IAEA NUCLEAR SECURITY SERIES No. XX

STEP 11 Second review of the draft publication by the review Committee
Date :13 Feb 2025

Information Security for Nuclear Security

DRAFT IMPLEMENTING GUIDE

INTERNATIONAL ATOMIC ENERGY AGENCY
VIENNA, 20XX

CONTENTS

1. INTRODUCTION

BACKGROUND

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

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

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

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

1.3. 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 [~~8] as its Fundamental Principle L~~2] and in Article 7 of the International Convention for the Suppression of Acts of Nuclear Terrorism [~~9] as Article 7.~~3].

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

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

1.5. IAEA Nuclear Security Series ~~Nos~~No. 13, Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5) [~~3],~~4]; No. 14, Nuclear Security Recommendations on Radioactive Material and Associated Facilities [~~4~~5] and No. 15, Nuclear Security Recommendations on Nuclear and Other Radioactive Material out of Regulatory Control [~~5~~6] provide recommendations on the protection of sensitive information.

1.6. Groups or individuals wishing to ~~plan or~~ commit a criminal or ~~other~~ intentional unauthorized act involving nuclear ~~material or~~and other radioactive material or associated

Formatted: Font: Italic
Formatted: Font: Italic
Formatted: Font: Italic
Formatted: Font: Italic
Formatted: Font: Italic
Formatted: Font: Italic
Formatted: Font: Italic
Formatted: Font: Italic
Formatted: Font: Italic
Formatted: Font: Italic
Formatted: Font: Italic
Formatted: Font: Italic
Formatted: Font: Italic
Formatted: Font: Italic
Formatted: Font: Italic
Formatted: Font: Italic
Formatted: Font: Italic
Formatted: Font: Italic
Formatted: Font: Italic
Formatted: Font: Italic

facilities and 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" [27].

1.7. This Implementing Guide 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 unauthorised acts (e.g. cyber-attack, insider threat).

1.8. Paragraph 1.3 of IAEA Nuclear Security Series No. 42-G, Computer Security for Nuclear Security [68] states that:

1.7. "… "The security of sensitive information and sensitive information assets implies protecting the confidentiality, integrity and availability of such information and assets."

1.9.1.8. Some sensitive information is created, controlled, stored, processed or communicated through computer based systems (i.e. sensitive digital assets). Ref. [6],Reference [8] provides further guidance on addressing computer security utilizing a graded approach, based on the severity of potential consequences for protecting, to protect the confidentiality, integrity, and availability of computer based systems[1], the compromise of which could adversely affect nuclear security or nuclear safety.

1.10.1.9. The terms used in this publication are to be understood as explained in the IAEA Nuclear Safety and Security Glossary [27], unless otherwise stated in the text.

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

OBJECTIVE

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

1.13.1.11. This publication 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 programmemanagement system.

1.14.1.12. 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

[1] Including bothComputer 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 perform,that provide or control services involving such information. Additionally, Ref. [12]IAEA Nuclear Security Series No. 17-T, Computer Security Techniques for Nuclear Facilities [9] provides further considerationguidance on how Confidentiality, Integrity,confidentiality, integrity and Availabilityavailability 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).

Formatted: Outline numbered + Level: 3 + Numbering Style: 1, 2, 3, … + Start at: 1 + Alignment: Left + Aligned at: 0.1" + Indent at: 0.1"

considerations that apply to nuclear security, and by outlining the particular provisions and conditions for information security within a nuclear security regime.

SCOPE

~~1.15.~~1.13. This ~~Implementing Guide~~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.

~~1.16.~~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.

~~1.17.~~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.

~~1.18.~~1.16. The intended audience for this publication is all those who are responsible for the security of sensitive information, for example, competent authorities, including regulatory bodies; management in facilities, companies or organizations involved in the use, storage or transport of nuclear ~~material or~~and other radioactive material; response organizations for nuclear or radiological emergencies~~,~~; facility operators and personnel~~,~~; designers~~,~~; vendors ~~and in particular,~~ security personnel; contractors or other third parties working for competent authorities, organizations or facility operators; or any other entities that have been given legitimate access to sensitive information.

STRUCTURE

~~1.19.~~1.17. Section 2 introduces key terms and concepts for information security. Section 3 describes the elements necessary to build a framework for the security of sensitive information within a State. Section 4 presents considerations for determining which information can be considered sensitive ~~information~~ and ~~would~~ therefore ~~need~~needs to be managed as such. Section 5 ~~contains considerations~~presents a four-stage model for managing the ~~sharing and disclosure~~life cycle of sensitive information~~. Section 6~~ and describes the ~~necessary actions~~activities to be undertaken at ~~the regulated entity or regulated competent authority for managing and operating measures to secure sensitive information~~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.

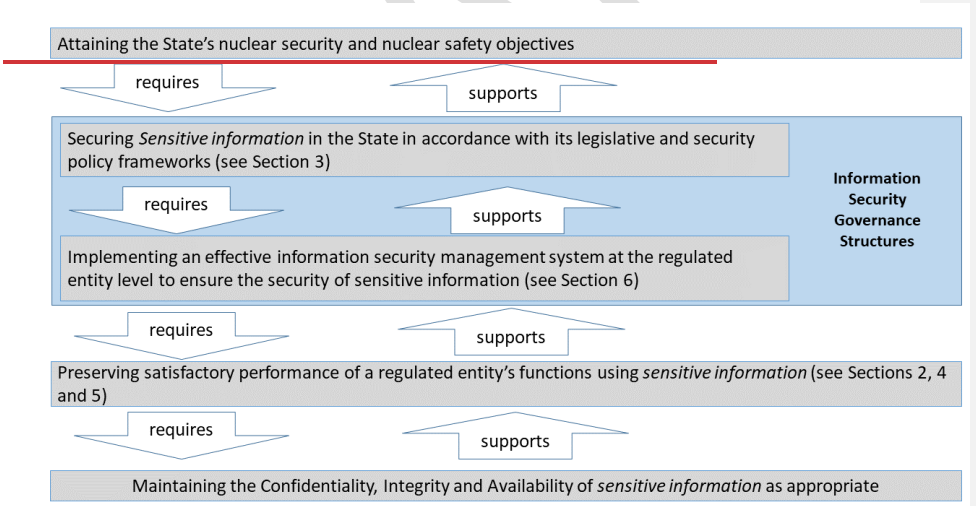
2. INFORMATION SECURITY CONCEPTS

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[3], integrity[4] and availability[5] 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.

2.4. A ~~State's~~State's legislative, regulatory and policy frameworks (see Section 3) and the information security management system[6] 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~~), as~~). This is because some functions performed by an organization[7] (e.g. the safe operation of a nuclear facility) that are directly relevant to the ~~State's~~State's nuclear security[8] and nuclear safety[9] objectives rely upon the confidentiality, integrity and availability of sensitive information, as illustrated in ~~Figure~~Fig. 1.



[3] The property that information is not made available or disclosed to unauthorized individuals, entities or processes [~~2~~7].
[4] The property of accuracy and completeness of information [~~2~~7].
[5] The property of being accessible and usable upon demand by an authorized entity [~~2~~7].
[6] ~~The~~ 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) ~~jointly employ 'information security management system' abbreviated with the acronym 'ISMS' as their formal terminology~~ in the ISO/IEC 27000 family of standards~~[15], while various~~ [10]. Some national authorities ~~opt for 'information~~use the term 'information security ~~programme'~~programme' to reflect this concept in their regulatory frameworks.
[7] Ref. [~~1~~29] uses the term 'facility functions' to describe the functions performed by a nuclear facility.
[8] For the purposes of this publication 'nuclear ~~security~~security' is to be interpreted as including nuclear material accountancy and control.
[9] For the purposes of this publication 'nuclear ~~safety~~safety' is to be interpreted as including emergency preparedness and response.

Formatted: Space Before: 0 pt, After: 0 pt, Line spacing: single

Formatted: Default Paragraph Font, Font: 11 pt, English (United Kingdom)

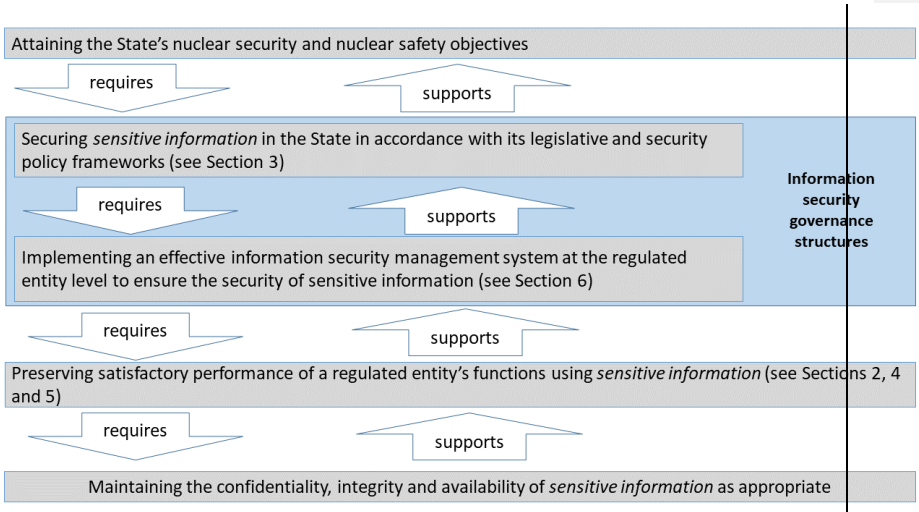


FIG. 1. Relationship between the State's nuclear security objectives, information security governance structures and the confidentiality, integrity and availability of information (adapted from Ref. [~~6~~8]).

~~ABSTRACT~~ INFORMATION

2.5. Information ~~comprises~~includes facts, data, ~~symbols or instructions in whatever form. Information can represent~~ ideas, concepts, events, processes, thoughts ~~and,~~ 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. ~~Without this context, information remains disconnected from its practical significance and potential implications.~~ This distinction between ~~contextualised~~contextual and abstract information is ~~particularly~~ crucial for the proper interpretation and ~~the~~ application of information security.

INFORMATION OBJECTS

2.6. An information object is "knowledge or data that have value to the organization" [~~2~~7]. Information objects can be ~~tangible~~ physical or digital collections of information on paper, on film, on magnetic or optical media, in charts, in documents, in executable software ~~executables, and~~files, or in any other ~~forms and channels~~form or channel used for transferring information.

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

(a) The information within an information object shares certain properties, such as a common usage, purpose ~~or~~, associated risk ~~and~~, or form of creation, processing, storage or transmission;

(b) The information object has sufficient context (i.e. includes information that ~~supports identifying it's~~allows its use and value~~) that is sufficient~~ to be identified) to allow the ~~associated~~ information within it to be assessed;

(c) The information object can be labelled, enabling the application of targeted and specific security controls ~~applied~~ 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 ~~is in the appropriate~~has context~~, can be viewed~~) 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.

~~INDIVIDUALS AND~~ 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 ~~utilizing~~that utilizes information or information objects.

2.10. Information assets~~, which include control systems, networks, and information systems,~~ actively facilitate the handling, management~~,~~ and utilization of information objects through various operations such as ~~storing~~the storage, processing, ~~controlling,~~control or ~~transmitting~~transmission of information~~, and while~~. 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 ~~or processing~~ and subsequent ~~utilization~~use of information contained in its abstract form, by utilizing information objects or information assets. Individuals ~~and~~can also use information assets ~~can also interact in order~~ 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, ~~individuals~~ and the functions performed. The diagram should be read from left to right, following the arrows ~~to indicate that~~. It illustrates how information can be represented in information objects, which are then used or processed by individuals and information assets~~, who or which~~ that can take action to affect the functions performed or other information produced.

