IAEA NUCLEAR SECURITY SERIES No. XX

STEP 11 Second review of the draft publication by the review Committee
Date: 29 May 2025

Information Security for Nuclear Security

DRAFT IMPLEMENTING GUIDE

INTERNATIONAL ATOMIC ENERGY AGENCY
VIENNA, 20XX

02 June 2025

CONTENTS

1. INTRODUCTION

BACKGROUND

1.1. Paragraph 3.9 of IAEA Nuclear Security Series No. 20, Objective and Essential Elements of a State's Nuclear Security Regime [1] states:

> "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."

1.2. Paragraph 3.3 of Ref. [1] states:

> "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*."

1.3. The need for protecting the confidentiality of information is identified in Fundamental Principle L of the Amendment to the Convention on the Physical Protection of Nuclear Material [2] and in Article 7 of the International Convention for the Suppression of Acts of Nuclear Terrorism [3].

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

> "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."

1.5. IAEA Nuclear Security Series No. 13, Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5) [4]; No. 14, Nuclear Security Recommendations on Radioactive Material and Associated Facilities [5] and No. 15, Nuclear Security Recommendations on Nuclear and Other Radioactive Material out of Regulatory Control [6] provide recommendations on the protection of sensitive information.

1.6. Groups or individuals wishing to commit a criminal or intentional unauthorized act involving or directed at nuclear material, other radioactive material, associated facilities or

associated activities 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" [1].

1.7. Paragraph 1.3 of IAEA Nuclear Security Series No. 42-G, Computer Security for Nuclear Security [8] states that "The security of sensitive information and sensitive information assets implies protecting the confidentiality, integrity and availability of such information and assets."

1.8. Some sensitive information is created, controlled, stored, processed or communicated through computer based systems (i.e. sensitive digital assets). Ref. [8] provides further guidance on addressing computer security utilizing a graded approach, based on the severity of potential consequences, to protect the confidentiality, integrity and availability of computer based systems[1], the compromise of which could adversely affect nuclear security or nuclear safety.

1.9. The terms used in this publication are to be understood as explained in the IAEA Nuclear Safety and Security Glossary [7], unless otherwise stated in the text.

1.10. This publication supersedes IAEA Nuclear Security Series No. 23-G, Security of Nuclear Information[2].

OBJECTIVE

1.11. This publication provides guidance on applying the principles of information security to support a State's nuclear security regime. More specifically, it 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 management system[3].

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.

[1] Computer based systems include information technology (IT), operational technology (OT), and other systems that create, provide access to, process, compute, communicate or store digital information, or that provide or control services involving such information. IAEA Nuclear Security Series No. 17-T, Computer Security Techniques for Nuclear Facilities [9] provides guidance on how confidentiality, integrity and availability may be managed differently based on the facility function being performed by a computer based system in a nuclear facility.

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

3 The term 'information security management system' is used throughout this publication, in line with the terminology employed by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) in the ISO/IEC 27000 family of standards [10]. Some national authorities use the term 'information security programme' to reflect this concept in their regulatory frameworks.

SCOPE

1.13. This publication provides guidance on information security for nuclear security, and its interfaces with nuclear safety such as the protection of nuclear safety functions against criminal or intentional unauthorized acts (e.g. cyber-attack, insider threat), 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.

1.16. 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 or other radioactive material; response organizations for nuclear or radiological emergencies; facility operators and personnel; designers; vendors; 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 and therefore needs to be managed as such. Section 5 presents a four-stage model for managing the life cycle of sensitive information and describes the activities to be undertaken at each stage. Section 6 provides guidance on information security management systems. 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. Annex IV shows how various information life cycle activities can be mapped to the model presented in Section 5.

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[4], integrity[5] and availability[6] 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 security or nuclear safety function[7].

2.4. A State's legislative, regulatory and policy frameworks (see Section 3) and the information security management system of a regulated entity or regulated competent authority (see Section 6) should together form information security governance structures that reflect the information security measures and activities necessary to support the nuclear security regime and its interfaces with nuclear safety throughout the entire information life cycle (see Section 5). This is because some functions performed by an organization[8] (e.g. the safe operation of a nuclear facility) that are directly relevant to the State's nuclear security[9] and nuclear safety[10] objectives rely upon the confidentiality, integrity and availability of sensitive information, as illustrated in Fig. 1.

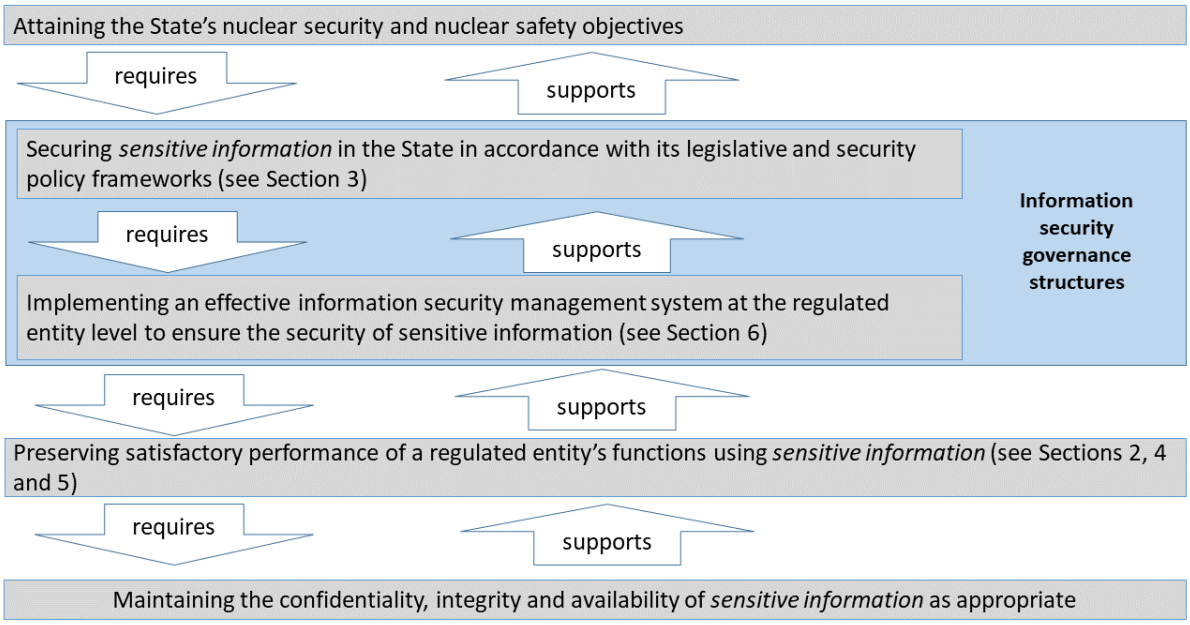

FIG. 1. Relationship between the State's nuclear security objectives, information security governance structures and the confidentiality, integrity and availability of information (adapted from Ref. [8]).

[4] The property that information is not made available or disclosed to unauthorized individuals, entities or processes.
[5] The property of accuracy and completeness of information.
[6] The property of being accessible and usable upon demand by an authorized entity.
[7] A set of activities designed and coordinated to achieve a specific objective.
[8] Ref. [9] uses the term 'facility functions' to describe the functions performed by a nuclear facility.
[9] For the purposes of this publication 'nuclear security' is to be interpreted as including nuclear material accountancy and control.
[10] For the purposes of this publication 'nuclear safety' is to be interpreted as including emergency preparedness and response.

INFORMATION

2.5. Information includes facts, data, ideas, concepts, events, processes, thoughts, patterns, symbols and instructions in any form. Information can be represented and communicated by almost any means, but becomes meaningful and valuable only when placed within appropriate context. This distinction between contextual and abstract information is crucial for the proper interpretation and application of information security.

INFORMATION OBJECTS

2.6. Information objects are physical or digital collections of information on paper, on film, on magnetic or optical media, in charts, in documents, in executable software files, or in any other form or channel used for transferring information.

2.7. For the purposes of security, effective information management and user convenience, information can be grouped into information objects. Information objects have the following characteristics:

(a) The information within an information object shares certain properties, such as a common usage, purpose, associated risk, or form of creation, processing, storage or transmission;
(b) The information object has sufficient context (i.e. includes information that allows its use and value to be identified) to allow the information within it to be assessed;
(c) The information object can be labelled, enabling the application of targeted and specific security controls to protect it proportionately.

2.8. 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 has context) that targeted and specific 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.

INFORMATION ASSETS AND INDIVIDUALS

2.9. Information assets are any equipment or components that are used to store, process, control or transmit information, including control systems, networks and information systems. Information assets might contain one or more information objects, and/or multiple pieces of information and might perform a function or contribute to a function that utilizes information or information objects.

2.10. Information assets actively facilitate the handling, management and utilization of information objects through various operations such as the storage, processing, control or transmission of information. While many use digital technology, some information assets perform these actions without digital technology (e.g. safes with mechanical locks).

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

FUNCTIONS AND INFORMATION

2.12. 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.

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

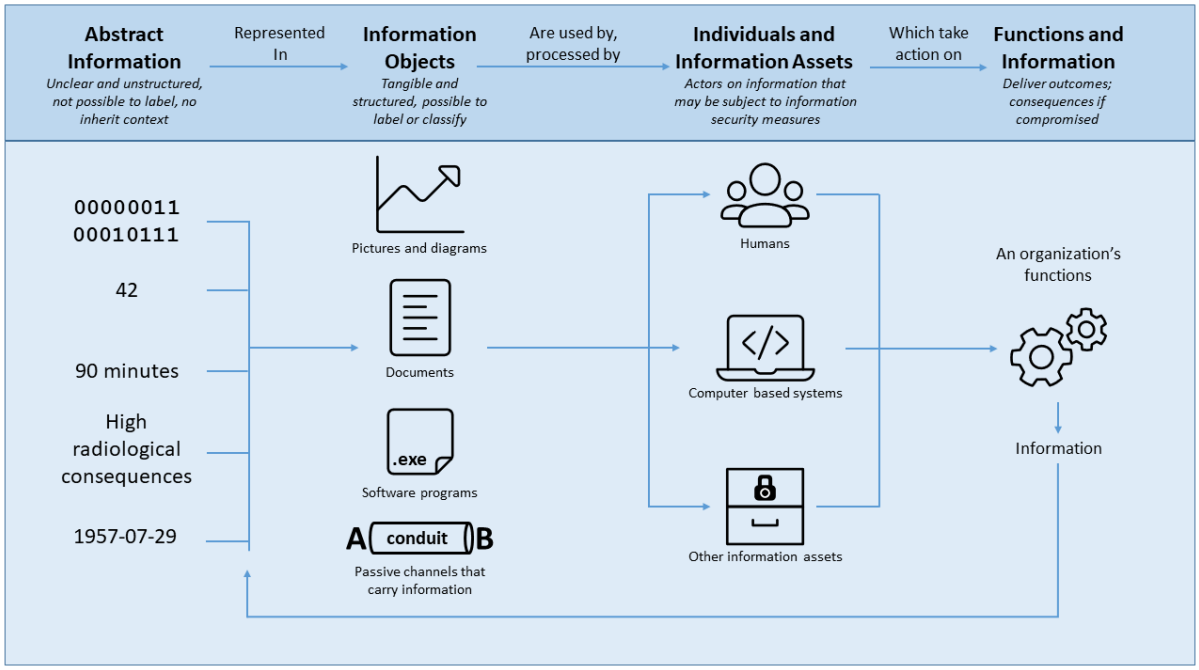

FIG. 2. Conceptual model illustrating the relationship between abstract information, information objects, information assets and the functions performed, with examples.

