of a guard force can reassure the public and potentially act as a deterrent.
B. Establishment of guard force and current capabilities at particular sites	[II-1]	Confidentiality	Information of this nature could be of use to an adversary when planning an incursion into a nuclear site for the purpose of sabotage or theft. This type of information could undermine the capability of guard forces to effectively respond to an attack.
C. Number of personnel on shift at a site during different shifts	[II-1]	Confidentiality	
D. Weapons and other special equipment available to the guard force, and the number of trained users of firearms in the guard force for individual sites	[II-1]	Confidentiality	
E. Response force location, capabilities, weapons, special response vehicles and hours on duty at a site	[II-1]	Confidentiality	Any information that could help an adversary to estimate in advance the scale of response and the capabilities available in a tactical operational unit are to be secured against disclosure.
F. Deployment plans	[II-1]	Confidentiality	
5.2. Escorts for nuclear material movements			
A. Deployment and capabilities of the escort	[II-1]	Confidentiality	This information could be of use to an adversary planning to attack a convoy.

Category	References	Sensitivity	Rationale for sensitivity
B. Radio frequencies in use to enable communication with a response force or local police forces	[II-1]	Integrity	Such information could be used by an adversary to tamper with, or falsify, radio frequencies, preventing timely contact with response forces or police and hindering effective coordination during response operations.
6. NUCLEAR MATERIAL ACCOUNTING AND CONTROL			
6.1. Description			
A. Statements concerning general material accounting principles	[II-1]	Not sensitive	General principles of this type exist in the public domain.
B. Design information questionnaire and description, and the location of material balance areas and key measurement points	[II-1]	Confidentiality	Such detailed information on the location and quantities of nuclear material could be of use to an adversary planning a criminal or other intentional unauthorized act.
C. Forms concerning physical and chemical material measurements at key measurement points	[II-1]	Confidentiality	
6.2. Measurements and instrumentation data			
A. Precision and accuracy of standard laboratory techniques	[II-1]	Not sensitive	This information is often in the public domain.
B. Data that reveal the sensitivity of measurements or the alarm limits for material unaccounted for at a particular nuclear facility	[II-1]	Confidentiality	Precision and accuracy data relating to actual or typical measurements at sites, whether aggregated or disaggregated, could be of use to an adversary planning the theft of material.

Category	References	Sensitivity	Rationale for sensitivity
6.3. Nuclear material flow and inventory data stored on IT systems, in hard copy or in any other form of storage medium	[II-1]	Integrity	An adversary might alter the nuclear material flow or inventory data, misrepresenting the actual movement or stock of nuclear material, which could lead to undetected diversion or misplacement.
6.4. Material unaccounted for			
A. Annual material unaccounted for figures for a site which does not reveal the material balance area concerned	[II-1]	Not sensitive	In many States, aggregated, annual material unaccounted for figures are, or can be, published in the public domain.
B. Material unaccounted for in material balance areas or key measurement points	[II-1]	Availability	Unavailability of material unaccounted for data for particular material balance areas or key measurement points can hamper accurate material accounting.
C. Details of investigations into particular material unaccounted for, unless formally approved for release	[II-1]	Confidentiality	Disclosure of investigation details could affect the investigative process, potentially revealing details to perpetrators who may alter their tactics, techniques and procedures.
D. Limit of error for material unaccounted for or other specific indications concerning the uncertainty of material unaccounted for figures	[II-1]	Integrity[a]	Manipulation of limits of error or uncertainty indicators could hide actual discrepancies in nuclear material accounting.
7. APPLICATIONS FOR LICENSING AND PERMISSIONS			

.

Category	References	Sensitivity	Rationale for sensitivity
7.1. Applications for licensing and permissions, without detailed information on security measures, and the type, form and quantity of material	[II-1], [II-2]	Not sensitive	The content of such applications will vary depending on the legal and regulatory framework, and the specific end use. If applications contain sensitive information that could be of potential use to an adversary, the application is to also be treated as sensitive information.
7.2. Applications for licensing and permissions containing detailed information on security measures, and the type, form and quantity of material	[II-1], [II-2]	Confidentiality	The content of such applications will vary depending on the legal and regulatory framework, and the specific end use. If applications contain sensitive information that could be of potential use to an adversary, the application is also to be treated as sensitive information.
8. SAFETY CASES, ENGINEERING DOCUMENTS AND OTHER INFORMATION ON SAFETY, ENVIRONMENTAL INFORMATION			
8.1. Safety cases			While most information concerning safety cases could be made public for transparency, some information could be considered sensitive if relating to nuclear security.
A. Details of potential hazards or other information that could be used to evaluate the impact of radioactive releases, or details on the impacts of radioactive releases	[II-1], [II-2]	Confidentiality	The type of detailed information contained in safety cases could be useful to adversaries, for example for selecting targets and planning attacks
B. Details concerning the strengths and weaknesses of processes, structures and protection systems designed to contain, control or secure nuclear material or other radioactive material	[II-1], [II-2]	Confidentiality	+.