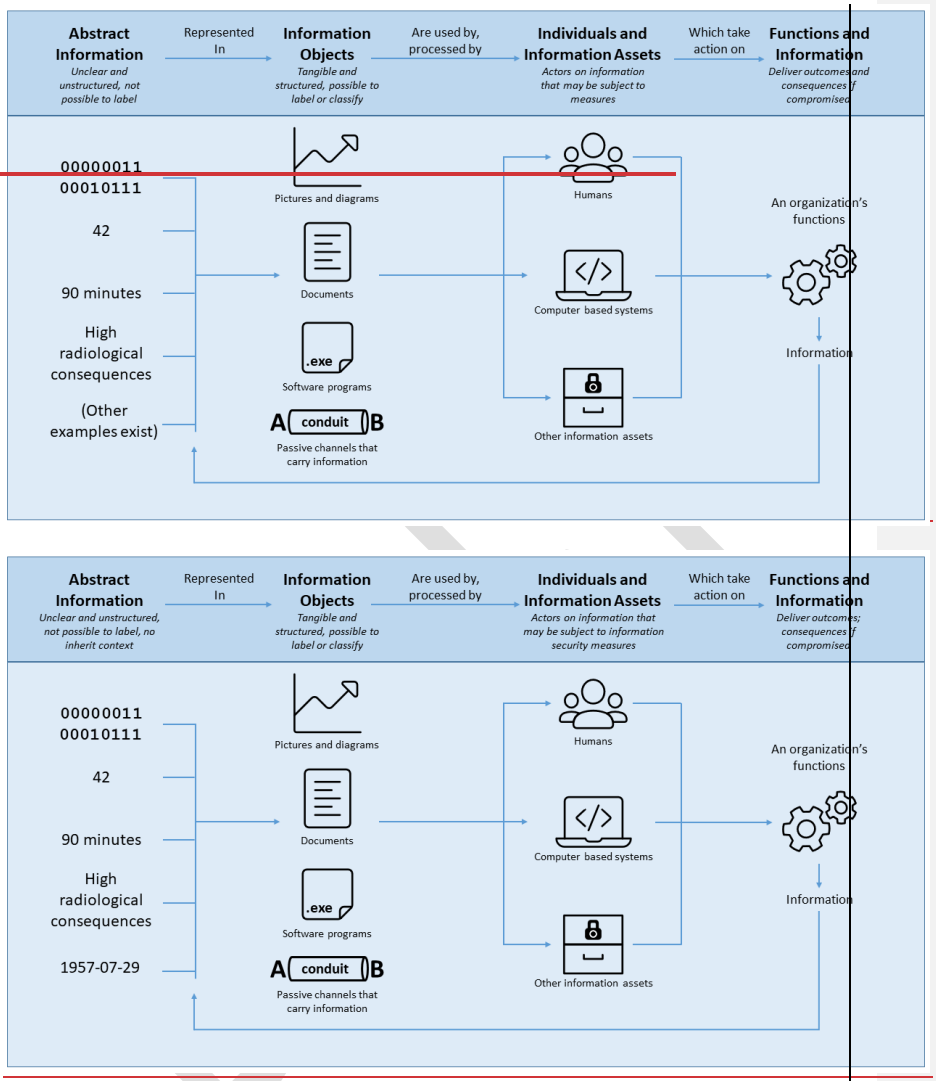


FIG. 2. Conceptual ~~information~~ model illustrating the relationship ~~of~~between abstract information ~~to~~, information objects, information assets and the functions performed, with examples.

2.14. An adversary might seek to provoke a consequence by affecting the functions performed in the final column of Fig. 2. The adversary ~~can have~~might achieve this ~~effect~~ by acting on information, information objects, information assets or individuals relating to that specific function. However, conventional information security measures can generally only be applied to information objects, information assets~~,~~ and individuals in an effort to protect the relevant functions. Information security measures should be designed to protect information as comprehensively as practicable in both its tangible and abstract forms. Abstract information may ~~require~~need context (i.e. being interpreted as an information object) to determine its value and to implement targeted and specific information security measures~~, but~~. However,

untargeted measures ~~such as~~(e.g. training on information security~~,~~), should be applied~~,~~ even if technical ~~controls~~measures might not be effective.

2.15. ~~For~~When the information ~~security for nuclear security, any or all of the entities or organizations listed below can attribute a different value to~~contained in information objects and information assets~~, when the information they contain~~ 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, ~~and~~ 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 ~~an inconsequential part~~ of ~~routine operations.~~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 ~~other~~ intentional unauthorized act. Information should therefore be protected consistent with the highest impact and consequence.

2.17. ~~It is important to note that an~~An adversary could create or modify information, information objects and information assets for criminal or other intentional unauthorized purposes. The latter could include attacks that are specifically designed and executed to mislead human or machine based decision making. This type of attack should be considered when protecting information ~~on the~~that is used as a basis ~~of which decisions are made~~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 ~~material, nuclear facilities,~~or other radioactive material~~,~~ and ~~their~~ associated facilities and activities. Such information can also be used to undermine the detection of and response to nuclear security events, as well as to compromise the security of nuclear ~~material or~~and other radioactive material during transport.

2.19. The information necessary for the performance of a function important to nuclear security ~~and~~or nuclear safety can be considered as sensitive. ~~Sensor~~For example, sensor values that are used to ensure the nuclear safety function to control reactivity~~, for example,~~ are likely to be considered as sensitive information. Sensitive information ~~could~~ also ~~describe~~includes vulnerabilities that an adversary could exploit to undermine those functions. For example, ~~the sensor values that are used to ensure the nuclear safety function to control reactivity might be converted using~~if a calibration table~~, which is used in the case of multiple sensors that serve different purposes. If the calibration table~~ used to convert sensor values is modified, multiple functions could be adversely affected~~, which means that the sensor data~~. 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 ~~assessed~~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[10]. 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 nuclear accident. In such cases the protection of integrity and availability ~~may~~should be ~~prioritised~~prioritized over confidentiality ~~as~~if the potential consequences to nuclear security and nuclear safety ~~may be~~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) Descriptions of nuclear security arrangements at a facility (e.g. physical protection, information security, insider threat mitigation, incident response arrangements);
(c) Software applications or communications (e.g. network communications, process signalling) important to the performance of nuclear security and nuclear safety functions;
(d) Details on the location or the transport of nuclear material ~~or~~and other radioactive material;
(e) Information concerning vulnerabilities in arrangements at ports and airports for the detection of material out of regulatory control;
(f) Details of an organization's personnel with authorized access to nuclear or radioactive materials;
(g) Details of essential equipment and systems;
(h) Details of a weakness in a system of minor importance that would indicate the presence of the same weakness in a system of greater importance for safety or security.

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

2.23. 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 ~~other~~ 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 ~~the guards~~they are armed, the size of the response force and the estimated time that it would take the response force to arrive on-site. ~~This same~~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

[10] 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.

function, which would allow the adversary to more effectively plan the attack. Therefore, the compromise of sensitive information by an adversary increases the likelihood that the adversary can negatively impact functions important to nuclear security and nuclear safety.

2.25. The conceptual ~~information~~ model illustrated in ~~Figure~~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 restricted to those individuals who have a genuine need for this access for the performance of their work. The dissemination of sensitive information should thus be limited to authorized individuals and sensitive information assets on a 'need to know' basis. ~~Such~~Authorized individuals should be identified and authenticated, ~~with~~ and lists should be maintained ~~lists~~ documenting all ~~persons granted~~those individuals with the rights to access ~~privileges~~sensitive information.

2.27. The 'need to know' and 'least privilege' ~~(i.e. the minimum level of access to perform the function)~~[11] principles should be used to guide management and control of access rights to sensitive information. The risks associated with information security are more enhanced when sensitive information is shared by individuals who do not understand the potential value of the information.

2.28. 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 ~~and~~. The measures should be re-evaluated if a previously unknown consequence comes to light, as this could significantly amplify the impact. ~~The greater the potential consequences of a compromise, the stronger the security measures that should be applied.~~ Specific guidance on measures to protect against internal adversaries can be found in IAEA Nuclear Security Series No. 8-G (Rev. 1), Preventive and Protective Measures against Insider Threats [~~7~~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 and processing equipment). Figure 3 depicts all the information and computer based systems within a State and how they relate to one another. The area ~~referred to~~marked as ~~"~~'digital ~~assets"~~assets' in ~~Figure~~Fig. 3 is where ~~sensitive~~information and information assets intersect with computer based systems. This area is the domain of computer security. Computer security is a particular aspect of information security that is concerned the protection of computer based systems against compromise. Additional guidance on computer security for nuclear security can be found in Ref. [6].

[11] The principle of least privilege dictates that individuals and information assets only have the level of access they need to perform the necessary function.

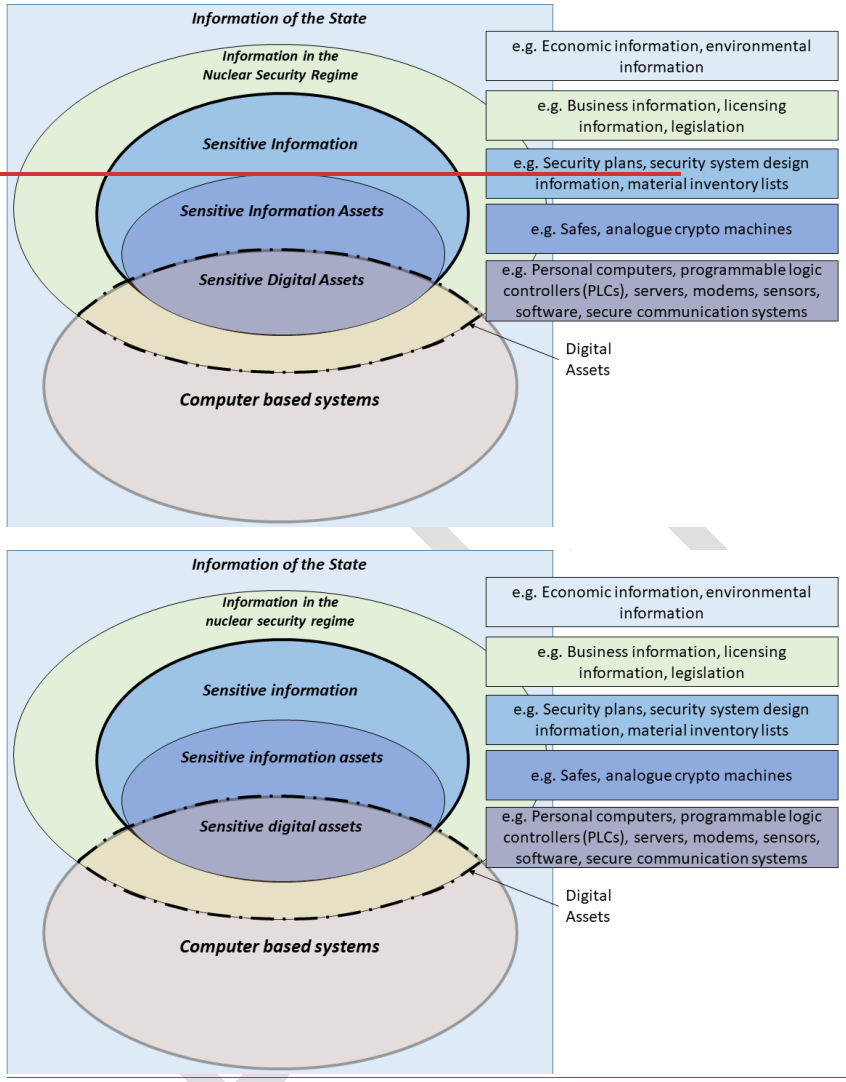


FIG. 3. ~~Information~~Relationship between the information and computer based systems in the State and in the nuclear security regime (adapted from Ref. [~~68~~]).