2.14. An adversary might seek to provoke a consequence by affecting the functions performed in the final column of Fig. 2. The adversary might achieve this 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. Information security measures should be designed to protect information as comprehensively as practicable in both its tangible and abstract forms. Abstract information may need context (i.e. being interpreted as an information object) to determine its value and to implement targeted and specific information security measures. However, untargeted measures (e.g. training on information security), should be applied even if technical measures might not be effective.

2.15. When the information contained in information objects and information assets contributes to the performance of nuclear security related functions, a different value might be attributed to these objects and assets by each of the entities and organizations listed below:

(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;
(f) Third parties and entities in the supply chain (e.g. vendors, contractors, suppliers).
(g) Potential adversaries (e.g. individuals, organized entities);
(h) The media;
(i) The public.

2.16. Each entity or organization could have a different use (i.e. in relation to a function) and perception of the value of information (e.g. the impact of potential consequences it relates to), 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 of little value. To a potential adversary, however, such information might be of high value as it could reveal a weakness or vulnerability that could be exploited in the context of a criminal or intentional unauthorized act. Information should therefore be protected consistent with the highest impact and consequence.

2.17. 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 that is used as a basis for decision making.

SENSITIVE INFORMATION

2.18. Sensitive information can be used by an adversary in the conduct of criminal or intentional unauthorized acts targeting nuclear or other radioactive material and 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 and other radioactive material during transport.

2.19. The information necessary for the performance of a function important to nuclear security or nuclear safety can be considered as sensitive. For example, sensor values that are used to ensure the nuclear safety function to control reactivity are likely to be considered as sensitive information. Sensitive information also includes vulnerabilities that an adversary could exploit to undermine those functions. For example, if a calibration table used to convert sensor values is modified, multiple functions could be adversely affected. If there are high consequences associated with some of these functions the sensor values, the calibration table, the calibration algorithm, and any associated set points should be considered as sensitive information.

2.20. 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 and nuclear safety[11]. 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 modified 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

[11] Authenticity and non-repudiation may also be considered. These properties are sometimes considered components of integrity but can also be treated as distinct information security objectives that strengthen overall information security.

nuclear accident. In such cases the protection of integrity and availability should be prioritized over confidentiality if the potential consequences to nuclear security and nuclear safety are greater.

2.21. 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) Details of the design basis threat (DBT), threat and vulnerability assessments;
(c) Descriptions of nuclear security arrangements at a facility (e.g. physical protection, information security, insider threat mitigation, incident response arrangements);
(d) Software applications or communications (e.g. network communications, process signalling) important to the performance of nuclear security and nuclear safety functions;
(e) Details on the location or the transport of nuclear material and other radioactive material;
(f) Information concerning vulnerabilities in arrangements at ports and airports for the detection of material out of regulatory control;
(g) Details of an organization's personnel with authorized access to nuclear or radioactive materials;
(h) Details of essential equipment and systems;
(i) 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.

2.22. 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 of sensitive information, the rationale for sensitivity, and the potential consequences of compromise are provided in Annex II.

2.23. 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 intentional unauthorized acts. If, for example, an adversary attempting the theft of nuclear or other radioactive material acquires the security plan of a facility, the adversary could gain knowledge of physical protection barriers, the presence of guards and whether they are armed, the size of the response force and the estimated time that it would take the response force to arrive on-site. The security plan would might also indicate the location of important targets within the facility and the established security measures to protect such targets.

2.24. Similarly, an adversary seeking to commit an act of sabotage could attempt to modify 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 execute the attack. Therefore, the compromise of sensitive information by an adversary increases the likelihood that the adversary can negatively impact functions important to nuclear security and nuclear safety.

2.25. The conceptual model illustrated in Fig. 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.

2.26. Access to sensitive information, sensitive information objects, and sensitive information assets should be limited to individuals who genuinely need it to perform their job duties. Similarly, the sharing of sensitive information should be restricted to authorized personnel and resources, based strictly on a 'need-to-know' basis. Authorized individuals should be

identified and authenticated, and lists should be maintained documenting all those individuals with the rights to access sensitive information.

2.27. The 'need to know'[12] and 'least privilege'[13] principles should be used to guide management and control of access rights to sensitive information. This is because 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.

2.28. 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. The measures should be re-evaluated if a previously unknown consequence comes to light, as this could significantly amplify the impact. Specific guidance on measures to protect against internal adversaries can be found in IAEA Nuclear Security Series No. 8-G (Rev. 1), Preventive and Protective Measures against Insider Threats [11].

INFORMATION SECURITY OF SENSITIVE INFORMATION

2.29. Information security for nuclear security, at a minimum, covers the security of sensitive information held, processed and communicated by authorized individuals and sensitive information assets, and the detection of and response to unauthorized access including:

(a) Security of sensitive information objects (e.g. records of sensitive information on paper and electronic media).
(b) Security of sensitive information assets (e.g. information storage, processing equipment, and computer based systems). Detailed guidance on the security of computer based systems and sensitive digital assets can be found in Ref. [6] and Ref. [8].

2.30. The relationship between sensitive information and sensitive information assets is depicted in Fig. 3.

[12] The principle that individuals, processes and systems are granted access to only the information, capabilities and assets that are necessary for execution of their authorized functions.

[13] The principle that a human or a machine has the minimum authority and capabilities to perform their required tasks.

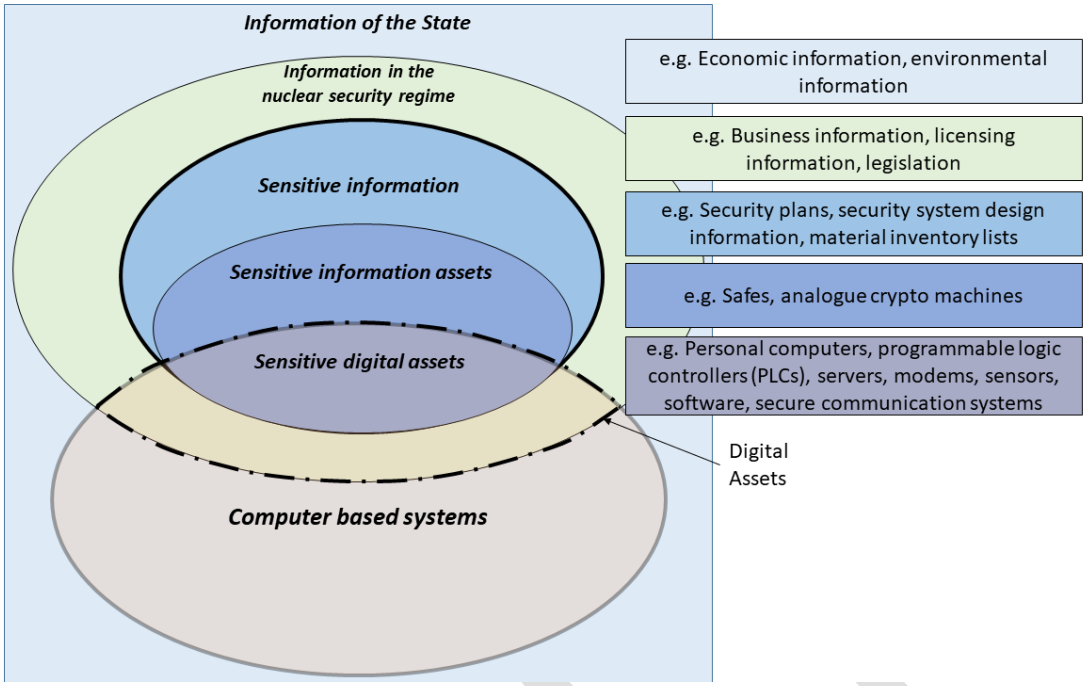

FIG. 3. Relationship between the information and computer based systems in the State and in the nuclear security regime (adapted from Ref. [8]).

2.31. The choice of suitable security measures should be made on the basis of a risk analysis, with the objective of reducing risks to an acceptable level. The State or competent authority should ensure that the risk analysis is kept up to date through a process of periodic review, as part of the 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.

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

2.33. Information security measures for confidentiality will often differ from those for integrity and may be in conflict with information security measures for availability unless they are carefully designed to work together.

2.34. Information security activities should be conducted in accordance with the State's overall legislative, regulatory and policy frameworks 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 that contain sensitive information relating to other physical security measures (e.g. access control databases, site security plans).

2.35. Gaps or deficiencies in one security domain can affect the security of other domains, so it is essential to adopt a comprehensive approach that considers all domains. Legislative, regulatory and policy frameworks for securing sensitive information should also consider the need to take into account other objectives (e.g. relating to operation, transparency and safety) and should provide adequate measures to do so.

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

3.1. Effective legislative, regulatory 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 handle sensitive information within the nuclear security regime. 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.

3.2. An information security policy framework is a structured system that defines how policies, procedures and guidelines are formed to govern how sensitive information is protected and managed across a nuclear security regime.

COMPETENT AUTHORITY FOR INFORMATION SECURITY IN THE NUCLEAR SECURITY REGIME

3.3. States typically have governmental 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 national 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 are not specifically designed for nuclear security.

3.4. 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 [12], provides more information on such responsibilities.

3.5. If there is more than one competent authority for information security in relation to the nuclear security regime, or if 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.

3.6. If a State’s national information security policy framework extends beyond the scope of the nuclear security regime, the competent authority for information security should ensure that the framework is sufficient for nuclear security. If the framework is determined to not adequately address nuclear security, it should be supplemented with the necessary requirements, in a manner that is coherent with the nuclear security regime and the national information security policy framework.

3.7. In instances where the State’s national information security policy framework is deemed by the State to not be sufficiently comprehensive for nuclear security, not directly applicable, or if a more focused approach is preferred (e.g. to provide more effective concurrent oversight of both governmental and commercial entities), an information security policy framework should be established specifically for the nuclear security regime falling under the purview of the competent authority for information security in coordination with the national security authorities (hereafter ‘information security policy framework’ refers to either the

supplemented national framework or a framework established specifically for the nuclear security regime).