Category	References	Sensitivity	Rationale for sensitivity
C. Specific details regarding access control to the nuclear material production process, encompassing both physical security measures and protocols for the removal of material and for control and monitoring.	[II-1], [II-2]	Integrity	Tampering with access control information could facilitate unauthorized entry or removal of material, compromising the integrity of the production process.
9. CONTINGENCY PLANS, RESPONSE PLANS AND EXERCISES			
9.1. Response and contingency			
A. Existence of a security response plan and a contingency plan	[II-1], [II-2]	Not sensitive	Publicizing the existence of such plans can reassure the public and potentially act as a deterrent.
B. Detailed content of a security response plan and a contingency plan	[II-1], [II-2]	Confidentiality	Details from the plans could indicate the capabilities, limitations and response times, and could therefore be useful to an adversary in planning a deliberate attack.
9.2. Communication channel established between a technical support centre and the control room in an emergency	[II-1]	Confidentiality, integrity, availability	A compromise of the communication channel could disrupt effective coordination, enable misinformation, and potentially impact timely decision-making in mitigating consequences of an emergency severe emergency conditions. Secure/reliable communications would contribute to preventing this [II-4].

Category	References	Sensitivity	Rationale for sensitivity
9.3. Security contingency plans, including detailed information	[II-1], [II-2]	Confidentiality, availability	Such documents contain information on established security measures, on the capabilities of the police or guard force contingents and on the response to a potential security incident. The inaccessibility of such plans can lead to disorganized and ineffective responses in actual security incidents.
9.4. Exercises			
A. Information concerning exercises that are to be undertaken, or that have already been undertaken	[II-1], [II-2]	Not sensitive	Publicizing the existence of exercises can reassure the public, provided that the level of detail (e.g. date, time, location of a future exercise) would not assist an adversary in the conduct of an attack.
B. Details of security exercises at a site, including the scenario, information on aspects of the security plan that are being tested, whether a response force will be involved and the results of the exercise	[II-1], [II-2]	Confidentiality, integrity	This information could provide adversaries with information on the nature, size and capabilities of the response force, information on the time needed to respond, details of the response force armaments and the nature of tactics employed. Tampering with exercise details could lead to inadequate testing of security plans, and the masking of vulnerabilities and operational inefficiencies.
C. Details of safety exercises	[II-1], [II-2]	Not sensitive	Safety exercises are often run in an open and transparent manner. They can typically be considered non-sensitive as long as they do not reveal detailed information on security measures.
10. PERSONAL INFORMATION			

Category	References	Sensitivity	Rationale for sensitivity
10.1. Personal information			
A. Information from trustworthiness determinations	[II-1], [II-2]	Integrity	Manipulation of trustworthiness check data could lead to unauthorized individuals gaining access to sensitive areas or information, which could pose a security threat.
B. Information in personnel files	[II-1], [II-2]	Confidentiality	Most national privacy regulations will mandate the protection of this type of information since it can be used for blackmail or extortion purposes.
11. RADIOACTIVE WASTE INVENTORY			
11.1. Information on radioactive waste			
A. General information about inventories that does not contain any details that could be exploited (e.g. on the fact that waste is stored at a particular site, or on aggregated quantities of waste without providing the location)	[II-1]	Not sensitive	Such information is generally in the public domain and does not describe the specifics that could be useful to potential adversaries.
B. Information that could be used in a criminal or other intentional unauthorized act or could enable identification of a specific building at a facility and the material held in the building	[II-1]	Confidentiality	Such information could be useful to adversaries planning sabotage.
12. DECOMMISSIONING			