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

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

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

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

2.34. Gaps or deficiencies in one security domain can affect the security of other domains, ~~and~~ so it is essential to adopt a comprehensive approach that considers all ~~these~~ domains. Legislative, regulatory and policy frameworks for securing sensitive information should also consider the need to take into account other objectives~~, such as operational 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 ~~are handling~~handle sensitive information. Such frameworks should also ensure the criminalization of related offences. When creating security frameworks specific to the nuclear regime, the State should establish the following:

(a) Provisions for describing the responsibility of the State for information security;

(b) A legislative framework covering information security for sensitive information;

~~(c)~~ An information security policy framework, including guidance and classification schemes for information security.

~~3.2.~~(c) ~~An information security policy framework~~ This 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.

Formatted: List of items, Indent: Left: 0", Hanging: 0.3", Numbered + Level: 1 + Numbering Style: a, b, c, … + Start at: 1 + Alignment: Left + Aligned at: 0.25" + Indent at: 0.5"

Formatted: English (United Kingdom)

COMPETENT AUTHORITY FOR INFORMATION SECURITY IN THE NUCLEAR SECURITY REGIME

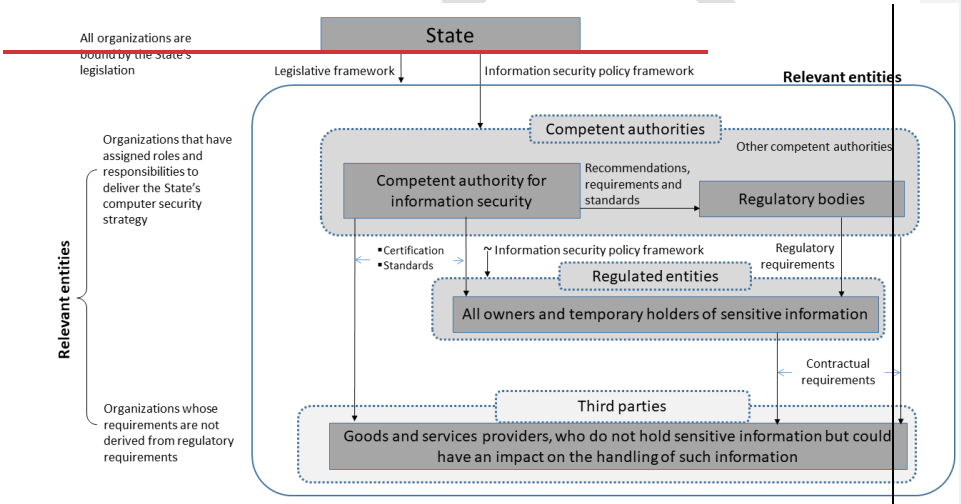
~~3.3.~~3.2. States typically have ~~government~~governmental organizations or agencies that are responsible for overall national security (hereafter referred to as 'national security authorities'). National security authorities have the responsibility of defining the State's information security policy 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.~~3.3. 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 ~~[10].~~

~~3.5.~~3.4. ~~In the case that~~If there is more than one competent authority for information security in relation to the nuclear security regime, or ~~that~~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.~~3.5. ~~The State can choose to implement an~~If a State's information security policy framework ~~that is not limited to~~ extends beyond the scope of the nuclear security regime, ~~with the scope of some laws and regulations extending beyond the nuclear security regime. In such cases,~~ the competent authority for information security should ensure that the ~~information security policy~~ framework is sufficient for nuclear security. If the framework does not adequately address nuclear security, ~~the State~~it should ~~supplement the information security policy framework~~be supplemented with the necessary requirements, in a manner that is coherent with the nuclear security regime.



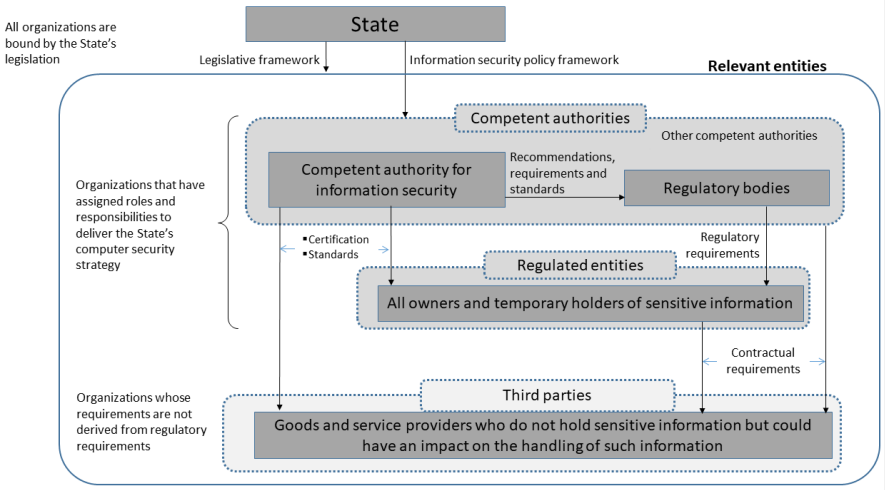


FIG. 4. The relationship between the State and entities relevant to the nuclear security regime for the purposes of information security (adapted from Ref. [~~6~~8]).

~~3.7.~~3.6. Figure 4 provides an illustration of the ~~organizations~~relationship between entities that could have an impact on the security of sensitive information in the nuclear security regime. The figure ~~illustrates a potential~~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[12] and third parties (e.g. vendors ~~and~~, technical support ~~organisations~~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

~~3.8.~~3.7. The State should identify and ensure the coordination of all organizations ~~having~~that have a role in the nuclear security regime~~, described in this publication as~~ (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 ~~within regulated entities. Regulated entities are those entities that have access to sensitive information within the nuclear security regime.~~.

~~3.9.~~3.8. Regulated entities may include ~~all organizations~~any organization that ~~deal~~deals with matters identified by the State as being necessary to maintain information security within the nuclear security regime. A State could require any entity that holds and processes sensitive information, including providers of commercial goods and services and other 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 ~~create~~establish separate information security requirements for competent authorities ~~holding~~that hold and ~~processing~~process sensitive information ~~to follow~~.

Formatted: English (United States)

[12] For the purposes of this publication, 'regulated entities' are those entities that have access to sensitive information within the nuclear security regime.

~~3.10.~~3.9. Some third parties ~~never~~do not retain sensitive information, but they could still have an impact on the security of sensitive information. ~~Such~~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. Although these third parties ~~could be~~are relevant entities ~~but~~, they might not fall into the category of regulated entities. ~~These entities~~They should therefore be ~~the~~ subject ~~of~~to controls in order to maintain adherence to the regulations outlined in the information security policy framework. ~~For example, third parties (e.g. equipment vendors) could provide technical equipment (e.g. document safes, computer based systems, security equipment) to regulated entities (e.g. operators of nuclear power plants) that will process sensitive information.~~ The relevant requirements for ~~such organizations~~these third parties, and for their products or services, could be defined directly or through contractual agreements, ~~operating~~ within the overall legislative framework.

~~3.11.~~3.10. 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.

~~3.12. The State can determine thatinternational contractors who hold sensitive information, and who are outside of the State's legislative framework, should nevertheless be the subject of controls imposed through contracts. Alternatively, the State could demand that international contractors maintain a local presence, in which case these contractors would be constrained by the State's legislative framework.~~

~~3.13.~~3.11. Legislation should also be established to define the competent authorities ~~in charge of controlling~~for information security and the ~~sanctions or punishment~~penalties that will be applied to individuals or organizations that breach information security. This legislation ~~could have sections that~~should define the severity of, and the corresponding ~~sanctions~~penalties for, specific types of breach~~, for example~~ (e.g. in relation to confidentiality, integrity~~,~~ or availability of sensitive information, sensitive information objects and sensitive information assets~~.~~).

~~3.14.~~3.12. The reporting of information security incidents to the competent authorities should be mandatory, and laws or regulations should specify ~~sanctions or~~ penalties for failure to make such reports within the defined ~~timeframes~~time frame.

~~3.15.~~3.13. ~~The~~Competent authorities should have regulatory powers ~~of competent authorities~~, established through the legislative framework, ~~should allow the authorities~~ to place obligations on the holders of sensitive information. Laws enacted for this purpose should ~~enable sanctions or punishment~~impose penalties for the unauthorized disclosure, storage, modification or falsification of sensitive information. The legislation should also mandate ~~the~~specific State ministries, departments, agencies and other ~~organizations that are~~entities to provide the competent authorities with the ~~necessary~~ support~~, enabling the latter~~ they need to ~~fulfil the obligation of ensuring~~ensure the security of sensitive information.

~~3.16.~~3.14. ~~The~~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 ~~(e.g. conventions~~, such as ~~Refs. [8][9]) while defining and implementing information security as it relates to nuclear security. Examples could be found in the~~ the following:

Formatted: Condensed by 0.15 pt

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

Formatted: French (France)
Formatted: French (France)
Formatted: French (France)

ROLES AND RESPONSIBILITIES FOR INFORMATION SECURITY

~~3.17.~~3.15. 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.~~3.16. 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.~~3.17. The State should ensure that sufficient financial, human and technical resources are available to the competent authorities so that they can ~~effectively~~ fulfil their responsibilities in ~~correctly~~ implementing the legislative framework and the information security policy framework relating to information security in the State's nuclear security regime.

~~3.20.~~3.18. 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.~~3.19. Many regulated entities ~~will~~ operate within an international marketplace ~~wherein~~where goods and services are supplied from vendors and contractors from other States. ~~Where the sharing of sensitive information is necessary to support contracts, it~~This could result in sensitive information ~~being~~having to be sent outside ~~of~~ the jurisdiction of the originating State's legislative framework and information security policy framework. ~~As such,~~In turn, this might undermine enforcement actions relating to breaches of security requirements~~,~~ or the control of legal authorization to access information~~, could be undermined.~~. To address such issues, ~~States can form~~the State could sign reciprocal agreements with other States to protect ~~other States'~~each other's classified information under their own security policy ~~framework~~frameworks. The content of these agreements could differ from one State to another. Under these circumstances, it might be necessary ~~within the State's information security policy framework~~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 ~~ON~~OF INFORMATION SECURITY WITH OTHER DOMAINS

~~3.22.~~3.20. The State should ensure efficient functioning ~~and performance~~ of interfaces between information security and other elements of ~~a State's~~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. ~~This may include providing~~The State should provide guidance on, or requirements for~~ the methods of coordination.~~, how to coordinate such interfaces. Actions ~~could~~ might need to be ~~necessary on the part of the State~~ taken that are outside the scope of information security ~~(e.g.~~, for example placing requirements on information generated within other domains or ~~accepting to apply~~applying the disclosure requirements of other domains~~, such as provisions~~ (e.g. related to freedom of information~~, on~~) to information security~~).~~.

~~3.23.~~3.21. 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.~~3.22. The State's information security policy framework should define criteria ~~necessary~~ to identify the information that the State wishes to protect and should indicate how sensitive information is to be protected. The framework ~~generally sets~~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~~, indicating the information's~~ according to its level of sensitivity, and ~~hence~~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.~~3.23. Detailed ~~policy and~~ guidance on how to implement ~~the requirements of~~ the information security policy framework in the nuclear security regime should be developed by the competent authority for information security, in close liaison with the national security authorities and in consultation with the users of sensitive information within regulated entities ~~of the nuclear security regime.~~. This type of guidance should ~~typically~~cover how to define what constitutes sensitive information, ~~should~~how to divide the ~~types of~~ information ~~into a series of related topics,~~classes (see Section 4), and ~~should indicate~~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.~~3.24. At the regulated entity and competent authority level, the importance of specific information can be indicated in an information security management system, which should also describe how sensitive information is to be protected in compliance with the information security policy framework and legislative framework (see Section 6 for additional information).