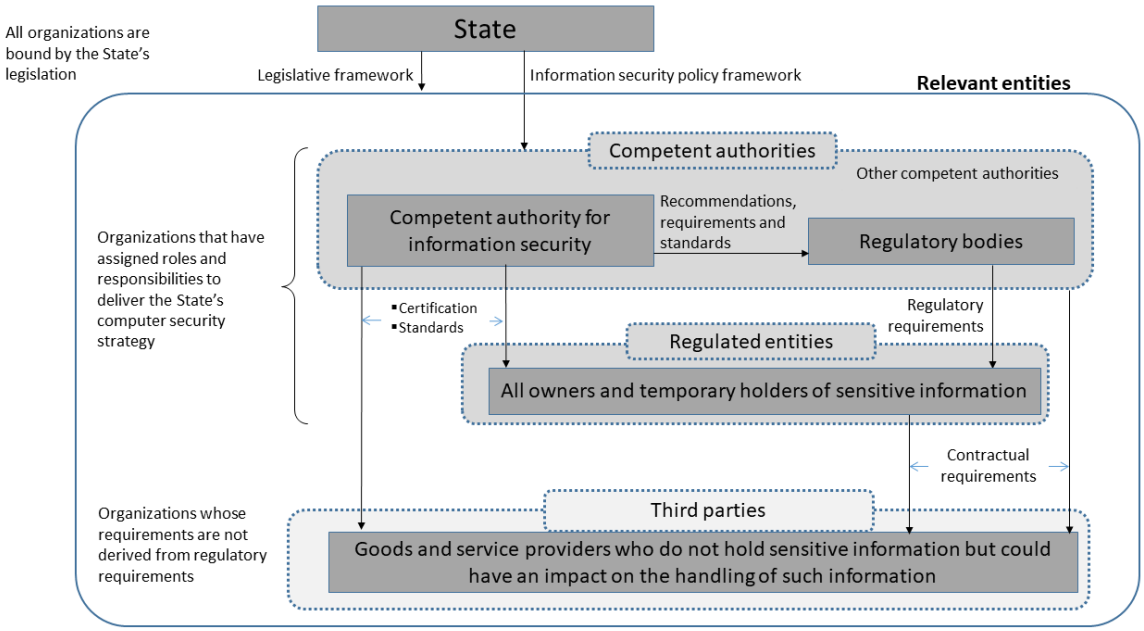

FIG. 4. The relationship between the State and entities relevant to the nuclear security regime for the purposes of information security (adapted from Ref. [8]).

3.8. Figure 4 provides an illustration of the relationship between entities that could have an impact on the security of sensitive information in the nuclear security regime. The figure shows the possible relationship between the provisions of the State's legislative framework and information security policy framework and relevant entities, comprising competent authorities, regulated entities[14] and third parties (e.g. vendors, technical support organizations). 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

3.9. The State should identify and ensure the coordination of all organizations that have a role in the nuclear security regime (i.e. competent authorities, regulated entities and third parties). The competent authority for information security should create a regulatory framework that enables oversight of the adherence by regulated entities to the State's legislative framework and information security policy framework.

3.10. Regulated entities are those organizations that a State has determined hold and process sensitive information or deal with matters necessary for maintaining information security within the nuclear security regime. A State could require any such entity (including authorized persons, providers of commercial goods and services, and competent authorities) to fall within the category of regulated entities and therefore be subject to direct regulatory requirements relating to information security (regulated entities and regulated competent authorities are hereafter referred to collectively as 'regulated entities'). Alternatively, a State could establish

[14] For the purposes of this publication, 'regulated entities' are those entities that have access to sensitive information within and fall under the provisions of the regulation of the nuclear security regime.

separate information security requirements for competent authorities that hold and process sensitive information.

3.11. Some third parties do not retain sensitive information, but they could still have an impact on the security of sensitive information. For example, an equipment vendor might provide technical equipment (e.g. document safes, computer based systems, security equipment) that processes or stores sensitive information to a nuclear power plant operator or a cloud service provider might offer encrypted computational services without access to the underlying data. Although these third parties are relevant entities, they might not fall into the category of regulated entities. They should therefore be subject to controls in order to maintain adherence to the regulations outlined in the information security policy framework. The relevant requirements for these third parties, and for their products or services, could be defined directly or through contractual agreements.

3.12. The State should establish specific provisions within its legislative framework to accommodate legitimate law enforcement activities while maintaining appropriate governance over sensitive information. For international contractors who hold sensitive information but are outside of the national legislative framework, the State should nevertheless ensure that they are subject to controls, through the contracts they sign. Alternatively, the State could demand that international contractors maintain a local presence, so that they have to adhere to the national legislative framework.

3.13. Legislation should also be established to define the competent authorities for information security and the penalties that will be applied to individuals or organizations that breach information security (e.g. suspension of authorization, civil fines, criminal penalties). This legislation should define the severity of, and the corresponding penalties for, specific types of breach (e.g. in relation to confidentiality, integrity or availability of sensitive information, sensitive information objects and sensitive information assets).

3.14. The reporting of information security incidents to the competent authorities should be mandatory, and laws or regulations should specify penalties for failure to make such reports within the defined time frame.

3.15. Competent authorities should have regulatory powers, established through the legislative framework, to place obligations on the holders of sensitive information. Laws enacted for this purpose should impose penalties for the unauthorized disclosure, storage, modification or falsification of sensitive information. The legislation should also mandate specific State ministries, departments, agencies and other entities to provide the competent authorities with the support they need to ensure the security of sensitive information.

3.16. When establishing laws on the definition and implementation of information security as it relates to nuclear security, the State should consider alignment with other laws and with international legal instruments, such as the following:

(a) Laws concerning information and computer offences;
(b) Laws on terrorism;
(c) Laws on the protection of critical national infrastructure;
(d) Laws on the disclosure of information;
(e) Laws on privacy and the handling of personal information;
(f) International conventions (e.g. Refs [2, 3]);
(g) International multilateral and bilateral agreements.

ROLES AND RESPONSIBILITIES FOR INFORMATION SECURITY

3.17. The State should identify all regulated entities 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.

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

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

3.20. Regulated entities 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.

3.21. Many regulated entities operate within an international marketplace where goods and services are supplied from vendors and contractors from other States. This could result in sensitive information having to be sent outside the jurisdiction of the originating State's legislative framework and information security policy framework. In turn, this might undermine enforcement actions relating to breaches of security requirements or the control of legal authorization to access information. To address such issues, the State could sign reciprocal agreements with other States to protect each other's classified information under their own security policy frameworks. The content of these agreements could differ from one State to another. Under these circumstances, it might be necessary for the State to place greater emphasis on the robustness of the operator's contractual requirements, controls and assurance arrangements within its information security policy framework. Other laws or requirements, such as requirements for data sovereignty, originating from outside the nuclear security regime, could also apply to the regulated entity.

INTERFACES OF INFORMATION SECURITY WITH OTHER DOMAINS

3.22. The State should ensure efficient functioning of interfaces between information security and other elements of the national 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, and related aspects of nuclear safety. The State should provide guidance on, or requirements for, how to coordinate such interfaces. Actions might need to be taken that are outside the scope of information security, for example placing requirements on information generated within other domains or applying the disclosure requirements of other domains (e.g. related to freedom of information) to information security.

3.23. The State should ensure that the information security policy framework defines the 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

3.24. The State's information security policy framework should define criteria to identify the information that the State wishes to protect and should indicate how sensitive information is to be protected. The framework should set 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 according to its level of sensitivity, and indicate 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.

3.25. Detailed guidance on how to implement the information security policy framework in the nuclear security regime should be developed by the competent authority for information security, in close liaison with the national security authorities and in consultation with the users of sensitive information within regulated entities. This type of guidance should cover how to define what constitutes sensitive information, how to divide the information classes (see Section 4), and how to ascertain the importance of a particular piece of information, and thus its sensitivity and the degree of protection to be applied.

3.26. 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

3.27. The State's information security policy framework, or the more detailed guidance, should identify clearly the regulated entities within the nuclear security regime that have responsibility for analysing and managing risks and for establishing rules for the protection of sensitive information throughout its life cycle (see Section 5), as well as the regulated entities that have to follow these rules through an information security management system (see Section 6). This delineation can allow some regulated entities 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 information on mandatory measures for the security of sensitive information in the nuclear security regime. Alternatively, the State's competent authority for information security could delegate the responsibility for identifying appropriate measures to a regulated entity that demonstrates sufficient competence, along with the authority to manage certain risks locally with consideration of the national threat assessment or design basis threat. This delegation should be in compliance with the State's legislative framework, information security policy framework, and other elements of the State's nuclear security regime (e.g. a decision made in coordination with the competent authority for computer security should take into account any impacts on the State's computer security strategy, see Ref. [8]) thus ensuring a harmonized approach to risk management across the nuclear security regime.

3.28. The competent authority for information security should also cooperate closely with the other competent authorities in the nuclear security regime and 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 [13].

SECURITY POLICIES AND MANAGEMENT SYSTEM AT THE ORGANIZATION LEVEL

3.29. Each regulated entity and competent authority that handles sensitive information should develop its own information security policy and information security management system, on the basis of guidance provided by the competent authority for information security, so as to comply with the State's information security policy framework and legislative framework. The policy should be communicated to intended users in an accessible and understandable way. Section 6 contains additional guidance on establishing an information security management system.

3.30. The competent authority for information security should indicate national or international standards that may be adopted by regulated entities 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' information security policy and information security management system.

4. IMPACT ASSESSMENT AND CLASSIFICATION OF SENSITIVE INFORMATION

4.1. Implementing information security management systems and associated measures involves both resources and time. It is not feasible to ensure that all the information (in particular information objects and information assets) at a regulated entity is protected in the same manner. A risk-informed, graded approach should therefore be used to protect sensitive information in a manner that is proportionate to the level of sensitivity and the assessed risks of compromise[15]. It is therefore important to identify which information is sensitive, its level of sensitivity and the specific risks associated with it.

4.2. The competent authority for information security should specify how to determine which information relating to nuclear and 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 and potential harmful consequences arising from 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 nuclear security and nuclear safety, and its potential value to adversaries seeking to compromise these functions;
(b) The impact of and potential harmful consequences arising from the compromise of the information's integrity or availability, in relation to decisions made on the basis of the information, considering that the information may be targeted by adversaries as part of an attack designed to mislead human or machine based decision making.

4.3. Information should thus be classified using a graded approach, and a classification scheme should be developed and applied within regulated entities. 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 should be. When applying a graded approach

[15] The accidental or deliberate violation of confidentiality, loss of integrity or loss of availability of information.

consideration should also be given to the potential for aggregated information to warrant a higher classification, even if individual components are less sensitive.

4.4. Some information that is not considered to be sensitive by the nuclear security regime could be considered sensitive for other reasons (e.g. the reliability of electricity generation by a nuclear power plant, nuclear safeguards, privacy related regulations). Regulated entities might need to take these factors into account in identifying sensitive information.

4.5. The competent authority for information security should specify who is responsible for the classification of sensitive information, either in the information security policy framework, in the information security management system of the competent authority or regulated entities, or both.