Category	References	Sensitivity	Rationale for sensitivity
12.1. Plans to decommission a nuclear facility	[II-1]	Not sensitive	Plans to decommission facilities are often publicly announced.
12.2. Waste from decommissioning			
A. Information that a store is to be built, and its location.	[II-1], [II-2]	Not sensitive	This information is often in the public domain.
B. Details on the construction, security measures and quantity or type of material that is to be stored in facilities (i.e. new build) for the treatment and storage of waste and contaminated material arising from processing activities during decommissioning	[II-1], [II-2]	Confidentiality	This information can provide useful information to adversaries who are targeting facilities for sabotage.
13. THREAT ASSESSMENTS AND INFORMATION ON SECURITY ALERTS			
13.1. Threat assessments issued by the State, national security authorities or other competent authorities	[II-1], [II-2]	Confidentiality	A breach of such information could lead to the discovery and compromise of intelligence sources and methods, which could be a significant setback for national security operations and intelligence capabilities supporting nuclear security.
13.2. Details of the design basis threat	[II-1]	Confidentiality	If adversaries are aware of the required effectiveness of security measures from the design basis threat, they can prepare to overcome or bypass them, rendering physical protection defences less effective.
13.3. Details on a vital area identification study	[II-1]	Confidentiality	Understanding where a facility or competent authority has identified vital areas could allow adversaries to infer where security is weaker and identify alternative points of exploitation.

Category	References	Sensitivity	Rationale for sensitivity
13.4. Reasons for any security alert that could be in place and for any changes to the state of alert	[II-1], [II-2], [II-3]	Confidentiality, integrity	A falsely elevated security alert could result in the unnecessary deployment of security resources away from an adversary's intended target and reduce the effectiveness of physical protection.
14. NUCLEAR TECHNOLOGY			
14.1. Detailed operational data and process control system configurations about the production or processing of nuclear material	[II-1]	Integrity	Compromised integrity of process control system configurations could lead to equipment operating outside safe parameters, causing equipment failure and loss of process availability, or creating potentially hazardous conditions.
14.2. Designs of new technologies submitted for licensing (e.g. advanced reactors)	[II-1]	Confidentiality	Sensitive elements of designs of new technologies could enable adversaries to develop advanced methods to compromise systems, leading to a functional impact on the facility.
14.3. Detailed information that would assist in the disassembly of nuclear or radioactive devices to gain access to sources, or would otherwise assist in defeating security measures	[II-2]	Confidentiality	Information on precise disassembly times could allow an adversary to time an attack so that it coincides with periods of lower defence readiness, or to exploit gaps in surveillance in physical protection functions.
14.4. Vulnerability studies of technology designs	[II-1], [II-2], [II-3]	Confidentiality	Access to the content of confidential vulnerability studies could directly assist adversaries in identifying and exploiting weaknesses within technology designs, leading to targeted attacks that could contribute to a nuclear security event.
15. HISTORICAL INFORMATION FOR THE ABOVE TOPICS			

Category	References	Sensitivity	Rationale for sensitivity
15.1. Historical information of current relevance and still sensitive, whether the information is classified or not	[II-1], [II-2], [II-3]	Confidentiality	Information of this nature, although dated, could still be of use to adversaries.

REFERENCES TO ANNEX II

[II-1] INTERNATIONAL ATOMIC ENERGY AGENCY, IAEA Nuclear Safety and Security Glossary: Terminology Used in Nuclear Safety, Nuclear Security, Radiation Protection and Emergency Preparedness and Response, 2022 (Interim) Edition, IAEA, Vienna (2022).

[II-2] INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5), IAEA Nuclear Security Series No. 13, IAEA, Vienna (2011).

[II-3] INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Recommendations on Radioactive Material and Associated Facilities, IAEA Nuclear Security Series No. 14, IAEA, Vienna (2011).

[II-4] INTERNATIONAL ATOMIC ENERGY AGENCY, Method for Developing Arrangements for Response to a Nuclear or Radiological Emergency, Emergency Preparedness and Response , IAEA, Vienna (2003)

Annex III

ELEMENTS OF AN INFORMATION SECURITY TRAINING PROGRAMME

I–1. Annex III provides example elements for an information security training programme. When deciding the content of an information security awareness programme, a regulated entity or competent authority can consider the relevance of the topics and methods highlighted in this annex and develop a programme accordingly.