RISK MANAGEMENT

3.27.3.25. The State's information security policy framework, or the more detailed nuclear security guidance, should identify clearly the regulated entities within the nuclear security regime that have delegated responsibility for analyzing risks, analysing and managing risks and definingfor establishing rules for the protection of sensitive information throughout its lifecyclelife cycle (see Section 5), as well as the regulated entities that are requiredhave to follow the definedthese 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 and mandatory information concerning security on mandatory measures that are specific tofor the security of sensitive information in the nuclear security regime. Alternatively, the State's competent authority for information security could delegate thisthe responsibility for identifying appropriate measures to a regulated entitiesentity that demonstratedemonstrates sufficient competence, along with the authority to manage certain risks locally with consideration of the national threat assessment or design basis threat. This authorizationdelegation should always be in compliance with the State's legislative framework, information security policy framework, and other elements of athe State's nuclear security regime (such ase.g. a decision made in coordination with the competent authority for computer security takingshould take into account any impacts on the State's computer security strategy, see Ref. [6])8]) thus ensuring a harmonized approach to risk management across the nuclear security regime.

3.28.3.26. 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 [1113].

SECURITY POLICIES AND MANAGEMENT SYSTEM AT THE ORGANIZATION LEVEL

3.29.3.27. Each regulated entity and competent authority that handles sensitive information should compiledevelop its own information security policy and information security management system, on the basis of documented expectations fromguidance provided by the competent authoritiesauthority 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 a form that is relevant,an accessible and understandable way. Section 6 contains additional guidance on establishing an information security management system.

3.30.3.28. The competent authority for information security could designateshould 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 (with an emphasis onin 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. ~~Identifying~~It is therefore important to identify which information is sensitive ~~information is thus important, as is determining the degree~~, its level of sensitivity ~~of this sensitive information~~ and the specific risks associated with ~~this sensitive information~~it.

4.2. The competent authority for information security should specify how to determine which information~~,~~ relating to nuclear ~~material,~~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 ~~on the consequences of~~, in relation to decisions made on the basis of the information, considering that the information may be targeted by adversaries ~~within~~as part of an attack designed ~~and executed~~ to mislead human or machine based decision making.

4.3. Information ~~can~~should thus be classified using a graded approach, and a classification scheme ~~may~~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.

4.4. Some information that is not considered to be sensitive by the nuclear security regime could be considered sensitive for other reasons. ~~Regulated entities might need to combine a graded approach common to the nuclear security regime and other factors used to identify sensitive information (e.g.~~ (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 ~~how~~ who is responsible for the classification ~~responsibilities are assigned~~of sensitive information, either ~~through~~in the information security policy framework, ~~within a competent authority or regulated entities'~~in the information security management system of the competent authority or regulated entities, or ~~through a combination of~~ both.

SCALE OF IMPACT FOR SENSITIVE INFORMATION

4.6. The State might find it helpful to establish a common scale of impact and classification scheme. ~~As~~, an example of which is shown in Fig. 5~~, information~~. Information security requirements can then be developed using a graded approach, in proportion to the severity of the consequences of compromise of a function arising from the loss of confidentiality, integrity or availability of the information.

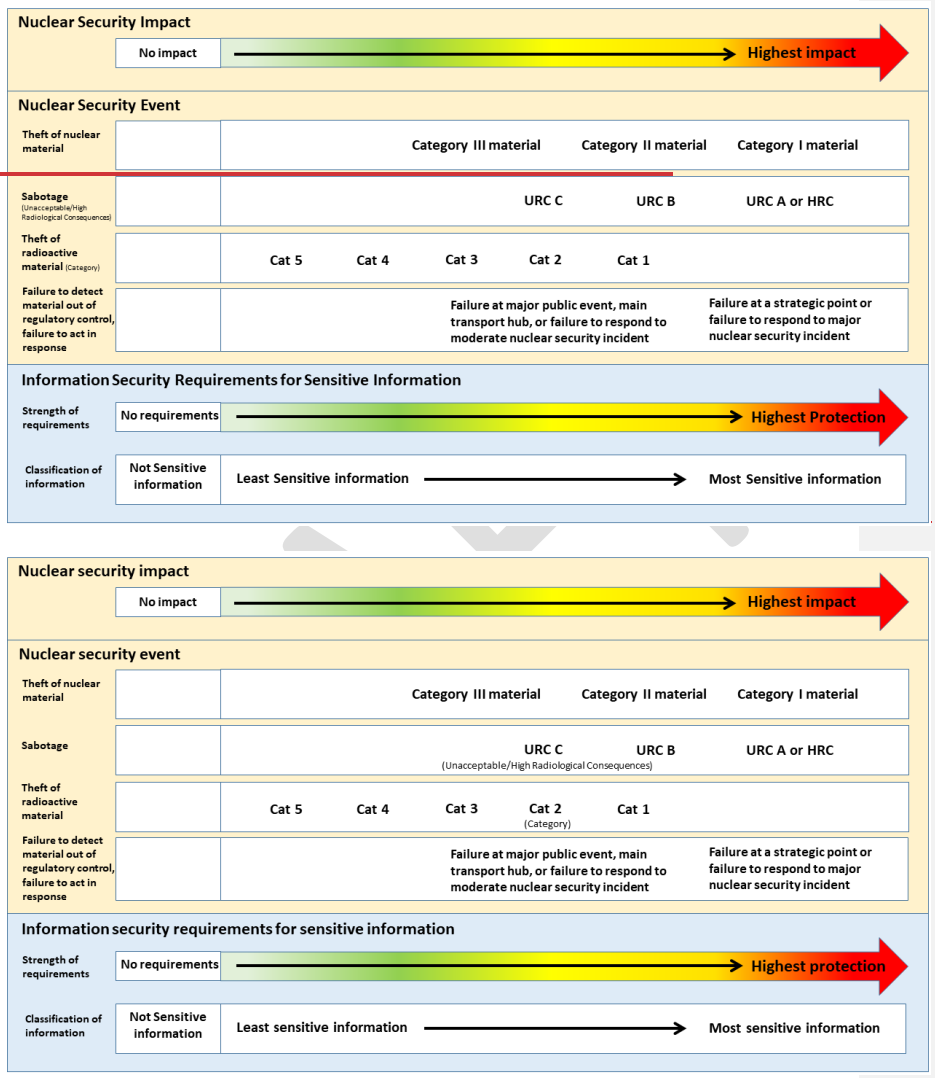


FIG. 5. Example common scale of impact and a graded approach to protecting sensitive information (adapted from Ref. [~~6~~8])[13].

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

[13] ~~Fig.~~Figure 5 relates to sensitive information ~~that may~~, the compromise of which might have an impact ~~in relation to~~ on the nuclear security regime. ~~It is acknowledged that other~~Other information ~~(recorded as "no impact" above) will~~ is likely to be held~~, where the impact~~ that, if compromised, will not affect nuclear security or ~~it's~~its interfaces with nuclear safety ~~thus~~(indicated as 'no impact' in Fig. 5). The information security requirements ~~and impact~~for such information are considered outside the scope of this ~~document~~publication.

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

(a) Very complex classification systems ~~could contain~~with many levels ~~and~~might become cumbersome~~, proving~~ and prove to be impractical.

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

(c) ~~Over classification~~Overclassification (i.e. requiring more stringent security than is necessary) can lead to unnecessary additional expense for regulated entities and conflict with ~~policies for~~ transparency policies, whereas ~~under classification~~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 ~~a complex and complete scheme for information classification~~completeness and the need for ~~a practical scheme~~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. ~~This~~When developing such guidance ~~may consider~~ the following ~~factors~~might be taken into consideration:

(a) ~~Specific consideration should be given to the~~The accumulation of information, and logical or physical points of aggregation ~~(e.g.~~. 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 ~~and~~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) ~~An~~The compromise of information ~~compromise~~ at a regulated entity could affect other entities and the functions they perform, having a broader ~~impacts~~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, ~~it might not always be clear to those tasked with assessing the value~~ 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. [~~68~~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 ~~overtime~~over time as the understanding of threat capabilities and the consequences ~~that could be realised~~ 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 ~~for the classification~~ 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 ~~or others as defined by the State~~, in descending order[14]:

~~(a)~~(1) Secret;

~~(b)~~(2) Confidential;

~~(c)~~(3) Restricted.

Formatted: Bullets and Numbering

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

4.11. Classification schemes for sensitive information have traditionally been designed in response to the potential ~~impacts~~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 ~~options~~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 ~~is a~~. However, this solution ~~that~~ could be overly complicated for users.

(c) Utilizing technology to manage ~~these~~ complex classifications ~~is a possible solution that~~. This may reduce ~~the~~ reliance on the understanding of the person performing the classification.

4.12. Some example definitions for the classification labels '~~SECRET', 'CONFIDENTIAL'~~secret', 'confidential' and '~~RESTRICTED'~~restricted' are given in Annex I. These definitions can be applied in relation to confidentiality, integrity and availability ~~considerations~~.

4.13. Additional caveats[15] for information security could indicate restrictions on the distribution of sensitive information, in accordance with the nature of ~~this sensitive~~the information, or enhance the 'least privilege' or 'need to know' principles, which allow only

[14] In many States, there is a ~~further~~higher classification of ~~TOP SECRET. This level of classification~~'top secret', but it is almost never used in the civilian sector ~~of most States~~.

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

users who have a legitimate need to access the information. ~~The following is a very small set of examples that illustrate the use~~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.

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 ~~addressed through~~handled in accordance with information security measures [~~12~~] ~~are as follows~~9], includes information in the following categories:

(a) Details of physical protection systems, computer security measures and any other security measures established for nuclear ~~material,~~and other radioactive material~~,~~ and associated facilities and activities, including information on guards and response forces and arrangements ~~related~~relating to transport security;
(b) Information relating to the quantity and form of nuclear ~~material or~~and other radioactive material in use or storage, including nuclear material accounting information;
(c) Information relating to the quantity and form of nuclear ~~material or~~and other radioactive material in transport;
(d) Information ~~related~~relating to the facility and its operations, the misuse of which could compromise safety and security;
(e) Detailed information ~~related~~relating to ~~the~~both the physical and digital storage location of sensitive information ~~both physically and digitally~~;
(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 ~~of the~~ information in the categories listed in para. 4.~~13~~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.

5. ~~THE~~ LIFE CYCLE OF SENSITIVE INFORMATION

5.1. Managing the life cycle of information, and more specifically the life cycle of sensitive information, allows regulated entities 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 ~~of generic~~[16] information life cycle[17], as illustrated in Fig. 6.

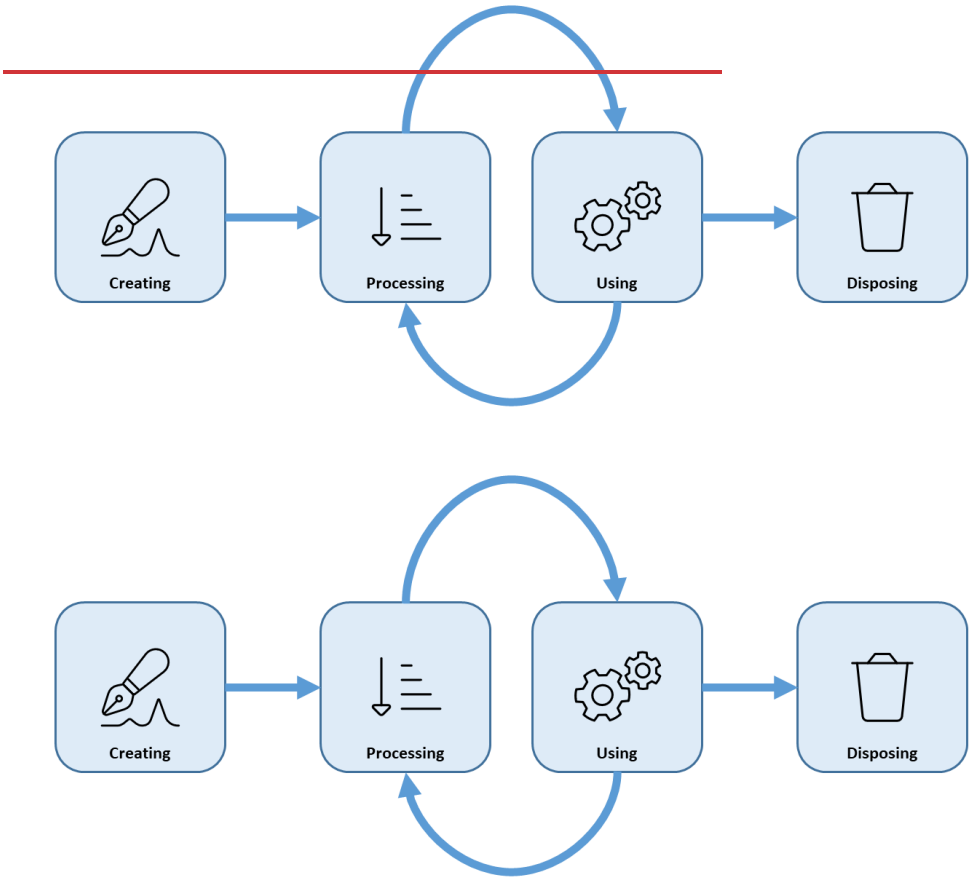


FIG. 6. The four stages ~~of the~~in a generic information ~~lifecycle~~life cycle and ~~their~~the relationships between them.