SCALE OF IMPACT FOR SENSITIVE INFORMATION

4.6. The State might find it helpful to establish a common scale of nuclear security impacts linked to a classification scheme, an example of which is 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.

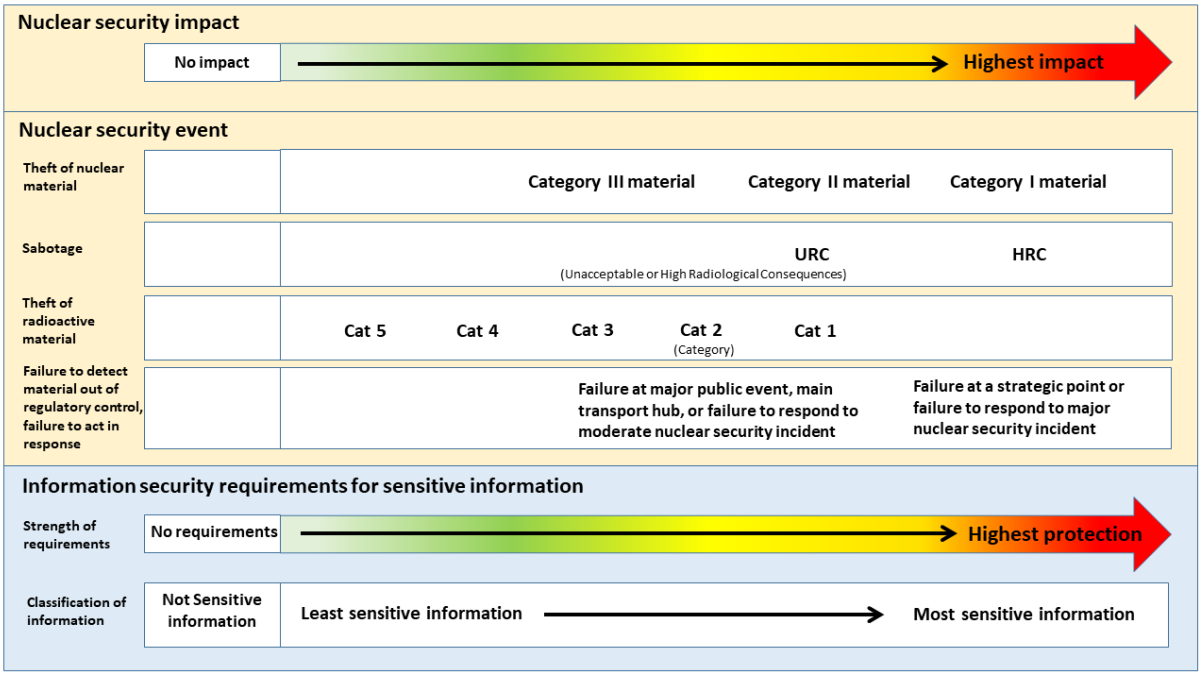

FIG. 5. Example common scale of impact and a graded approach to protecting sensitive information (adapted from Ref. [8])[16].

CLASSIFICATION OF SENSITIVE INFORMATION

4.7. 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

[16] Figure 5 relates to sensitive information, the compromise of which might have an impact on the nuclear security regime. Other information is likely to be held that, if compromised, will not affect nuclear security or its interfaces with nuclear safety (indicated as 'no impact' in Fig. 5). The information security requirements for such information are considered outside the scope of this publication.

in selecting the number of impact levels and the corresponding information security classifications:

(a) Very complex classification systems with many levels might become cumbersome and prove to be impractical.

(b) Very simple systems might not provide sufficiently precise classifications.

(c) Overclassification (i.e. requiring more stringent security than is necessary) can lead to unnecessary additional expense for regulated entities and conflict with transparency policies, whereas underclassification (i.e. requiring less stringent security than is necessary) can put sensitive information at an unacceptable risk of compromise.

4.8. When designing and implementing the classification scheme, a balance should be achieved between the need for completeness and the need for practicality. The classification scheme should be accompanied by effective guidance that allows personnel in the nuclear security regime to easily understand and use the scheme. When developing such guidance the following might be taken into consideration:

(a) The accumulation of information, and logical or physical points of aggregation. For example, collections of non-sensitive information objects could become sensitive information objects if the relationship between the non-sensitive information objects provides additional context for an adversary. In this case, the non-sensitive information objects may be managed as sensitive information).

(b) Large collections of sensitive information represented in one information object or stored in an information asset could warrant a more stringent classification and more stringent associated requirements than when the sensitive information is classified individually.

(c) The compromise of information at a regulated entity could affect other entities and the functions they perform, having a broader impact on the nuclear security regime.

(d) The usefulness of specific information to an adversary might not be clear to the individual(s) assessing the information.

(e) The value of information can often be complex to determine, and multiple individuals may have differing perceptions of the value. It can also be difficult to identify the most appropriate individuals to determine the classification of information but methods to identify this may be provided in guidance (e.g. through understanding the relationship to functions and consequences as described in Section 2).

(f) Labelling and classification schemes have long existed to assess the confidentiality of information, but these schemes may not have considered 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, or personnel implementing them, as being applicable to the integrity and availability of information).

(g) The information security policy framework for implementing a classification scheme should consider the practicalities of labelling information objects (including through metadata). Consideration should also be given to the practicalities of enforcing restrictions on the processing of labelled information objects by information assets as well as how associated requirements will be implemented in computer security measures (see Ref. [8]);

(h) Guidance may be more effective if targeted at the classification and protection of information objects and information assets, as the value of the sensitive information represented or contained within them will be more apparent (see para. 2.8);

(i) The need for classifying certain information objects and information assets may change over time as the understanding of threat capabilities and the consequences evolve (e.g. through a periodically updated threat and risk assessment).

(j) Information that has been identified as sensitive but has not yet been classified should initially be managed using a conservative approach in order to prevent inappropriate sharing and disclosure of information.

4.9. A possible classification scheme for sensitive information, with classes that indicate the level of confidentiality of particular information objects, could be determined and could contain the following levels, in descending order[17]:

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

4.10. The protection of sensitive information within the nuclear security regime depends on maintaining a balance between availability, integrity and confidentiality that is necessary to ensure that the function is protected from the consequences of compromise. For example, measures to protect the availability of information could differ from those to protect the confidentiality of information.

4.11. Classification schemes for sensitive information have traditionally been designed in response to the potential impact 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 approaches:

(a) Extending the use of established classification labels (e.g. secret) to encompass all aspects of confidentiality, integrity and availability. This 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 (e.g. Secret-C, Confidential-I, Restricted-A). However, this solution could be overly complicated for users.
(c) Utilizing technology to manage complex classifications (e.g. an information management system that enforces multi-dimensional classification schemes while presenting simplified interfaces to users). This may reduce reliance on the understanding of the person performing the classification.

4.12. Some example definitions for the classification labels ‘secret’, ‘confidential’ and ‘restricted’ are given in Annex I. These definitions can be applied in relation to confidentiality, integrity and availability.

4.13. Additional caveats[18] for information security could indicate restrictions on the distribution of sensitive information, in accordance with the nature of the information, or enhance the ‘least privilege’ or ‘need to know’ principles, which allow only users who have a legitimate need to access the information. Examples of caveats include the following:

(a) No further distribution;
(b) Distribution controlled by the originator;
(c) Restricted distribution;
(d) Not releasable to foreign nationals.

[17] In many States, there is a higher classification of ‘top secret’, but it is almost never used in the civilian sector.

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

4.14. In the case of international activity that involves the sharing of information between States or with an organization that falls 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.

4.15. Examples of information that could be identified as sensitive information that is classified and handled in accordance with information security measures [9], includes information in the following categories:

(a) Details of physical protection systems, computer security measures and any other security measures established for nuclear and other radioactive material and associated facilities and activities, including information on the performance of physical protection elements, command and control procedures, guards and response forces and arrangements relating to transport security;
(b) Information relating to the quantity and form of nuclear and other radioactive material in use or storage, including nuclear material accounting information;
(c) Information relating to the quantity and form of nuclear and other radioactive material in transport[19];
(d) Information relating to the facility and its operations, the misuse of which could compromise safety and security;
(e) Detailed information relating to both the physical and digital storage location of sensitive information;
(f) Authentication credentials for and details of computer systems, including communications systems that process, handle, store or transmit information that is directly or indirectly important to nuclear safety and security;
(g) Information crucial to the correct performance of computer systems;
(h) Contingency and response plans for nuclear security events;
(i) Personal information about employees, vendors and contractors;
(j) Threat assessments and information concerning security alerts;
(k) Details of vulnerabilities or weaknesses that relate to the above topics;
(l) Historical information on any of the above topics.

4.16. Some information in the categories listed in para. 4.15 (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.

4.17. 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.

[19] For safety reasons, such information may be required to be displayed on transport packaging in accordance with national and international transport regulations.

5. 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 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 a generic four stage[20] information life cycle, as illustrated in Fig. 6.

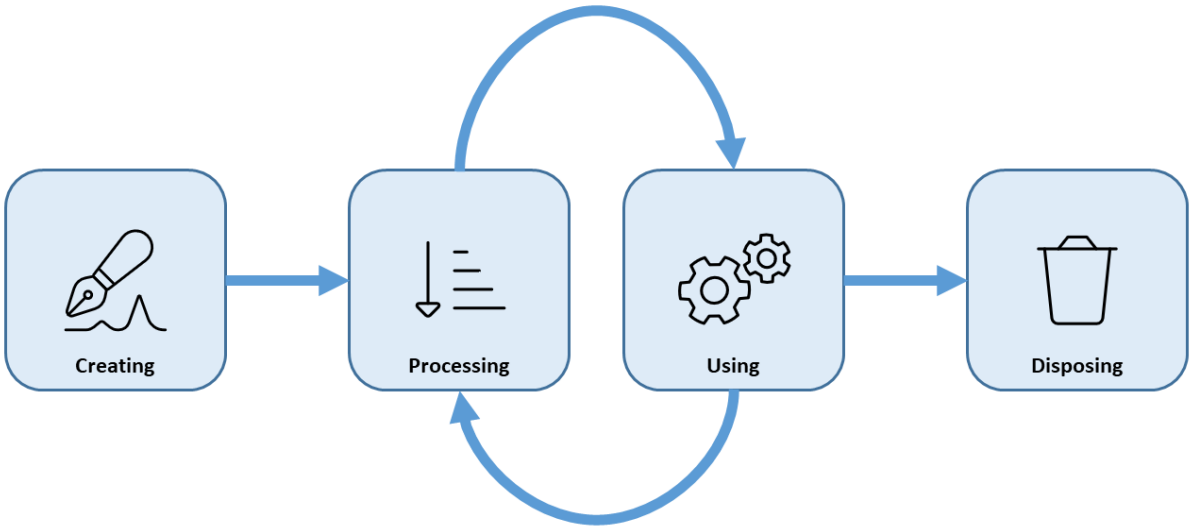

FIG. 6. The four stages in a generic information life cycle and the relationships between them.