I–2. Maintaining robust awareness of security is a crucial foundation for effective nuclear security. When included among various other measures, such as organizational, physical, and information and computer security measures, enhancing security awareness can also be cost efficient. IAEA Nuclear Security Series No. 7, Nuclear Security Culture [III-1], provides a more in depth understanding of this subject.

I–3. Security training can be broadly divided into the following four types:

(1) Awareness training that increases awareness of threats and vulnerabilities, and recognition of the need to protect information and information assets, as well as the need to ensure the correct performance of functions.
(2) Specific training that delves into particular security facets applicable to all personnel, such as protocols for handling sensitive information, identifying compromised information, and identifying reporting procedures, and procedures for managing information security incidents.
(3) Professional training that typically offers in depth technical knowledge tailored to individuals in specialized roles. Personnel concerned could include administrators, information system developers, security personnel, and those involved in the classification and declassification of information.
(4) Specialized security training that provides focused, advanced level instruction, primarily for those in managerial or supervisory roles overseeing the information security management system or large collections of sensitive information. This training encompasses areas such as risk management, prevention of incidents, and response strategies.

INFORMATION SECURITY AWARENESS TRAINING

I–4. The information security awareness training could include content to raise awareness on the following topics:

(a) Overview of the national security infrastructure;
(b) Different aspects of information security and why they are important to nuclear security;
(c) The national classification system;
(d) Correct use of markings of the classification of information;
(e) Practical examples of applying security procedures as part of the tasks that personnel need to undertake;
(f) Actions to be taken if a breach of security is suspected or discovered;
(g) Security principles, for example granting access on the basis of the ‘need to know’ principle;
(h) Current risks to security in relation to deliberate actions resulting from the following:
    (i) Hostile intelligence services in respect of espionage;
    (ii) Subversive organizations;
    (iii) Other individuals and groups, such as information brokers and investigative journalists seeking to gain unauthorized access to sensitive information or to nuclear sites and facilities;
    (iv) Insider adversaries.

(i) Contemporary extremist factions or adversary organizations planning sabotage;

(j) The risks and consequences of internal loss or leaks of sensitive information, perhaps through inadvertent behaviour or to intentionally cause harm, for example deliberate betrayal for political motives or to assist with terrorist actions.

(k) Conduct or activities likely to help potential adversaries or increase the risk of compromise, including the following:

  (i) Vulnerable behaviour, such as casual attitudes to security or careless discussions;

  (ii) Unwitting behaviour that can attract the attention of hostile agencies, along with the precautions that need to be taken in everyday activities, for example, in social approaches, travel, correspondence and acquaintances.

(l) Information on ongoing security events or new approaches being used by hostile agencies, which need to be disseminated rapidly within the organization.

(m) Emphasis on the need to immediately report all suspicious circumstances and potential compromises of information, perceived weaknesses in security procedures or vulnerable behaviour apparent in colleagues. The means of reporting in confidence would have to be made widely known.

(n) Information on recognizing the importance of protection of information and seamlessly integrating this recognition into the daily responsibilities of every user under the information security management system.

(o) The effect of national laws and regulations and their relevance to individuals, for example, laws governing secrecy, anti-terrorism, security, data protection and freedom of information, as well as the sanctions and punishment for the transgression of laws.

(p) The effects of computer based systems on the aggregation of information and the need for the evolution of computer security measures as vulnerabilities and attack methods change faster than technology.

(q) An explanation of the levels of security clearance; how trustworthiness determinations are carried out; why they are necessary in the nuclear and radiation industry; and which levels of access relate to particular clearance and trustworthiness levels, as well as how this relates to the to the security risks mentioned above.

(r) Scenarios that demonstrate compromises of confidentiality, integrity and availability of information, with a particular focus on integrity and availability, both of which are generally less understood, through the following:

  (i) Unauthorized disclosure — a breach of confidentiality.

  (ii) Denial of use (e.g. preventing an organization from having access to information when needed) or destruction of information — a breach of availability.

  (iii) Unauthorized modification of or interference with information — a breach of integrity.

OPPORTUNITIES TO PROVIDE INFORMATION SECURITY TRAINING AND ASSURANCE

I–5. The organization could integrate information security considerations into the personnel and contractor onboarding process, including the following:

(a) Introductory security briefing: This is a one hour session led by the team responsible for information security within the organization, emphasizing the importance of security. This briefing can also guide personnel on where to find security procedures, how to seek further advice and how to report information security incidents.