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

[17] ~~There is no single, universally recognized information life cycle, but most have between four and seven activities. The different activities have been categorized into a four stage cycle provided above.~~

5.2. ~~FIG.~~The four stages depicted in Fig. 6 ~~is comprised of~~are the following ~~stages~~:

(1) Creating~~, involves activities related to~~: assembling an information object from abstract information or other information objects ~~and includes~~ , including activities such as ~~collecting~~the collection and ~~classifying~~classification of information;

(2) Processing~~, involving~~: activities performed on information objects ~~that have been~~ created before and throughout their active use ~~such as~~(e.g. handling, transmission and storage~~;~~ activities);

(3) Using~~, which covers~~: activities that leverage information ~~within~~during the performance of functions, including the sharing, replication, dissemination, disclosure ~~and~~, reclassification ~~,~~and further processing of ~~the~~ information;

(4) Disposing, including archiving and destroying information.

5.3. ~~An example mapping of~~ Annex IV shows how the information ~~lifecycle~~life cycle activities ~~into the~~ described in other publications can be mapped to the generic four- stage ~~generic~~ information ~~lifecycle is provided in Annex IV~~life cycle described in this section.

CREATING INFORMATION

5.4. Information ~~will~~is generally ~~be~~ created in an abstract, unstructured and unlabelled form (see Fig. 2). For example, a person could ~~calculate~~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. 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. 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 ~~information~~, regulated entities should implement mechanisms to manage ~~sensitive~~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. ~~Both the~~The computer based systems and humans ~~who~~that process and use information ~~can be considered~~ fall under the category of 'individuals and information ~~assets and individuals (see~~assets' indicated in Fig. 2~~) and, in~~). In general, only they have the necessary ability to apply information security controls to the information objects containing sensitive information. A computer based system ~~that processes or uses information~~ could be, for example, ~~be~~ an IT system that processes documents, a control system ~~performing~~that performs functions in a nuclear power plant, or an information management system. Computer based systems ~~or~~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. ~~Locked cabinets are another suitable measure to protect the confidentiality and integrity of information (e.g. documents, physical media), but~~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 ~~transportation~~transport.

5.10. The access of individuals to sensitive information should be controlled by a ~~process or~~ procedure that grants access on the basis of the 'need to know' principle and rescinds ~~this~~ access when this need no longer exists. The 'need to know' principle could nevertheless be perceived as incompatible with the overall need to share information in order to support the performance of functions across a regulated entity, 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 ~~the~~which authorized individuals ~~who~~ need access to sensitive information should be made, taking into account other factors (e.g. safety considerations) that might introduce risks for the State. For example, individuals who are responsible for elements of the design and safe operation of a facility should be made aware of all sensitive information relevant to their ~~tasking~~work if this would reduce the risk ~~to the State~~ 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' has~~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 ~~are at times~~can be impractical for enabling the use of information whose sensitivity has a brief lifespan, for ~~instance~~example during the transport of nuclear ~~or~~and other radioactive material. Paragraph 5.45 of IAEA Nuclear

Security Series No. 9-G Rev. 1, Security of Radioactive Material in Transport [~~13~~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 ~~context~~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 ~~and meaning~~ 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~~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 ~~an~~one entity, it is often necessary for information to be ~~shared~~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 ~~or~~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. ~~Similarly, the~~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 ~~could also occur~~.

5.18. Both sharing and disclosure should be managed in a way that ensures that sensitive information ~~is~~does not inadvertently ~~shared with, or disclosed to,~~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 ~~dissemination~~sharing of information between authorities should be governed by the State's security procedures. The ~~dissemination~~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 ~~maintain equivalent protection of~~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 ~~would~~ typically describe the necessary protection measures to be applied to sensitive information for the different classification levels in each State. These agreements should also consider how particular requirements (e.g. freedom of information legislation, see para. 5.23) in any one State might affect the handling of the other States' sensitive information.

5.21. In practice, most information ~~will be~~is shared using computer based systems, meaning that computer security controls ~~will be~~are needed to avoid ~~any~~the compromise ~~to~~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. [~~6~~8].

Need for disclosure of sensitive information

5.22. Most States have ~~established~~ laws to address the security of information that is of importance to national ~~interest~~interests. Such laws specify ~~sanctions~~penalties that will be imposed if a person~~, either~~ (a national of either that State or ~~otherwise,~~another) breaches ~~the~~these information security laws ~~governing such information. There are also usually laws that regulate an individual's access to official government information.~~.

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

~~Preparing~~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 ~~compiling~~developing such guidance, the responsible entity ~~will typically~~ should consult relevant government departments and ~~relevant~~ 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 ~~information can be disclosed~~, to whom ~~information can be disclosed~~ and by which ~~methods information can be disclosed~~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 ~~destined for~~to be used in conference presentations, web ~~postings~~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 ~~and~~, information that ~~might be~~was once considered sensitive and unsuitable for disclosure ~~at one time~~ might ~~be significantly~~become less sensitive and more suitable for disclosure ~~at a later~~over time (or vice versa~~), guidance will be subject to change.~~). All guidance should therefore be reviewed and updated periodically and ~~in the event of~~whenever there are significant changes in policies or circumstances.

~~Disclosing~~Disclosure and ~~reclassifying~~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. ~~It is therefore important that difficulties~~Difficulties in reclassification should be considered ~~in~~when first classifying the ~~original classification, and consideration be given to 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 ~~decisions could~~might be undertaken to take into account ~~for~~:

(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 ~~status~~;
(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.

~~DISPOSINGINFORMATION~~

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. ~~Certain~~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~~, such as~~:

(a) Records of nuclear material accountancy;

(b) Historical design information of nuclear facilities;

(c) Records covered under treaties and international agreements.

5.32. The ~~archival~~archiving of such information ~~may~~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. ~~Such an~~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 ~~in the case where~~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 ~~information~~ for many decades, the means of transformation and destruction (e.g. cryptographic methods[18]) 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.

6.2. ~~Regulated entities~~Each regulated entity within the State's nuclear security regime should develop ~~their~~its own information security ~~policies~~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 ~~obligatory~~ rules without much flexibility. In contrast, larger entities, such as nuclear power plants that face unique and complex security challenges, could possess more autonomy in tailoring their information security policy to adhere to a number of regulatory systems 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. ~~Such~~An example of such a cycle for an information security management system is depicted in Fig. ~~6~~7.

6.5. The information security management system should be integrated with the regulated entity's other management systems (e.g. for safety, quality, physical security and computer

[18] ~~Some State's believe~~ It is possible that the advent of quantum computing might undermine traditional public-key cryptographic methods, as quantum algorithms can efficiently solve ~~their~~ underlying mathematical problems.

security) in a coherent manner, forming an integrated management system to ensure a holistic approach to overall management.

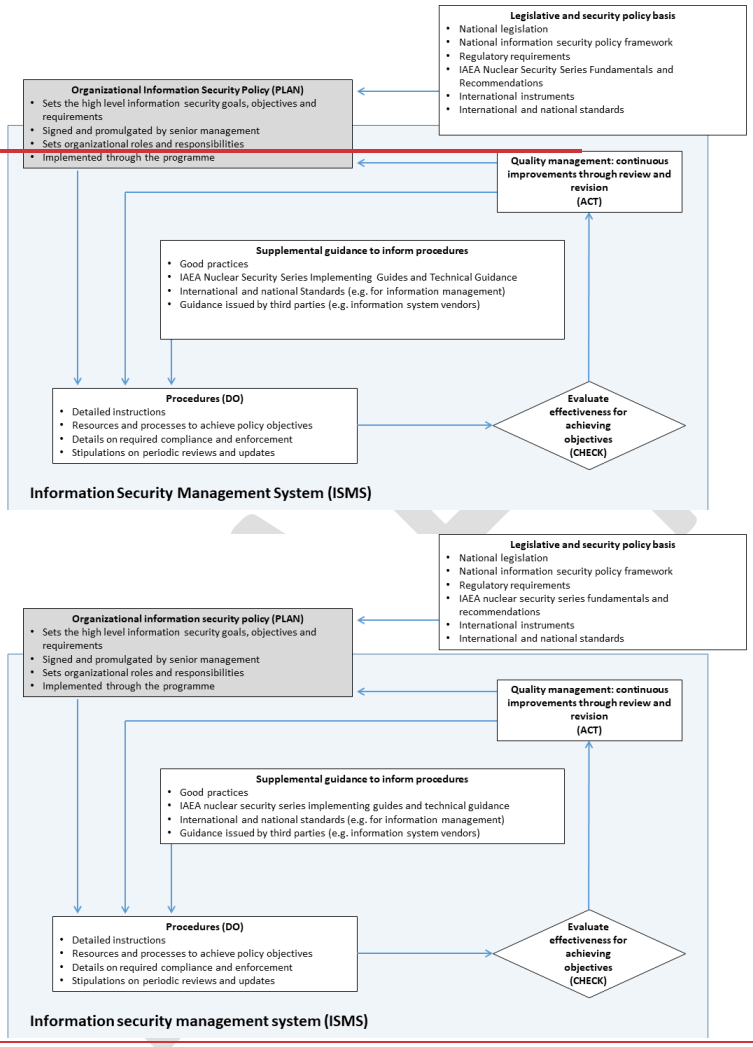


FIG 7. ~~A~~ An example of a 'plan, do, check, act' cycle for the continuous improvement ~~cycle for~~of the information security management system (adapted from Ref. [~~6~~8]).

ELEMENTS OF AN INFORMATION SECURITY MANAGEMENT SYSTEM

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 ~~encompasses~~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 ~~is~~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 ~~ceasing~~ their term of employment ~~as appropriate~~.

6.8. The objectives of the information security management system should be clearly documented in the organization level policy, reflecting ~~the~~a commitment to ~~meet~~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 ~~to adapt, in~~, 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. ~~Risk~~The risk management objectives are to reduce risks to an acceptable level through the application of adequate information security systems and measures throughout the ~~lifecycle~~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, ~~recognizing~~ and ~~leveraging~~ interdependencies with other processes and management systems. may be recognized and leveraged. This integration may also extend beyond the regulated ~~entity's~~entity's boundaries to encompass third parties with information security responsibilities, where ~~necessary~~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 ~~would~~ encompass the ~~allocation of the appropriate~~ information resources, financial investments and the personnel necessary to maintain and enhance the regulated ~~entity's~~entity's information security posture.

6.14. A regulated entity's senior ~~management~~managers should visibly demonstrate their commitment to information security. ~~This includes~~, 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 [14415].