5.2. The four stages depicted in Fig. 6 are the following:

(1) Creating: assembling an information object from abstract information or other information objects, including activities such as the collection and classification of information;
(2) Processing: activities performed on information objects created before and throughout their active use (e.g. handling, transmission and storage activities);
(3) Using: activities that leverage information during the performance of functions, including the sharing, replication, dissemination, disclosure, reclassification and further processing of information;
(4) Disposing, including archiving and destroying information.

5.3. Annex IV shows how the information life cycle activities described in other publications can be mapped to the generic four stage information life cycle described in this section.

CREATING INFORMATION

5.4. Information is generally created in an abstract, unstructured and unlabelled form (see Fig. 2). For example, a person could record the maximum number of guards on duty at a nuclear power plant without any context, or a machine could generate a stream of binary data representing observations from a sensor that is measuring temperature or pressure.

[20] There is no single, universally recognized information life cycle, but most have between four and seven stages.

Weaknesses and vulnerabilities could exist in terms of the management and security of this information, until the information is labelled and classified.

5.5. It is only when information is structured and labelled as part of an information object that it can be identified as sensitive, 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 nuclear security and nuclear safety), and the value to adversaries seeking to cause harm by subverting those functions, which can be evaluated relative to the design basis threat, threat or vulnerability assessments. In order to perform the process of structuring and labelling information in a uniform and repeatable way, regulated entities need guidance in applying a classification scheme (see Section 4).

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

PROCESSING AND USING INFORMATION

5.7. The computer based systems and humans that process and use information fall under the category of ‘individuals and information assets’ indicated in Fig. 2). In general, only they have the necessary ability to apply information security controls to the information objects containing sensitive information. A computer based system could be, for example, an IT system that processes documents, a control system that performs functions in a nuclear power plant, or an information management system. Computer based systems and humans can implement a classification guidance to apply security measures to the level of protection necessary for a specific information object (e.g. a document or a computer program) through an information security management system (see Section 6).

5.8. 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 sensitive information. Locked cabinets can be used to protect the confidentiality and integrity of information (e.g. documents, physical media). 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. However, both locked cabinets and cryptography can have a negative impact on the availability of information for authorized users.

5.9. 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 transport.

5.10. The access of individuals to sensitive information should be controlled by a procedure that grants access on the basis of the ‘need to know’ principle and rescinds 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, to provide resilience and to 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).

5.11. 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.

5.12. An assessment to determine which authorized individuals 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 work if this would reduce the risk of a nuclear security event occurring.

5.13. With the widespread use of computer based systems to process and use information, the information security measures implemented to address the concept of replication have now changed. It is increasingly difficult to control sensitive information by controlling the number of copies of documents that exist, for example by focusing information security measures on the means of replication (e.g. photocopiers for physical documents). The regulated entity'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.

5.14. Traditional information security measures can be impractical for enabling the use of information whose sensitivity has a brief lifespan, for example during the transport of nuclear and other radioactive material. Paragraph 5.45 of IAEA Nuclear Security Series No. 9-G Rev. 1, Security of Radioactive Material in Transport [14] states that:

> "When a security related message is transmitted, care should be exercised in the handling of the information to ensure its protection. When open communications are used, techniques such as code words and phrases should be considered."

5.15. 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 meaning can be quickly inferred on the basis of context and to use this strategy only when other security measures are not feasible or proportionate. Authorized users should be pre-informed about the context of the code words and the expected responses 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 and sharing of information outside the regulated entity

5.16. Since nuclear security responsibilities are not typically confined to one entity, it is often necessary for information to be disseminated among regulated 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 could also arise, for example, among State agencies, between regulated entities handling nuclear and 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. 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.

5.17. There may also be a need to disclose sensitive information to other regulated entities or to the public in a manner that was unanticipated and therefore not specifically planned.

5.18. Both sharing and disclosure should be managed in a way that ensures that sensitive information does not inadvertently reach 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.

5.19. 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 sharing of information between authorities should be governed by the State's security procedures. The sharing 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 ensure that all sensitive information is equally protected from compromise.

5.20. 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 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, see para. 5.23) in any one State might affect the handling of the other States' sensitive information.

5.21. In practice, most information is shared using computer based systems, meaning that computer security controls are needed to avoid the compromise of the confidentiality, integrity or availability of sensitive information as it passes between jurisdictions. Further guidance on computer security controls can be found in Ref. [8].

Need for disclosure of sensitive information

5.22. Most States have laws to address the security of information that is of importance to national interests. Such laws specify penalties that will be imposed if a person (a national of either that State or another) breaches these information security laws.

5.23. Some States have freedom of information legislation 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 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 relating to the nuclear regime can be withheld to protect national security.

5.24. 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.

Development of guidance on disclosure

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

5.26. 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, to whom and by which means;
(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 to be used in conference presentations, web posts 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.

5.27. Given that circumstances evolve, information that was once considered sensitive and unsuitable for disclosure might become less sensitive and more suitable for disclosure over time (or vice versa). All guidance should therefore be reviewed and updated periodically and whenever there are significant changes in policies or circumstances.

Disclosure and reclassification of information

5.28. 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 disseminated. Difficulties in reclassification should be considered when first classifying the information, along with finding an 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 (see para. 5.29).

5.29. Disclosure and reclassification of information share many common practices. When considering disclosure or reclassification of sensitive information relating to the nuclear security regime, regulated entities should implement a formal review process. The reclassification process should be documented and include appropriate justification for any changes in classification levels. Reclassification might be undertaken to take into account:

(a) Changes in security threats and vulnerabilities;
(b) Changes in technology that might affect the sensitivity of information;
(c) Changes in the operational requirements or status of a nuclear facility;
(d) International or national agreements and obligations that might affect information handling requirements.

5.30. All requests to a regulated entity for disclosure or reclassification 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. 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. 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.

DISPOSING OF INFORMATION

5.31. The State's legislative and policy frameworks should define the rules for the retention, archiving, downgrading or declassification, and destruction of sensitive information that is no longer in use. In general, sensitive information should be kept only as long as needed, with sufficient information retained for the State's public record. In relation to the nuclear security regime, certain sensitive information, such as the following, may need to be archived for historical, legal or national security purposes:

(a) Records of nuclear material accountancy;
(b) Historical design information of nuclear facilities;
(c) Records covered under treaties and international agreements.

5.32. The archiving of such information should be managed by the regulated entity under direction from the competent authority for information security or the relevant authority for the archives of the State. This authority should implement standardized procedures for assuming custody of sensitive information, maintaining secure storage facilities, managing access controls, and ensuring the long-term preservation of archived sensitive information if the regulated entity ceases operations.

5.33. The destruction of sensitive information should transform the information beyond recognition and recovery, by any means available within the lifetime of the sensitive information, and should be aligned with international standards and good practices. For example, if the information is expected to be sensitive for many decades, the means of transformation and destruction (e.g. cryptographic methods[21]) 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 (see Section 3) should be implemented and sustained within a regulated entity, using an information security management system. With the widespread use of computer based systems within the creation, processing, and utilization of sensitive information, many of the elements of an information security management system described in this section may be addressed wholly or partly within a subordinate computer security programme as detailed in Ref. [8].

6.2. Each regulated entity within the State's nuclear security regime should develop its own information security policy in collaboration with the State's competent authority for information security. The policy should articulate high level goals, objectives and requirements for information security and represent senior management commitment and accountability. It should also reflect the extent of autonomy granted to the regulated entity in managing information security risks. For instance, smaller entities with simple nuclear security responsibilities could be required to adhere to a strict set of 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

[21] It is possible that the advent of quantum computing might undermine traditional public-key cryptographic methods, as quantum algorithms can efficiently solve underlying mathematical problems.

security policy to adhere to a number of regulatory systems and addressing their associated risks.

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

6.4. The establishment of goals, objectives and requirements should be effectively managed and subsequently maintained through the information security 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. An example of such a cycle for an information security management system is depicted in Fig. 7.

6.5. The information security management system should be part of the regulated entity's integrated management system (i.e. alongside safety, quality, physical security and computer security) system to ensure a holistic, balanced and risk-informed approach to overall management.

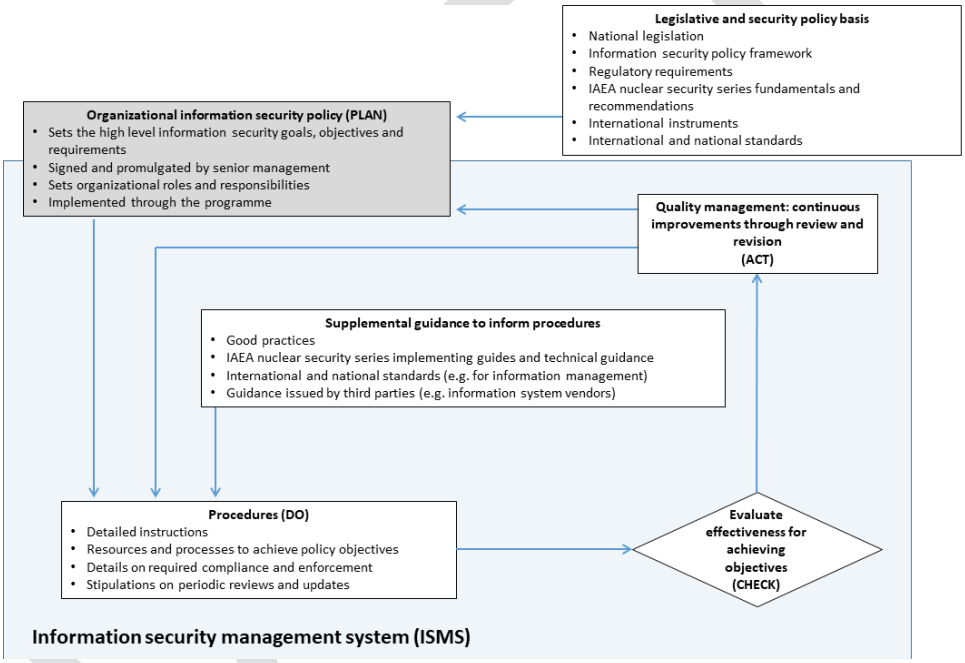

FIG 7. An example of a 'plan, do, check, act' cycle for the continuous improvement of the information security management system (adapted from Ref. [8]).

6.6. An information security management system is a regulated entity'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 should encompass a comprehensive set of subordinate procedures and processes (e.g. procedures for the assessment of risk and subsequent treatment through technical, administrative, physical or other interconnected security measures) designed to provide for the security of sensitive information, sensitive information objects and sensitive information assets.

6.7. 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 should be 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 their term of employment.

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

6.9. The information security management system should take into consideration the risks identified within its scope, to support the regulated entity in addressing the design basis threat or threat statement and in fulfilling regulatory requirements in accordance with the State's information security policy framework. The risk management objectives are to reduce risks to an acceptable level through the application of adequate information security systems and measures throughout the life cycle of sensitive information (see Section 5).