(b) Manager-led security orientation: This includes on-the-job training, where managers provide guidance on security related topics, contextualize the potential impacts of a compromise of sensitive information, and highlight the importance of information security and identifying and reporting

information security incidents. This approach ensures that security awareness is integrated into daily work practices and the team culture.

(c) Mandatory online security training: All new personnel are asked to complete a computer based training module on general security principles within the first month of their contract. This training would cover foundational security concepts and organizational security policies, and it needs to be designed to assist individuals in developing their intuition and experience detecting compromised information.

I–6. The organization could establish periodic security training and awareness during contract work could include the following:

(a) Annual security awareness training: A major yearly training session focusing on specific security topics relevant to that year, which have been selected on the basis of analysis of recent internal or external security incidents, or result from the implementation of new systems or policy updates.

(b) Regular security updates: Smaller, frequent updates through internal news articles or bulletins on relevant security topics, particularly on external security events or emerging threats.

(c) Organization-wide security drills: Periodic practical security tests for all personnel. These tests or drills include red team exercises, social engineering tests or phishing simulations to assess and enhance the organization's security readiness.

(d) Targeted training based on analysis: Utilize data from security tests and incident reports to provide tailored training for specific departments or groups, avoiding less effective approaches designed to target all audiences.

(e) Topical computer based training: Additional computer based training on specialized topics, such as information classification, working with contractors, cross-border information sharing, computer security, remote work guidelines, travel security, and insider threat awareness and response.

I–7. The organization could embed information security considerations during the process of personnel separation including:

(a) Exit interview for feedback: An exit interview with departing personnel to gather feedback on the organization. Such interviews can help identify unresolved issues or dissatisfaction, which might necessitate further attention both in terms of the individual and the organization.

(b) Asset retrieval: Verification that all departing personnel return assets belonging to the organization. These assets could include physical items (e.g. keys, badges, mobile phones) or digital assets (e.g. files, documents).

(c) Reminder of cconfidentiality obligations: Emphasizing that the confidentiality agreement signed by personnel remains in effect indefinitely, notwithstanding the termination of employment. Where applicable, remind personnel of the legal and criminal consequences of breaching this agreement.

(d) Completion and signing of standard departure form: Asking the departing personnel to sign a standard form confirming that the exit interview was conducted, all assets of the organization were returned, and personnel acknowledge the ongoing validity of confidentiality obligations.

I–8. In addition to an awareness training programme, there are a number of other methods by which security awareness messages can be transmitted to personnel and contractors by an organization, including the following:

(a) Posters to remind individuals of risks to security and of the principal security controls necessary to counter such risks. The impact of posters tends to be temporary, and so it is important to ensure that they are both prominently displayed and frequently changed.

(b) Stickers to remind personnel of their personal responsibility for the maintenance of security when using specific items of equipment.

(c) Security reminder notices during the start up (boot) phase of a computer system, which the user has to acknowledge having read before the computer will allow the user to log in to the system. Systems can also record such acknowledgements so that a user cannot deny having seen the notice.

(d) Security notices, bulletins and circulars drafted by security management to remind personnel of certain security rules, for example, or to counter possible complacency.

(e) Awareness raising initiatives focusing on instances of breaches of security and the lessons that can be identified.

(f) Warning personnel of specific or topical risks to security and providing guidance to counter these risks.

(g) Regular and periodic tests of security knowledge of personnel.

(h) Use of the organization's intranet site as a valuable tool for conveying or promoting the overall security message under the condition that the nature and the sensitivity of the material remain within the accredited level of classification for the network.

I–9. An organization can significantly strengthen its information security training programme by leveraging the common principles that exist in the overlap between safety and security domains. These shared principles allow for mutual reinforcement in training for both safety and security, and can support effectively conveying and equating fundamental concepts:

(a) Leadership and management play a pivotal role in establishing clear safety and security expectations and demonstrating exemplary behaviour.

(b) Employees should be aware of the real risks associated with safety and security incidents, including their consequences, underscoring the need for proactive prevention.

(c) It is essential for employees to be familiar with the procedures designed to avert safety and security incidents.

(d) Beyond knowing these procedures, employees must adhere to them, ensuring maximal efforts in preventing incidents.

REFERENCES TO ANNEX III

[III-1] INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Culture, IAEA Nuclear Security Series No. 7, IAEA, Vienna (2008)