6.16. Activities to assess The assessment of nuclear security culture within organisationsan organization should include information security, with outcomes feeding back into evaluating. The results should be used to evaluate the effectiveness of the information security management system. Evaluation results should be used to , to refine awareness programmes, to adjust security measures, considered within and to enhance personnel behaviours, taking into consideration human factors engineering, and be leveraged to support enhancing personnel behaviours.. People and processes that complement the use of technology are a key factorfactors in securing information, complementing the use of technology, and; the integration of information security into nuclear security culture programmes strengthens this approachcontributes to 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 towards compromisingthat might compromise the confidentiality, integrity, and or availability of sensitive information and sensitive information assets (e.g. social engineering, phishing).

6.18. All personnel should fulfil their security responsibilities, withand the regulated entity providingshould provide appropriate education and training to ensure theirthe 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 originatingthat create sensitive information and operatingoperate 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, or personnel;

(b) Personnel with access to sensitive information, as well as information;

(c) Information owners and managementmanagers accountable for information security at all levels of the organization, specific training and briefings regarding their responsibilities. .

6.20. 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

Formatted: Indent: Left: 0.1", No bullets or

these attributes, personnel are better equipped to effectively identify, report, assess and mitigate risks, ensuring a more robust information security management system.

6.21. ~~Information~~One-off information security training ~~events that are limited to one single event~~courses might not adequately reinforce ~~training, and over the long term could allow~~ the knowledge imparted, with the result that personnel ~~to~~ become complacent~~.~~ in the long term. All ~~those~~individuals who handle sensitive information, including ~~management, personnel and~~ contractors, should receive continual on the job training and be required to attend periodic refresher courses. Personnel who handle sensitive information without necessarily being aware of its content should also receive security training specific to their responsibilities. Records should be maintained of 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. ~~A suggested~~An example format and content for a training ~~and awareness programmes~~programme is provided in Annex III.

Security measures and information security system

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 ~~in the~~, based on a graded approach, should be described in the information security management system. ~~An~~For example ~~would~~, 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. ~~This process should result in a combination of~~These security measures ~~drawn from~~should encompass information security, computer security (see Ref. [~~68~~]), 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 ~~so~~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 ~~for personnel that need access~~; if deemed necessary, a limited check of an individual's background could be sufficient. For access to information with a higher classification level, a more comprehensive set of background checks ~~will~~should be ~~needed~~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~~. The obligations under such an agreement should be reinforced during activities associated with the cessation of employment.

(c) Physical protection measures should combine ~~a degree of~~ strictly managed access through a secure perimeter with one or more layers of other physical protection measures closer to

the information objects and information assets (e.g. safes, vaults or other secure ~~locations) that are being protected.~~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 ~~[6].~~(see Ref. [8]).

Formatted: Highlight

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. ~~Third parties (as~~As described in para. 3.10~~) can~~, third parties might provide goods ~~and~~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~~. Such agreements could involve~~ (e.g. relating to sensitive information ~~being~~ placed in the care of the third party~~. Contracting regulated~~). 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. ~~Regulated~~The contracting regulated entities should ~~require, and confirm,~~ ensure that any third parties ~~having~~with access to sensitive information operate an information security management system. In addition, ~~third parties~~the contracting regulating entity should ensure the following:

(a) ~~A~~The third party has established a contact point ~~is established~~ 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 regulated ~~entities~~entity or competent authorities, 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 ~~have~~ access ~~to,~~ or ~~the ability to~~ modify~~,~~

sensitive information and sensitive information assets. ~~Such a system should typically include the~~The following should be defined for such a system:

(a) ~~Defined responsibilities~~Responsibilities regarding the management of authorization ~~of~~to access ~~to~~ sensitive information;

(b) ~~Defined processes concerning who~~Who has the right to access and modify sensitive information and sensitive information assets, and who has the right to grant further access;

(c) ~~Defined processes concerning how~~How to verify, control and supervise the function of ~~assigning~~granting access;

(d) ~~Defined processes~~Processes to determine the duration of an authorization to access sensitive information and sensitive information assets;

(e) ~~Defined processes~~Processes to revoke authorization to access sensitive information and sensitive information assets due to an incident, employee turnover, and changes in job functions;

(f) ~~Defined processes~~Processes to maintain full traceability ~~with regard to the management of rights during all of the steps involved~~ in ~~the management of~~managing authorizations to access sensitive information and sensitive information assets.

Information security management system 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 [~~7~~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 ~~logging and alert~~ systems should be used to detect and alert on insider activities. Such systems should be capable of identifying unauthorized sensitive information transfers (i.e. ~~a~~ data loss prevention).

6.34. Paragraph 4.10(c) of Ref. [~~7~~11] states that ~~a key mitigation aspect of information security is~~preventive measures against insider threats can be used "to minimize opportunities for malicious acts by limiting access, authority and knowledge of insiders~~". Such limitations can be accomplished, for example,~~." One way of accomplishing this is by dividing critical functions into two parts that necessitate separate authorizations (i.e.~~g.~~ use of the 'two person rule').

Assurance activities for the management system

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 ~~establish~~ ensure that there are internal resources and ~~a process~~established processes to conduct self-assessments and ~~audits utilising an~~ independent ~~auditor~~audits. These ~~inspections~~self-assessments and audits should ~~be performed to determine~~ascertain whether the ~~practiced~~ regulated entity's approach to information security complies with ~~the regulated entity's~~ its information security policy, and whether ~~it remains~~the

Formatted: Font: Italic

Formatted: Font: Italic

Formatted: Font: Italic

Formatted: Font: Italic

approach is in compliance with the State's regulatory and policy frameworks. ~~Through such inspections, the regulated entity will be able to check compliance more frequently than they would in the case of having to undergo external inspections. Moreover, the~~The regulated entity may establish internal training ~~and procedures for inspections~~on self-assessments and audits, ~~to enable conduct by trained~~so that they can be conducted by personnel who are familiar with the internal requirements, procedures and systems ~~allowing the identification of~~. 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 ~~that differ from those discovered through external inspection~~.

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, ~~issues of~~ consideration should be given to confidentiality and trustworthiness ~~should be addressed in relation to the exchange of~~when sharing sensitive information ~~with these external auditors~~.

6.39. ~~Inspection and audit results~~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 regulated entity or the competent authority for information security ~~and~~, with specific time frames ~~for the rectification or implementation of actions~~assigned. There should be ~~assigned. Organizations should also ensure~~a mechanism in place to follow up ~~of rectification and~~ on the implementation ~~actions, verifying the overall~~and effectiveness of these actions.

Continuous improvement of the information security management system

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. ~~6). Additionally, this~~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, ~~and~~ particularly those stemming from criminal or ~~other~~ intentional unauthorized acts, necessitate an adaptable response strategy. These incidents can range from unauthorized disclosure of sensitive information to malicious modification of sensitive information ~~in use contributing to the realization of~~, with a corresponding nuclear security impact (see ~~figure~~Fig. 5). Incident response is necessary ~~for~~in relation to both digital and physical collections of sensitive information (i.e. sensitive information objects and sensitive information ~~assets including sensitive digital~~ assets).

6.42. Additional guidance on computer security incident response specific to nuclear facilities can be found in Appendix 1 of ~~IAEA Nuclear Security Series No. 17-T Rev. 1, Computer Security Techniques for Nuclear Facilities [12~~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 ~~various types~~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 prepare an incident response plan. This plan should do the following:

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

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

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

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

(e) Outline steps to contain the incident so as to prevent further loss of confidentiality, integrity or availability. These steps might involve mobilizing other resources ~~in~~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 ~~relating to~~arising from the incident, such as reporting obligations, data protection laws, and ~~potential~~ engagement with law enforcement or legal counsel~~;~~.

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

(j) ~~Plan~~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, ~~through the use of~~based on feedback from drills, lessons identified ~~in~~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~~, for~~ (e.g. unauthorized exfiltration of sensitive information), the ~~alerting of monitoring personnel in an~~ expeditious ~~manner, for ensuring effective~~alert of personnel, monitoring of the incident, and ~~for verifying on an~~ ongoing ~~basis~~verification of the integrity and availability of backups of information and information assets. ~~An example of a detection security measure is a system that detects unauthorized exfiltration of sensitive information.~~

6.47. 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. ~~Incidents, such as the breach of highly classified~~Some information ~~or a sophisticated cyber attack against an instrumentation and control system, can~~ security incidents occur without any prior indication, ~~and necessitate immediate response measures to mitigate their~~

~~impact. However, experience has shown such incidents may actually~~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 ~~nuclear security, including breaches of~~ information security~~,~~ in the nuclear security regime to the competent authority for information security and to other ~~defined~~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 escalated 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 ~~organization~~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 ~~would be~~is the failure to lock up or secure a document properly, with no result in terms of the loss or compromise of information. ~~A~~An example of a major incident~~, for example, would be~~ is the theft of a highly sensitive document outlining security procedures, resulting in a significant risk ~~for~~to the ~~organization~~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 ~~in security failures~~ should be identified and ~~could underline a~~the need for changes to the information security policy framework or for improvements in the information security management ~~systems~~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).

~~[2]~~[1] ~~INTERNATIONAL ATOMIC ENERGY AGENCY, IAEA Nuclear Safety and Security Glossary: Terminology Used in Nuclear Safety, Nuclear Security, Radiation Protection and Emergency Preparedness and Response, 2022 (Interim) Edition, IAEA, Vienna (2022).~~

~~[3]~~[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).

~~[4]~~[5] INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Recommendations on Radioactive Material and Associated Facilities, IAEA Nuclear Security Series No. 14, IAEA, Vienna (2011).

~~[5]~~[6] EUROPEAN POLICE OFFICE ~~EUROPOL~~, INTERNATIONAL ATOMIC ENERGY AGENCY, INTERNATIONAL CIVIL AVIATION ORGANIZATION, INTERNATIONAL CRIMINAL POLICE ORGANIZATION–INTERPOL, UNITED NATIONS INTERREGIONAL CRIME AND JUSTICE RESEARCH INSTITUTE, UNITED NATIONS OFFICE ON DRUGS AND CRIME, WORLD CUSTOMS ORGANIZATION, Nuclear Security Recommendations on Nuclear and Other Radioactive Material out of Regulatory Control, IAEA Nuclear Security Series No. 15, IAEA, Vienna (2011).

[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).

~~[6]~~[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).

~~[7]~~[11] INTERNATIONAL ATOMIC ENERGY AGENCY, Preventive and Protective Measures against Insider Threats, IAEA Nuclear Security Series No. 8-G (Rev. 1), IAEA, Vienna (2020).

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

~~[9]~~[1] ~~International Convention for the Suppression of Acts of Nuclear Terrorism, United Nations, New York (2005).~~

~~[10]~~[12] INTERNATIONAL ATOMIC ENERGY AGENCY, Developing Regulations and Associated Administrative Measures for Nuclear Security, IAEA Nuclear Security Series No. 29-G, IAEA, Vienna (2018).

~~[11]~~[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).