6.10. The information security management system may be integrated at all levels of the regulated entity, and interdependencies with other processes and management systems may be recognized and leveraged. This integration may also extend beyond the regulated entity's boundaries to encompass third parties with information security responsibilities, where appropriate. The integration of external parties can ensure a comprehensive approach to information security.

6.11. The information security management system, including all subordinate policies, procedures and processes, should be formally documented (e.g. bearing an official status, endorsed and promulgated, registered as authoritative in an enterprise document management system). 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.

6.12. 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.

6.13. The regulated entity should ensure that the necessary resources are available for the implementation of information security. Such resources encompass the information resources, financial investments and the personnel necessary to maintain and enhance the regulated entity's information security posture.

6.14. A regulated entity's senior managers should visibly demonstrate their commitment to information security, including by 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

6.15. A robust nuclear security culture is particularly important for information security in the nuclear sector because of the broader set of personal responsibilities involved, as described in IAEA Nuclear Security Series No. 7, Nuclear Security Culture [15].

6.16. The assessment of nuclear security culture within an organization should include information security. The results should be used to evaluate the effectiveness of the

information security management system, to refine awareness programmes, to adjust security measures and to enhance personnel behaviours, taking into consideration human factors engineering. People and processes that complement the use of technology are key factors in securing information; information security should be an integral part of nuclear security culture programmes to ensure the sustainability of nuclear security.

6.17. All personnel within the regulated entity 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 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 to 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;
(d) Provides examples of adversarial actions that might compromise the confidentiality, integrity or availability of sensitive information and sensitive information assets (e.g. social engineering, phishing).

6.18. All personnel should fulfil their security responsibilities, and the regulated entity should provide appropriate education and training to ensure the competence and accountability of personnel 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.

6.19. Regulated entities that create sensitive information and operate sensitive information assets should designate information owners with specific responsibilities and accountabilities for determining and verifying the information security arrangements for sensitive information under their purview.

6.20. The regulated entity should provide the following personnel with specific training on their responsibilities:

(a) Personnel with specific, security related responsibilities;

(b) Personnel with access to sensitive information;

(c) Information owners and managers accountable for information security at all levels of the organization.

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.

6.21. One-off information security training courses might not adequately reinforce the knowledge imparted, with the result that personnel become complacent in the long term. All individuals who handle sensitive information, including 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 the 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. An example format and content for a training programme is provided in Annex III.

SECURITY MEASURES

6.22. The handling of sensitive information should be governed by policies and procedures, in accordance with the regulated entity'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, based on a graded approach, should be described in the information security management system. For example, requirements might be established for the minimum cryptographic algorithm security lifetime (i.e. how long sensitive information protected by the cryptographic algorithm could be expected to remain secure) used for the electronic transmission of information.

6.23. 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, in a risk-informed approach, and to meet the relevant requirements. These security measures should encompass information security, computer security (see Ref. [8]), physical protection and personnel security.

6.24. 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 to ensure 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 access to information with a low classification level, the regulated entity should decide whether any determinations are necessary; if deemed necessary, a limited check of an individual's background could be sufficient. For access to information with a higher classification level, a more comprehensive set of background checks should be undertaken 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. The obligations under such an agreement should be reinforced during activities associated with the cessation of employment.

(c) Physical protection measures should combine 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. safes, vaults or other secure containers).

(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.g. through cryptographic methods).

(e) A system should be in place to identify, monitor and assess potential security incidents, encompassing both physical and digital threats to sensitive information, while enabling a timely response to unauthorized access attempts, or anomalous activities that could compromise information confidentiality, integrity or availability.

(f) Interfaces with a subordinate computer security programme should address computer security aspects of sensitive information assets, objects and digital collections of sensitive information (see Ref. [8]).

6.25. 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 (e.g. the implementation of workplace monitoring systems).

ARRANGEMENTS WITH THIRD PARTIES

6.26. As described in para. 3.10, third parties might provide goods or 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.

6.27. 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 (e.g. relating to sensitive information placed in the care of the third party). Regulated entities entering into contracts with third parties should adhere to any national policies or legislation covering such agreements.

6.28. It is the responsibility of the contracting regulated entity, 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, although not necessarily identical in terms of the measures involved.

6.29. The contracting regulated entities should ensure that any third parties with access to sensitive information operate an information security management system. In addition, the contracting regulated entity should ensure the following:

(a) The third party has established a contact point to direct and manage security in coordination with the contracting regulated entity;
(b) Security arrangements at the third party’s premises can be regularly inspected by the competent authorities or regulated entities, in accordance with the provisions of the legal agreement.

MANAGING ACCESS TO SENSITIVE INFORMATION

6.30. A system should be in place to control why, when, to what extent and how specific individuals and information assets are authorized to access or modify sensitive information and sensitive information assets. The following should be defined for such a system:

(a) Responsibilities regarding the management of authorization to access sensitive information;
(b) Who has the right to access and modify sensitive information and sensitive information assets, and who has the right to grant further access;
(c) How to verify, control and supervise the function of granting access;
(d) Processes to determine the duration of an authorization to access sensitive information and sensitive information assets;
(e) Processes to revoke authorization to access sensitive information and sensitive information assets due to an incident, employee turnover, and changes in job functions;
(f) Processes to maintain full traceability in managing authorizations to access sensitive information and sensitive information assets.

ACTIVITIES FOR INSIDER THREAT MITIGATION

6.31. The information security management system should interface directly with the regulated entity's insider threat programme.

6.32. Reference [11] 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*" [1].

6.33. Independent, non-repudiable systems should be used to detect and alert on insider activities. Such systems should be capable of identifying unusual (e.g. large volume, unexpected time of day) or unauthorized sensitive information transfers (i.e. data loss prevention).

6.34. Paragraph 4.10(c) of Ref. [11] states that preventive measures against insider threats can be used "to minimize opportunities for malicious acts by limiting access, authority and knowledge of insiders." One way of accomplishing this is by dividing critical functions into two parts that necessitate separate authorizations (i.e. use of the 'two person rule').

ASSURANCE ACTIVITIES

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

6.36. 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's corrective actions.

6.37. The regulated entity should also ensure that there are internal resources and established processes to conduct self-assessments and independent audits. These self-assessments and audits should ascertain whether the regulated entity's approach to information security complies with its information security policy, and whether the approach is in compliance with the State's regulatory and policy frameworks. The regulated entity may establish internal training on self-assessments and audits, so that they can be conducted by personnel who are familiar with the internal requirements, procedures and systems. The advantages of conducting such internal activities are that they can be done more frequently than external inspections and they identify different opportunities for improvement.

6.38. 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, consideration should be given to confidentiality and trustworthiness when sharing sensitive information.

6.39. The results of self-assessments, internal audits and external inspections should highlight specific areas for action or improvement. Preventive and corrective actions should be identified by the competent authority for information security or regulated entity, with specific time frames assigned. There should be a mechanism in place to follow up on the implementation and effectiveness of these actions.

6.40. The regulated entity's information security management system relies on the 'plan, do, check, act' cycle for continuous assessment and improvement (see Fig. 7). This cycle should

also 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

6.41. Information security incidents, particularly those stemming from criminal or intentional unauthorized acts, necessitate an adaptable response strategy. These incidents can range from unauthorized disclosure of sensitive information to malicious modification of sensitive information, with a corresponding nuclear security impact (see Fig. 5). Incident response is necessary in relation to both digital and physical collections of sensitive information (i.e. sensitive information objects and sensitive information assets).

6.42. While this section provides the overall framework for information security incident response, additional guidance on technical aspects of computer security incident response specific to nuclear facilities can be found in Appendix 1 of Ref. [9].

6.43. The regulated entity 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 any type of information security incident (i.e. loss of confidentiality, integrity and/or availability).

6.44. A designated team within the regulated entity should establish and document the elements necessary for an effective response to information security incidents. These elements may be formally documented either as a dedicated, standalone incident response plan, or as an integrated section within another relevant response plan such as a contingency 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 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). The different levels and categories of incident could be determined, as well as who should be notified for each level and category.
(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 within the regulated entity, 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 and safety 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 and nuclear safety. The impact on relevant interested parties should also be assessed.
(g) Outline methods to recover information and information assets that have 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 any legal requirements arising from the incident, such as reporting obligations, data protection laws, and 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) Provide for a post-incident review process to analyse the incident, identify root causes and integrate improvements into the response plan.

6.45. The incident response plan should be subject to continual improvement, based on feedback from exercises, drills, lessons identified during actual incidents, and operating experience from other organizations.

6.46. The information security management system should include security measures for all stages in an information security incident, including the detection of suspicious activity (e.g. unauthorized exfiltration of sensitive information), the expeditious alert of personnel, monitoring of the incident, and ongoing verification of the integrity and availability of backups of information and information assets.

6.47. After an incident, the timeline of the incident should be established and its root causes identified. Lessons should be integrated into the regulated entity'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.

6.48. Some information security incidents occur without any prior indication, whereas others develop gradually through a series of minor events that initially go unnoticed, accumulating over time until they manifest as significant security consequences. Recognition of these smaller events within the incident response plan provides valuable opportunities for early detection and preventive action.

6.49. The regulated entity should report significant incidents or breaches of information security in the nuclear security regime to the competent authority for information security and to other necessary authorities in accordance with the State's laws or regulations.

6.50. Regulated entities should establish formal reporting arrangements to ensure that all information security incidents are communicated appropriately 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.

6.51. All information security incidents should be investigated by the regulated entity. Policies and procedures governing the investigation of information security incidents should be defined by the regulated entity 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 is the failure to lock up or secure a document properly, with no result in terms of the loss or compromise of information. An example of a major incident is the theft of a highly sensitive document outlining security procedures, resulting in a significant risk to the regulated entity.

6.52. The competent authority for information security should maintain records of the number and type of information security incident reported. Recurring incidents or trends should be identified and the need for changes to the information security policy framework or for improvements in the information security management system should be considered.

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

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

[4] 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).

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

[6] EUROPEAN POLICE OFFICE, 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).

[7] 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).

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

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

[10] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, INTERNATIONAL ELECTROTECHNICAL COMMISSION, Information Technology – Security Techniques – Information Security Management Systems – Overview and Vocabulary, ISO/IEC 27000:2018, ISO, Geneva (2018).

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

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

[13] 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).

[14] INTERNATIONAL ATOMIC ENERGY AGENCY, Security of Radioactive Material in Transport, IAEA Nuclear Security Series No. 9-G (Rev. 1), IAEA, Vienna (2020)

[15] 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

1–1. This Annex 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 relate to the following levels of classification:

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

In many States, there is a higher classification of 'top secret', but it is not discussed in this Annex since it is almost never used in the civil nuclear sector.[1]. The three levels used in this annex are the following:

1–2. 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, in particular if sensitive information can be derived from these items or objects through visual observation

1–3. 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 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 intentional unauthorized act that could cause grave damage to a facility with nuclear or other radioactive material, or during the transport of such material.