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

~~[13]~~[14] INTERNATIONAL ATOMIC ENERGY AGENCY, Security of Radioactive Material in Transport, IAEA Nuclear Security Series No. 9-G (Rev. 1), IAEA, Vienna (2020)

~~[14]~~[15] INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Culture, IAEA Nuclear Security Series No. 7, IAEA, Vienna (2008)

~~[15][1] 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).~~

Annex I

EXAMPLE OF A CLASSIFICATION SYSTEM FOR SENSITIVE INFORMATION

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

(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.[2]. The three levels used in this annex are the following:

~~I 2.~~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, ~~more specifically~~ in ~~the case that classified~~particular if sensitive information can be derived from ~~equipment~~these items or ~~physical~~ objects through visual observation ~~of internal or external appearance, structure, operation, testing, application or use.~~

~~I 3.~~1–3. The compromise of information or material classified as '~~SECRET~~'secret' would be likely to fulfil the following criteria:

(a) Raise international tensions;
(b) Cause serious damage to relations between governments;
(c) Threaten life directly, or ~~seriously prejudice~~ public order, individual security or liberty;
(d) Cause serious damage to the operational effectiveness or security of national security forces or to the continuing effectiveness of highly valuable security or intelligence operations;
(e) Cause substantial material damage in terms of national finances, or economic and commercial interests;

Formatted: Bullets and Numbering

Formatted: Indent: Left: 0", First line: 0", Outline numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 1 + Alignment: Left + Aligned at: 1.97" + Indent at: 2.02"

Formatted: Bullets and Numbering

[1] ~~However, inIn exceptional cases, particularly concerning intelligence information and sources pertaining~~in particular relating to the prevention of, or response to, a nuclear security event, a TOP SECRET classification might be warranted. This classification would typically involve highly sensitive intelligence 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.

[2] However, inIn exceptional cases, particularly concerning intelligence information and sources pertainingin particular relating to the prevention of, or response to, a nuclear security event, a TOP SECRET classification might be warranted. This classification would typically involve highly sensitive intelligence 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.

(f) Be of use to an adversary planning a criminal or ~~other~~ intentional unauthorized act that could cause grave damage to a facility with nuclear or other radioactive material, or during the transport of such material.

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

(a) Damage diplomatic relations between States;
(b) ~~Prejudice~~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;
(g) Seriously impede the development or ~~operation~~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 ~~other~~ intentional unauthorized act that could cause serious damage at a facility with nuclear or other radioactive material, or during the transport of such material.

~~I–5.~~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 ~~earnings~~earning potential to individuals or companies, or facilitate improper gains or advantages for an adversary;
(e) ~~Prejudice~~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 ~~other~~ intentional unauthorized act that could cause significant damage at a facility with nuclear or other radioactive material, or during the transport of such material.

~~I–6.~~1–6. The above classification levels can be applied to ensure the control of sensitive ~~nuclear~~ 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:

Formatted: Bullets and Numbering

Formatted: Bullets and Numbering

Formatted: Bullets and Numbering

(i) Design of security systems or specific vital equipment;

(ii) Building plans;

(iii) Methods and procedures for the transfer, accountability and handling of nuclear ~~or~~and other radioactive material;

(iv) Security plans, procedures and capabilities;

(v) Existing vulnerabilities of the security systems and computer based systems ~~which are not eliminated yet and are~~ documented ~~after~~in audits, inspections~~, exercises etc~~ 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 using the following:

(i) Design information ~~useful in developing a device~~;

(ii) Location of material needed to manufacture a device;

(iii) Location of a nuclear weapon.

(e) Dispersing nuclear or other radioactive material in the environment using information on the location, form and quantity of ~~nuclear or other radioactive~~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~~,~~ ~~hindering~~ 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 ~~or~~and other radioactive ~~materials~~material, its use or storage.

Annex II

EXAMPLES OF SENSITIVE INFORMATION RELEVANT TO NUCLEAR SECURITY

II–1. This Annex II provides an example of what mayexamples of information relevant to nuclear security that might be considered sensitive information. The. Each State is to decidedecides the exact level of classification to be applied to each item of information, or produceproduces guidance within the information security policy framework to delegateon delegating this decision to regulated entities. Table II–1 includespresents examples of sensitive information categories and identifies the sensitivity issues associated with this informationeach category.

II–2. The categories of information presented in Table II–1 are not intended as a comprehensive list or model, and; they are simply indicative of what might be considered sensitive information. The relevance of these categorieseach category and theiritsits potential inclusion in a national tableclassification 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 divided by header rows representing topics relevant to nuclear security. The second column indicates whether this category is usually applicable to nuclear material and nuclear facilities (NSS 13 [II–1]), other radioactive material and associated facilities (NSS 14 [II–2]), the detection of and response to material outside of regulatory control (NSS 15 [II–3]) or a combination of these. The third column indicates whether this information could be considered sensitive (in terms of confidentiality, integrity, or availability) or not sensitive. The final column provides an explanation of the sensitivity of information and the rationale for securing it.. The 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 whether an item is sensitive,sensitivity given in the third column, and the explanation, and the rationale given in the fourth column are provided as non-exhaustive examples only.[3]. For most scenarios, in each row in Table II Icategories of sensitive information, a combination of confidentiality, integrity and availability willsensitivities apply.

[3] 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 non-exhaustive exampleexamples of security concerns relevant to nuclear security for each item from produced from expert opinion.. Other attributes, explanations, and rationales willmay apply, depending on the specific context, implementation, and use case among other factors. These will be different betweenvary among regulated entities.

~~In most cases,~~ even if only one or two are specified in the table ~~identifies a single sensitivity associated with the scenario. In some cases there are multiple scenarios described.~~. 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. ~~In terms of~~When designating the ~~designation~~sensitivity of information ~~as sensitive~~ and ~~the assignment of a potential~~assigning classification level, the State ~~can~~might give consideration to whether the information ~~that has already appeared~~is in the public domain~~, or to any previous compromise or possible compromise of information~~ or has previously been compromised. It might be impractical to assign and manage a classification level for such information.

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

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

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

			precise details of where material is stored within the site. For nuclear facilities, such plans ~~would~~ also contain details of other areas essential to the operation of the site.
1.4. Security reports			
A. Reports from security surveys, inspections and assessments, and other reports on physical protection or technical security measures used at a site or facility	[II-1], [II-2]	Confidentiality	Access to these reports could provide adversaries with details on the location of material, the measures taken to protect material and any assessed vulnerabilities, thus assisting adversaries in ~~avoiding~~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 ~~avoid~~bypass security measures and could assist them in ~~the~~ targeting a facility.
C. Results of security investigations at a site or facility, including those into leaks and losses of sensitive information	[II-1], [II-2]	Integrity	An 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 ~~arrangements~~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	[II-1], [II-2]	Confidentiality	Detailed information about the physical layout, security features, and storage locations could be leveraged by malicious

medium (e.g. hard copy, electronic files), showing features of physical protection relevant to the prevention of criminal or ~~other~~ intentional unauthorized acts			actors to identify potential vulnerabilities in the ~~facility's~~facility's security system or otherwise aid in planning an attack.
B. Details of construction of vital areas at nuclear power plants and other nuclear facilities	[II-1]	Confidentiality	Information of this nature ~~can~~could help adversaries to ~~avoid~~bypass security ~~arrangements~~measures and could possibly assist them in ~~the~~ targeting a facility for sabotage purposes.
1.6. Physical protection systems			
A. The computer ~~program~~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 ~~can~~could leave sensitive areas vulnerable to unauthorized access or to criminal or ~~other~~ intentional unauthorized acts, since surveillance, access control and alarms would not operate as intended to detect or prevent such activities.
B. The types and locations of intrusion detection system sensors and the associated surveillance cameras, including circuit diagrams, the location of critical power supplies, cable runs, and maintenance and testing programmes for this equipment	[II-1], [II-2]	Confidentiality	Any details of this nature ~~would~~could be of use to adversaries who ~~wished~~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 ~~used in preparation of~~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 ~~list~~lists of authorized personnel ~~in the security procedures. Such tampering could lead to~~to obtain unauthorized access to sensitive material~~, with the~~. Such changes ~~potentially going~~might go unnoticed ~~given the perceived legitimacy of~~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~~, which clearly show such information~~.
1.10. Other matters associated with physical protection (e.g. location, ~~set up, manning~~layout, staffing and equipment ~~at~~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 ~~would~~could be of great use to ~~an adversary~~adversaries who ~~wished~~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 ~~material~~ and other radioactive material~~,~~ (e.g. sources that have been received or are being held in specified locations, including the exact locations where spent fuel is held)	[II-1]. [II-2]	Integrity	An insider could modify such records~~, which provide specific details on the nuclear material inventory. The adversary's modifications could~~ to misrepresent the actual quantities or types of nuclear material stored, and potentially facilitate the unauthorized removal or diversion of nuclear 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~~ concerning such inventories.~~. Not all such information is necessarily considered sensitive~~. Risk~~; risk informed processes ~~will~~can help determine whether something is to be designated as ~~'sensitive'~~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~~availability	A disruption in the availability of accurate and up to date information on the movement of nuclear material ~~can~~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	~~High~~As high security vehicles are ~~vehicles~~ specially designed to securely transport nuclear material~~. High security vehicles carry both the nuclear material and~~, this information ~~of the type listed in the column to the left (see 3.2 A to E), which~~ could be of use to an adversary planning ~~an attempt~~ to steal or sabotage nuclear material in transport.
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	
~~D. Load compartment keys, spare keys and combination lock settings, where used~~	~~[II-1]~~	~~Confidentiality~~	

~~E.~~D. ~~Vehicle~~Integrated vehicle tracking system ~~if fitted to the high security vehicles~~; system performance and communications systems	[II-1]	Confidentiality, integrity, availability	
3.3. Nuclear material transport containers			
A. Level of resistance to ~~the~~ attack (i.e. by various means) of transport containers	[II-1]	Confidentiality	This information ~~can~~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 ~~often available on~~typically in the ~~internet~~public domain.
C. Information on the design of specific transport containers (specially protected containers)	[II-1]	Confidentiality	This information ~~can~~could be useful to an adversary planning a sabotage attack with the aim of releasing nuclear material, or planning the theft of ~~the~~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. ~~Successful~~The compromise of these systems could enable an adversary to disrupt the operation of a facility, ~~at a minimum, and to disrupt~~in the ~~systems in a way that leads~~worst case, leading to the release of radioactive material ~~at worst~~ [II-~~5~~4][II-~~6~~5].
5. GUARD FORCES AND RESPONSE FORCES			
5.1. Guard force at a facility			
A. ~~Overall establishment~~Existence of ~~the~~a guard force and the current capabilities of the force	[II-1]	Not sensitive	~~Publicizing the~~The existence of a guard force ~~can~~is often publicized to reassure the public and potentially act as a deterrent.

B. ~~Establishment~~Existence of guard ~~force~~forces and their current capabilities at ~~particular~~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. ~~This type~~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	~~Any~~This information ~~that~~ could help an adversary to estimate in advance the scale of response and the capabilities available in a tactical operational unit ~~are to be secured against disclosure.~~ .
E. Response force location, capabilities, weapons, special response vehicles and hours on duty at a site	[II-1]	Confidentiality	
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 ~~exist~~are in the public domain.
B. Design information questionnaire, and the description~~,~~ and ~~the~~ location of material balance areas and key measurement points	[II-1]	Confidentiality	Such detailed information on the location and quantities of nuclear material could be of use to an adversary planning a criminal or ~~other~~ intentional unauthorized act.
C. Forms concerning physical and chemical material measurements at key measurement points	[II-1]	Confidentiality	
6.2. Measurements and instrumentation data			
A. Precision and accuracy of standard laboratory techniques	[II-1]	Not sensitive	This information is often in the public domain.
B. Data that reveal the sensitivity of measurements or the alarm limits for material unaccounted for at a particular nuclear facility	[II-1]	Confidentiality	Precision and accuracy data relating to actual or typical measurements at sites, whether aggregated or disaggregated, could be of use to an adversary planning the theft of material.
6.3. Nuclear material flow and inventory data stored on IT systems, in hard copy, or ~~in~~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~~, or can be,~~ published in the public domain.

B. Material unaccounted for in material balance areas or key measurement points	[II-1]	Availability	Unavailability of ~~material unaccounted for data~~these figures for particular material balance areas or key measurement points ~~can~~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 ~~affect~~compromise the investigative process, potentially ~~revealing details to~~allowing perpetrators ~~who may~~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	~~Modifications~~The modification of limits of error or uncertainty indicators could hide actual discrepancies in nuclear material accounting.
7. APPLICATIONS FOR ~~LICENSING~~LICENCES AND PERMISSIONS			
7.1 Applications for licensing and permissions for the use of nuclear and other radioactive materials.			
~~7.1~~A. Applications ~~for licensing and permissions,~~ without detailed information on security and safety measures~~, and the type, form and quantity of material~~.	[II-1], [II-2]	Not sensitive	The content of such applications ~~will vary~~varies depending on the legal and regulatory framework, and the specific end use~~. If applications contain~~ of the material. Consideration is focused on whether they include sensitive information ~~that could be of potential use~~related to ~~an adversary, the application is to also be treated as sensitive information~~nuclear security and its interfaces with nuclear safety.

Formatted: Indent: Left: 0", First line: 0"

~~7.2~~B. Applications for ~~licensing~~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	~~The content of such applications will vary depending on the legal and regulatory framework, and the specific end use.~~ If applications contain sensitive information that could be of potential use to an adversary, the application is also to be treated as sensitive information.
8. SAFETY CASES, ENGINEERING ~~DOCUMENTS AND~~ INFORMATION, OTHER INFORMATION ON SAFETY~~, ENVIRONMENTAL INFORMATION~~ 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. ~~the~~ 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 ~~type of~~ detailed information contained in safety cases could be useful to adversaries, for example for selecting targets and planning attacks.
B. Details concerning the strengths and weaknesses of processes, structures and protection systems designed to contain, control or secure nuclear ~~material or~~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			

Formatted: Indent: Left: 0", First line: 0"

9.1. Response and contingency			
A. Existence of a security response plan and a contingency plan	[II-1], [II-2]	Not sensitive	~~Publicizing~~ the existence of such plans ~~can~~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 ~~a deliberate attack.~~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 ~~an emergency~~ severe emergency conditions. Secure and reliable communications would contribute to preventing this ~~[II-4].~~ (more information is provided in Ref. [II-6]).
~~9.3. Security contingency plans, including detailed information~~	~~[II-1], [II-2]~~	~~Confidentiality, availability~~	~~Such documents contain information on established security measures, on the capabilities of the police or guard force contingents and on the response to a potential security incident. The inaccessibility of such plans can lead to disorganized and ineffective responses in actual security incidents.~~
9.~~4~~3. Exercises			

A.	Information ~~concerning~~on security exercises that are to be undertaken~~,~~ or ~~that~~ have already been undertaken	[II-1], [II-2]	Not sensitive	~~Publicizing the existence~~The conduct of security exercises ~~can~~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 ~~in the conduct of~~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 ~~response force armaments~~weapons used and ~~the nature of~~ 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 ~~will~~ mandate the protection of this type of information as it can be used for blackmail or extortion purposes, ~~this~~which could ~~also~~, 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. ~~on the fact that~~sites where waste is stored ~~at a particular site, or on~~, aggregated quantities of waste ~~without providing the location~~)	[II-1]	Not sensitive	Such information is generally in the public domain and does not ~~describe the~~provide specifics that could be useful to potential adversaries.
B. Information that could be used in a criminal or ~~other~~ intentional unauthorized act or could enable identification of the radioactive waste held in a specific building at a facility and ~~the material held in the building~~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 ~~store~~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 ~~on~~of the construction~~,~~ and security measures of the facility and the quantity or type of material that is to be processed and stored ~~in facilities (i.e. new build) for the treatment and storage of waste and contaminated material arising from processing activities during decommissioning~~there	[II-1], [II-2]	Confidentiality	This information ~~can~~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 ~~are aware of the required effectiveness of~~know how effective security measures need to be from the design basis threat, they can prepare to overcome or bypass ~~them~~these measures, rendering physical protection ~~defences~~ less effective.
13.3. Details ~~on a~~of vital area identification study	[II-1]	Confidentiality	~~Understanding where~~ Knowing the vital areas of a facility ~~or~~identified by the competent authority ~~has identified vital areas~~ could allow adversaries to infer where security is weaker and identify ~~alternative~~ points of exploitation.
13.4. ~~A security alert that could be~~Security alerts in place ~~and for any changes to the state of alert~~	[II-1], [II-2], [II-3]	Confidentiality, integrity	~~A~~ An adversary could falsely ~~elevated~~elevate a security alert ~~could result~~, resulting in the unnecessary deployment of security resources away from ~~an~~the adversary's intended target and ~~reduce~~a reduction in the effectiveness of physical protection.
14. NUCLEAR TECHNOLOGY			

14.1. Real-time operational data and process control system configurations ~~about~~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~~, or would otherwise assist in defeating security measures~~	[II-2]	Confidentiality	~~Information on~~Adversaries could use this information to calculate precise disassembly times ~~could allow an adversary~~in order to ~~time~~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 ~~the content of confidential vulnerability~~such studies could ~~directly~~ assist adversaries in identifying and exploiting weaknesses within technology designs, leading to targeted attacks that could contribute to a nuclear security event.
15. HISTORICAL INFORMATION FOR THE ABOVE TOPICS			
15.1. ~~Historical~~Sensitive information that dates back some time but is still of current relevance ~~that is still sensitive~~	[II-1], [II-2], [II-3]	Confidentiality	Information of this nature~~, although dated,~~ could still be of use to adversaries.

REFERENCES TO ANNEX II

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

~~[II-2]~~[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-3]~~[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]~~[II-1] ~~INTERNATIONAL ATOMIC ENERGY AGENCY, Method for Developing Arrangements for Response to a Nuclear or Radiological Emergency, Emergency Preparedness and Response, IAEA, Vienna (2003)~~

~~[II-5]~~[II-4] INTERNATIONAL ATOMIC ENERGY AGENCY, Computer Security for Nuclear Security, IAEA Nuclear Security Series No. 42-G, IAEA, Vienna (2021).

~~[II-6]~~[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**~~

~~ELEMENTS OF AN~~

Annex III

INFORMATION SECURITY TRAINING PROGRAMME

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

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

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

~~(1)~~(a) Awareness training ~~that increases awareness of~~on threats and vulnerabilities, and ~~recognition of~~ the need to protect information and information assets, as well as the need to ensure the correct performance of functions.

~~(2)~~(b) Specific training ~~that delves into~~on particular security ~~facets~~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.

~~(3)~~(c) Professional training ~~that typically offers~~providing in depth technical knowledge tailored to individuals in specialized roles~~. Personnel concerned could include~~, such as administrators, information system developers, security personnel, and those involved in the classification and declassification of information.

~~(4)~~(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.

~~INFORMATION SECURITY AWARENESS TRAINING~~

III-4. The information security awareness training could include ~~content to raise awareness on~~ the following topics:

(a) Overview of the national security infrastructure~~;~~.

(b) Different aspects of information security and why they are important to nuclear security~~;~~.

(c) The national classification system~~;~~ for information.

(d) ~~Correct use of markings of~~Markings to indicate the classification of information~~;~~.

(e) Practical examples of applying information security procedures as part of the tasks ~~that~~undertaken by personnel ~~need to undertake;~~.

(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) ~~Security~~ Information security principles, for example granting access to sensitive information on ~~the basis of the~~ a 'need to know' ~~principle;~~basis.

(h) Current risks to information security in relation to deliberate actions ~~resulting from~~by any of the following:

(i) Hostile intelligence services in respect of espionage;

(ii) Subversive organizations;

Formatted: Bullets and Numbering

(iii) Other individuals and groups, such as information brokers and investigative journalists seeking to gain unauthorized access to sensitive information or to nuclear sites and facilities;

(iv) Insider adversaries.

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

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

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

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

(ii) ~~Unwitting~~Vulnerable behaviour that can attract the attention of ~~hostile agencies, along~~adversaries (e.g. engaging in activities that could lead to blackmail);

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

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

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

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

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

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

~~(q)~~(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~~;~~.

~~(r)~~(q) ~~An explanation of the levels~~Levels of security clearance; how trustworthiness determinations are ~~carried out;~~conducted and why they are necessary in the nuclear and radiation industry; ~~and which~~ levels of access ~~relate to~~granted for particular clearance and trustworthiness levels, as well as how ~~this relates to the to the security risks mentioned above;~~trustworthiness determinations relate to protecting nuclear and other radioactive material.

~~(s)~~(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~~, through~~. Examples of possible scenarios include the following:

(i) Unauthorized disclosure ~~– a breach~~(compromise of confidentiality~~.~~);

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

(iii) Unauthorized modification of or interference with information ~~– a breach~~(compromise of integrity~~.~~).

OPPORTUNITIES TO ~~PROVIDE~~RAISE AWARENESS OF INFORMATION SECURITY ~~TRAINING AND ASSURANCE~~

Formatted: Indent: Left: 0.3", Hanging: 0.3", Numbered + Level: 1 + Numbering Style: i, ii, iii, … + Start at: 1 + Alignment: Left + Aligned at: 0.25" + Indent at: 0.5"

Formatted: Indent: Left: 0.3", No bullets or

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

(a) Introductory security briefing: ~~This is a one-hour~~A short session led by the team responsible for information security within the ~~organization~~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 ~~would cover~~covers foundational security concepts and organizational security policies, and ~~it needs to be~~is designed to assist individuals in developing their intuition and experience in detecting compromised information.

III-6. The ~~organization~~regulated entity could establish periodic ~~security~~refresher training and ~~awareness during contract work could include~~outreach, such as the following:

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

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

(c) Organization-wide security drills: Periodic practical security tests for all personnel~~. These tests or drills include~~, including 'red team[22]' exercises, social engineering tests or phishing simulations to assess and enhance the ~~organization's~~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: ~~Utilize data~~Data from security tests and incident reports are used to provide tailored training for specific departments or groups, ~~avoiding less~~which can be more effective ~~approaches designed to target~~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 ~~organization~~regulated entity could also embed information security considerations ~~during~~into the ~~process of~~ personnel separation process, including:

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

[22] '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.

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

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

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

III-8. In addition to an ~~awareness~~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 ~~by an organization~~, including the following:

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

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

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

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

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

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

(h) Use of the organization's intranet site ~~as a valuable tool for conveying~~to convey or ~~promoting~~promote the overall security message ~~under~~, 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 ~~significantly strengthen~~enhance its information security training programme by ~~leveraging~~utilizing the common principles ~~that exist in the overlap~~ shared between the safety and security domains. These ~~shared~~overlapping principles ~~allow for~~enable mutual reinforcement in training ~~for both safety~~, making it easier to convey and ~~security, and can support effectively conveying and equating~~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 ~~should~~need to be aware of the real risks associated with safety and security incidents, including their consequences, ~~underscoring~~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.

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

Formatted: English (United Kingdom)

Formatted: English (United Kingdom)

REFERENCES TO ANNEX III

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

Annex IV

~~EXAMPLE~~ MAPPING OF INFORMATION ~~LIFECYCLE~~LIFE CYCLE ACTIVITIES

IV-1. ~~Annex IV provides an example mapping of~~ Section 5 presents a four-stage information ~~lifecycle~~life cycle model. Table IV-1 shows how information life cycle activities ~~to the four-stage lifecycle model presented~~described in ~~Section 5.~~other publications can be mapped to this model. When considering information ~~lifecycle~~life cycle management, ~~a~~the State, competent authority for information security~~,~~ or regulated entity may ~~consider these example mappings as a reference point~~refer to Table IV-1 to understand how existing or proposed ~~lifecycle~~life cycle activities may be considered in the context of the four-stage model.

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

Reference	Creating	Processing	Using	Disposing
~~23 C Rev. 0~~	~~Create~~ ~~Collect~~ ~~Classify~~ ~~Identify~~ ~~Mark~~	~~Handle~~ ~~Transmit~~ ~~Store~~	~~Use~~ ~~Reclassify~~ ~~Replicate~~ ~~Reproduce~~	~~Destroy~~
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) ~~[IV-1]~~ https://doi.org/10.6028/NIST.IR.7298r3

Formatted: Indent: Left: 0.5", No bullets or