1–4. The compromise of information or material classified as 'confidential' would be likely to fulfil the following criteria:

(a) Damage diplomatic relations between States;
(b) Threaten 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;
(f) Impede the investigation of, or facilitate the commission of, serious crimes;

[1]In exceptional cases, in particular relating to highly sensitive intelligence information that directly impacts national security and concerns the capabilities of specific and imminent credible threats targeting facilities or material, or to the prevention of, or response to, a nuclear security event, a 'top secret' classification might be warranted.

(g) Seriously impede the development or implementation 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 intentional unauthorized act that could cause serious damage at a facility with nuclear or other radioactive material, or during the transport of such material.

1–5. 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 earning potential to individuals or companies, or facilitate improper gains or advantages for an adversary;

(e) Threaten 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 intentional unauthorized act that could cause significant damage at a facility with nuclear or other radioactive material, or during the transport of such material.

1–6. The above classification levels can be applied to ensure the control of sensitive information relating to the nuclear security regime, 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 and other radioactive material;

  (iv) Security plans, procedures and capabilities;

  (v) Existing vulnerabilities of the security systems and computer based systems documented in audits, inspections and drills, which have not yet been eliminated.

(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.

(e) Dispersing nuclear or other radioactive material in the environment using information on the location, form and quantity of such 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 and nuclear security;
   (ii) Disrupting the availability of sensitive information or sensitive information assets used for 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) Modifying or obstructing access to sensitive information regarding the safe and secure transport of nuclear and other radioactive material, its use or storage.

Annex II

EXAMPLES OF SENSITIVE INFORMATION RELEVANT TO NUCLEAR SECURITY

II–1. This Annex provides examples of information relevant to nuclear security that might be considered sensitive. Each State decides the exact level of classification to be applied to each item of information, or produces guidance within the information security policy framework on delegating this decision to regulated entities. Table II–1 presents examples of sensitive information categories and identifies the sensitivity issues associated with each category.

II–2. The categories of information presented in Table II–1 are not intended as a comprehensive list or model; they are simply indicative of what might be considered sensitive information. The relevance of each category and its potential inclusion in a national classification system are to be decided on the basis of a specific assessment by the State.

II–3. The whole table is split into 15 sections, each corresponding to a different area relevant to nuclear security. The first column of the table indicates the category of information and lists types of information that are included in each category. The second column gives references that indicate to which specific topic this category is usually applicable, as follows:

(a) Nuclear material and nuclear facilities: IAEA Nuclear Security Series No. 13, Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5) [II–1];
(b) Other radioactive material and associated facilities: IAEA Nuclear Security Series No. 14, Nuclear Security Recommendations on Radioactive Material and Associated Facilities [II–2];
(c) Detection of and response to material outside of regulatory control: IAEA Nuclear Security Series No. 15, Nuclear Security Recommendations on Nuclear and Other Radioactive Material out of Regulatory Control [II–3];
(d) A combination of the above.

The third column indicates what kind of sensitivity this information could be considered to have (i.e. in terms of its confidentiality, integrity or availability), if any. The fourth column provides an explanation for the sensitivity indicated in the previous column and the rationale for securing the information.

II–4. The identification of sensitivity given in the third column, and the explanation and rationale given in the fourth column are provided as non-exhaustive examples only.[2] For most categories of sensitive information, a combination of confidentiality, integrity and availability sensitivities apply even if only one or two are specified in the table. Many categories may address aspects of computer security, detailed guidance on computer security is provided in IAEA Nuclear Security Series No. 42-G and Computer Security for Nuclear Security [II-4] and IAEA Nuclear Security Series No. 17-T (Rev. 1), Computer Security Techniques for Nuclear Facilities [II-5].

II–5. When designating the sensitivity of information and assigning classification level, the State might give consideration to whether the information is in the public domain or has previously been compromised. It might be impractical to assign and manage a classification level for such information.

[2] The availability of all sensitive information may be important to legitimate business operations. Similarly, the integrity of most information is necessary for effective decision making. The confidentiality, integrity or availability attributes listed in the third column represent examples of security concerns relevant to nuclear security. Other attributes, explanations and rationales may apply, depending on the specific context, implementation and use case among other factors. These will vary among regulated entities.

II–6. Consideration could also be given to designating non-sensitive information as sensitive if it can be combined with other non-sensitive information to reveal sensitive information.

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

Category of information	References	Sensitivity	Explanation for sensitivity
1. SECURITY OF MATERIAL AND FACILITIES			
1.1. Regulations and guidance			
A. National security regulations governing the use of nuclear and other radioactive material	[II-1], [II-2], [II-3]	Not sensitive	Such information is typically in the public domain.
B. Guidance on 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, it could contain details of standards, types of equipment, procedures and security operations at a nuclear facility. Such details could be of use to adversaries planning a criminal or intentional unauthorized act.
1.2. National nuclear security policies			
A. General government policies on matters involving nuclear and 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.

1.3. Facility security plan	[II-1], [II-2]	Confidentiality	The plan typically contains detailed descriptions of the security measures in place at the site and precise details of where material is stored within the site. For nuclear facilities, such plans 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 bypassing 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 bypass security measures and could assist them in 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 insider could seek to modify such investigation data. This modification 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 measures.
1.5. Construction details			

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 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 could help adversaries to bypass security measures and could possibly assist them in targeting a facility for sabotage purposes.
1.6. Physical protection systems			
A. The computer code 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 could leave sensitive areas vulnerable to unauthorized access or to criminal or 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 could be of use to adversaries who wish to defeat the security systems at a facility.

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 these details to understand limitations in the access control systems or to prepare for 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 insider might modify the protocols or the lists of authorized personnel to obtain unauthorized access to sensitive material. Such changes might go unnoticed if the modified records are perceived as legitimate.
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.
1.10. Other matters associated with physical protection (e.g. location, layout, staffing and equipment of the central alarm station; location of the secondary alarm station; type of inner area barrier)	[II-1], [II-2]	Confidentiality	Details of this nature could be of great use to adversaries who wish 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 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]	Confidentiality and integrity	An insider could modify such records to misrepresent the actual quantities or types of nuclear material stored, and potentially facilitate the unauthorized removal or diversion of nuclear material. Additionally, information on the location, quantity, type and form of the material would be of high interest to an inside/outside threat looking to sabotage or steal material.

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 on these inventories is publicly available. Not all such information is necessarily considered sensitive; risk informed processes can 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 could 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, particularly if details of the security plans are known to an adversary.
3.2. High security vehicles			
A. Visual access to the interior of the vehicle and cargo compartment	[II-1]	Confidentiality	As high security vehicles are specially designed to securely transport nuclear material, this information could be of use to an
B. Physical security features of vehicle design and construction	[II-1]	Confidentiality	

C. Design and function of alarms, immobilization devices and key designs for special locks	[II-1]	Confidentiality	adversary planning to steal or sabotage nuclear material in transport.
D. Integrated vehicle tracking system; system performance and communications systems	[II-1]	Confidentiality, integrity, availability	
3.3. Nuclear material transport containers			
A. Level of resistance to attack (i.e. by various means) of transport containers	[II-1]	Confidentiality	This information could 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 typically in the public domain.
C. Information on the design of specific transport containers (specially protected containers)	[II-1]	Confidentiality	This information could 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.
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.
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 could provide an adversary with 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. Information relating to or processed by safety related 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 systems have control and operational monitoring functions. The compromise of these systems could enable an adversary to disrupt the operation of a facility, in the worst case, leading to the release of radioactive material [II-4][II-5].
4.4. Advanced cyber threats			
A. Information about zero-day vulnerabilities or unpatched security flaws in computer systems handling sensitive information	[II-1], [II-2], [II-3]	Confidentiality	Such information could enable adversaries to compromise systems before security patches are available.

B. Details about supply chain security verification processes and results	[II-1], [II-2], [II-3]	Confidentiality	Information revealing how a facility verifies the integrity of its supply chain could enable adversaries to bypass these controls.
C. Information about advanced persistent threat (APT) detections or indicators of compromise.	[II-1], [II-2], [II-3]	Confidentiality	Knowledge of detection methods could help adversaries evade security monitoring systems.
5. GUARD FORCES AND RESPONSE FORCES			
5.1. Guard force at a facility			
A. Existence of a guard force and the current capabilities of the force	[II-1]	Not sensitive	The existence of a guard force is often publicized to reassure the public and potentially act as a deterrent.
B. Existence of guard forces and their current capabilities at individual 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. The compromise of this 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	This information could help an adversary to estimate in advance the scale of response and the capabilities available in a tactical operational unit.
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.
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 are in the public domain.
B. Design information questionnaire, and the description and 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 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.

6.3. Nuclear material flow and inventory data stored on IT systems, in hard copy, or on any other form of storage medium	[II-1]	Integrity	An insider might modify 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 published in the public domain.
B. Material unaccounted for in material balance areas or key measurement points	[II-1]	Availability	Unavailability of these figures for particular material balance areas or key measurement points could hamper accurate nuclear material accounting.
C. Details of investigations into particular material unaccounted for, unless formally approved for release	[II-1]	Confidentiality	Disclosure of investigation details could compromise the investigative process, potentially allowing perpetrators to modify 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	The modification of limits of error or uncertainty indicators could hide actual discrepancies in nuclear material accounting.
7. APPLICATIONS FOR LICENCES AND PERMISSIONS			
7.1 Applications for licensing and permissions for the use of nuclear and other radioactive materials.			

A. Applications without detailed information on security and safety measures.	[II-1], [II-2]	Not sensitive	The content of such applications varies depending on the legal and regulatory framework, and the specific end use of the material. Consideration is focused on whether they include sensitive information related to nuclear security and its interfaces with nuclear safety.
B. Applications for licences and permissions containing detailed information on security measures and on the type, form and quantity of nuclear or other radioactive material	[II-1], [II-2]	Confidentiality	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 INFORMATION, OTHER INFORMATION ON SAFETY AND THE ENVIRONMENT

8.1. Safety cases			While some information concerning safety cases could be made public for transparency, other information could be considered sensitive if relating to nuclear security and its interfaces with nuclear safety (e.g. protection against sabotage of nuclear safety functions).
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 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 and other radioactive material	[II-1], [II-2]	Confidentiality	

C. Information 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, SECURITY 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	the existence of such plans is often publicized to 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, availability	Details from the plans could indicate the capabilities, limitations and response times, and could therefore be useful to an adversary in planning an attack. The inaccessibility of such plans can lead to disorganized and ineffective responses in actual security incidents.
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, inform adversaries of response actions, create misinformation, and potentially impact timely decision making in mitigating the consequences of severe emergency conditions. Secure and reliable communications would contribute to preventing this (more information is provided in Ref. [II-6]).
9.3. Exercises			

A. Information on security exercises that are to be undertaken or have already been undertaken	[II-1], [II-2]	Not sensitive	The conduct of security exercises is often publicized to reassure the public, provided that the level of detail (e.g. date, time, location of a future exercise) would not assist an adversary to plan 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	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 weapons used and tactics employed by the response force.
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			
10.1. Personal information			
A. Information from trustworthiness determinations	[II-1], [II-2]	Integrity	Modification 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 mandate the protection of this type of information as it can be used for blackmail or extortion purposes, which could, in turn, lead to a compromise of nuclear security.
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. sites where waste is stored, aggregated quantities of waste)	[II-1]	Not sensitive	Such information is generally in the public domain and does not provide specifics that could be useful to potential adversaries.
B. Information that could be used in a criminal or intentional unauthorized act or could enable identification of the radioactive waste held in a specific building at a facility and any associated security measures.	[II-1]	Confidentiality	Such information could be useful to adversaries planning theft or sabotage.
12. DECOMMISSIONING			
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 facility for the treatment and storage of waste and contaminated material arising from processing activities during decommissioning is to be built, and its location.	[II-1], [II-2]	Not sensitive	This information is often in the public domain.
B. Details of the construction and security measures of the facility and the quantity or type of material that is to be processed and stored there	[II-1], [II-2]	Confidentiality	This information could provide useful information to adversaries who are targeting facilities for theft or 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 know how effective security measures need to be from the design basis threat, they can prepare to overcome or bypass these measures, rendering physical protection less effective.
13.3. Details of vital area identification study	[II-1]	Confidentiality	Knowing the vital areas of a facility identified by the competent authority could allow adversaries to infer where security is weaker and identify points of exploitation.
13.4. Security alerts in place	[II-1], [II-2], [II-3]	Confidentiality, integrity	An adversary could falsely elevate a security alert, resulting in the unnecessary deployment of security resources away from the adversary's intended target and a reduction in the effectiveness of physical protection.
13.5 Details of vulnerability assessments	[II-1]	Confidentiality	An adversary could use information on vulnerability assessments, especially those identified but yet to be addressed, as a point of exploitation.
14. NUCLEAR TECHNOLOGY			
14.1. Real-time operational data and process control system configurations relating to 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	[II-2]	Confidentiality	Adversaries could use this information to calculate precise disassembly times in order to plan 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 such studies could 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			
15.1. Sensitive information that dates back some time but is still of current relevance	[II-1], [II-2], [II-3]	Confidentiality	Information of this nature could still be of use to adversaries.

REFERENCES TO ANNEX II

[II-1] INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5), IAEA Nuclear Security Series No. 13, IAEA, Vienna (2011).

[II-2] INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Recommendations on Radioactive Material and Associated Facilities, IAEA Nuclear Security Series No. 14, IAEA, Vienna (2011).

[II-3] EUROPEAN POLICE OFFICE, 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)

[II-4] INTERNATIONAL ATOMIC ENERGY AGENCY, Computer Security for Nuclear Security, IAEA Nuclear Security Series No. 42-G, IAEA, Vienna (2021).

[II-5] INTERNATIONAL ATOMIC ENERGY AGENCY, Computer Security Techniques for Nuclear Facilities, IAEA Nuclear Security Series No. 17-T (Rev. 1), IAEA, Vienna (2021)

[II-6] 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

INFORMATION SECURITY TRAINING PROGRAMME

III-1. This Annex provides example elements of an information security training programme that could be conducted at a regulated entity. When deciding the content of such a programme, the regulated entity can consider the relevance of the topics and methods highlighted in this Annex and develop the programme accordingly.

III-2. Maintaining a robust awareness of security is a crucial foundation for effective nuclear security. IAEA Nuclear Security Series No. 7, Nuclear Security Culture [III-1], provides guidance on this subject.

III-3. Information security training can be broadly divided into the following four types:

(a) Awareness training on threats and vulnerabilities, and the need to protect information and information assets, as well as the need to ensure the correct performance of functions.
(b) Specific training on particular security aspects 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.
(c) Professional training providing in depth technical knowledge tailored to individuals in specialized roles, such as administrators, information system developers, security personnel, and those involved in the classification and declassification of information.
(d) 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.

III-4. The information security awareness training could include 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 for information.
(d) Markings to indicate the classification of information.
(e) Practical examples of applying information security procedures as part of the tasks undertaken by personnel.
(f) Actions to be taken if a breach of information security is suspected or discovered, including relevant steps of the incident response plan or other applicable procedure.
(g) Information security principles, for example granting access to sensitive information on a ‘need to know’ basis.
(h) Current risks to information security in relation to deliberate actions by any of 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.
    (v) Contemporary extremist factions or adversary organizations planning sabotage.
(i) The risks and consequences of internal loss or leaks of sensitive information, either through inadvertent behaviour or intentionally (e.g. for political or terrorist motives).
(j) Conduct or activities likely to help potential adversaries or increase the risk of compromise of sensitive information, including the following:

(i) Casual attitudes to security or careless discussions;

(ii) Vulnerable behaviour that can attract the attention of adversaries (e.g. engaging in activities that could lead to blackmail);

Along with the precautions that need to be taken by personnel in everyday activities, for example, in social approaches, travel, correspondence and acquaintances.

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

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

(m) The importance of protection of information and the integration of this protection into the daily responsibilities of every individual under the information security management system.

(n) The effect of national laws and regulations (e.g. on secrecy, anti-terrorism, security, data protection and freedom of information) and their relevance to individuals, as well as the penalties for the transgression of laws.

(o) The effect of aggregation of information, potentially increasing the sensitivity level and necessitating enhanced protection measures.

(p) An explanation of why computer security measures must continuously evolve and adapt to address emerging vulnerabilities and attack methods, which often develop more rapidly than the underlying technology.

(q) Levels of security clearance; how trustworthiness determinations are conducted and why they are necessary in the nuclear and radiation industry; levels of access granted for particular clearance and trustworthiness levels, as well as how trustworthiness determinations relate to protecting nuclear and other radioactive material.

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

(i) Unauthorized disclosure (compromise of confidentiality);

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

(iii) Unauthorized modification of or interference with information (compromise of integrity).

OPPORTUNITIES TO RAISE AWARENESS OF INFORMATION SECURITY

III-5. The regulated entity could integrate information security considerations into the personnel and contractor onboarding process, including the following:

(a) Introductory security briefing: A short session led by the team responsible for information security within the regulated entity, 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 of 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 covers foundational security concepts and organizational security policies, and is designed to assist individuals in developing their intuition and experience in detecting compromised information.

III-6. The regulated entity could establish periodic refresher training and outreach, such as the following:

(a) Annual security awareness training: One major session per year focusing on current security topics relating to recent internal or external security incidents, new systems or policy updates.

(b) Regular security updates: Frequent circulation of internal news articles or bulletins on relevant security topics, in particularly external security events or emerging threats.

(c) Organization-wide security drills: Periodic practical security tests for all personnel, including 'red team[24]' exercises, social engineering tests or phishing simulations to assess and enhance the organization's security readiness. Such tests or drills may be conducted at irregular intervals to maintain an element of surprise, thereby preventing complacency and encouraging personnel to remain consistently vigilant and prepared.

(d) Targeted training based on analysis: Data from security tests and incident reports are used to provide tailored training for specific departments or groups, which can be more effective than targeting 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.

III-7. The regulated entity could also embed information security considerations into the personnel separation process, including:

(a) Exit interview: This interview with departing personnel can be used to gather feedback to identify unresolved issues or dissatisfaction that might necessitate further attention both in terms of the individual and the organization.

(b) Asset retrieval: Verification that departing personnel have returned assets belonging to the organization, including physical items (e.g. keys, badges, mobile phones) and digital assets (e.g. files, documents).

(c) Reminder of confidentiality obligations: Reminder to departing personnel that the confidentiality agreement they signed remains in effect indefinitely, notwithstanding the termination of employment, and that there may be legal and criminal consequences if this agreement is breached.

(d) Signing of departure form: Departing personnel are asked to sign a standard form confirming that the exit interview has been conducted and all assets of the organization have been returned, and acknowledging the ongoing validity of confidentiality obligations.

III-8. In addition to an information security training programme, there are a number of other methods by which security awareness messages can be transmitted by a regulated entity to its personnel and contractors, including the following:

(a) Posters to remind individuals of information security risks 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 maintaining security when using specific items of equipment.

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

[24] 'Red team' testing involves challenging the plans, programmes, assumptions and implementation of detection operations. This method often uses covert testing, whereby the red team serves as a surrogate adversary and attempts to introduce a threat into the system without being detected. Effective red team testing provides an opportunity to assess which defensive measures are working effectively, as well as which areas or processes are likely to be most vulnerable to adversary exploitation.

(d) Security notices circulated physically or digitally by security management to remind personnel of certain security rules, for example, to counter possible complacency.

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

(f) Warnings to personnel of specific or topical risks to security, and provision of guidance to counter these risks.

(g) Regular testing of the security knowledge of personnel.

(h) Use of the organization's intranet site to convey or promote the overall security message, on the condition that the nature and the sensitivity of the material remain within the accredited level of classification for the network.

III-9. An organization can enhance its information security training programme by utilizing the common principles shared between the safety and security domains. These overlapping principles enable mutual reinforcement in training, making it easier to convey and equate fundamental concepts effectively. In establishing such training, the following need to be taken into account:

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

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

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

MEASURING TRAINING EFFECTIVENESS AND CONTINUOUS IMPROVEMENT

III-10. The regulated entity should implement metrics to evaluate information security training effectiveness and adapt content accordingly:

(a) Pre and post-training assessments to measure knowledge acquisition;

(b) Simulated phishing and social engineering exercises with tracking of success rates over time;

(c) Periodic spot checks of security practices (e.g., clear desk audits, password compliance);

(d) Analysis of security incident reports to identify potential training gaps;

(e) Role-specific training effectiveness metrics tailored to different security responsibilities.

III-11. Results should be analyzed quarterly to identify trends and adapt training content to address emerging risks and observed compliance gaps. Different training approaches should be developed for personnel with specialized security roles versus general staff.

REFERENCES TO ANNEX III

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

Annex IV

MAPPING OF INFORMATION LIFE CYCLE ACTIVITIES

IV-1. Section 5 presents a four-stage information life cycle model. Table IV-1 shows how information life cycle activities described in other publications can be mapped to this model. When considering information life cycle management, the State, competent authority for information security or regulated entity may refer to Table IV-1 to understand how existing or proposed life cycle activities may be considered in the context of the four-stage model.

TABLE IV–1. MAPPING OF INFORMATION LIFE CYCLE ACTIVITIES DESCRIBED IN OTHER PUBLICATIONS TO THE FOUR-STAGE INFORMATION LIFE CYCLE MODEL

Reference	Creating	Processing	Using	Disposing
NIST Glossary [IV-1]	Creation	Processing Dissemination Store	Use	Disposition

REFERENCES TO ANNEX IV

[IV-1] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, Glossary of Key Information Security Terms, NIST Internal Report (NISTIR) 7298 Revision 3, NIST, Gaithersburg, United States of America (2019) https://doi.org/10.6028/NIST.IR.7298r3