IAEA NUCLEAR SECURITY GLOSSARY

TERMINOLOGY USED IN IAEA NUCLEAR SECURITY GUIDANCE

2020 EDITION

DRAFT, August 2020

CONTENTS

INTRODUCTION

BACKGROUND

The IAEA Nuclear Security Glossary is based on the terminology used in the IAEA Nuclear Security Series and is a companion publication to that Series. The first publication in the Series, Technical Guidance on border monitoring equipment [1] was issued in 2006. The second publication in the Series, on nuclear forensics, was also issued in 2006[1], and was superseded by an updated version [2] in 2015. Four further Technical Guidance publications on specific technical topics [3–6] were issued in 2006 and 2007, followed in 2008 and 2009 by five Implementing Guides on broader aspects of nuclear security[2] (some of which have recently been updated) [7–11] and in 2010 by Technical Guidance on an educational programme for nuclear security[3], which has also recently been updated [12]. Nuclear Security Recommendations for nuclear material and nuclear facilities [13], for radioactive material and associated facilities [14] and for nuclear and other radioactive material out of regulatory control [15] were issued in 2011, followed by further specific Technical Guidance for nuclear facilities[4] (one of which has recently been updated) [16, 17] and more general Implementing Guides on designing and applying nuclear security measures [18, 19]. Nuclear Security Fundamentals were published in 2013 [20], and further Implementing Guides and Technical Guidance on a range of topics [21–44] have been published in recent years. At the time of publication, the set of Nuclear Security Fundamentals, Recommendations and Implementing Guides (and therefore the main set of terminology for the guidance) is largely complete, and this edition of the Glossary represents the terminology of this first iteration of a complete Nuclear Security Series.

The IAEA's nuclear security guidance began with guidance for States on the physical protection of nuclear material, which was further developed through the 1980s and 1990s in the form of INFCIRC/225 and successive Revisions thereof. INFCIRC/225 came to be used by some States Parties to the Convention on the Physical Protection of Nuclear Material (CPPNM) [45] as guidance to assist them in meeting their obligations under the Convention, and the terminology used in INFCIRC/225 was largely the same as that in the Convention. Some guidance was also developed in the late 1990s relating to the security of radioactive sources, but largely as an extension to guidance on the safety of such sources and using some of the terminology of radiation protection.

Since the adoption of the IAEA's first Nuclear Security Plan in 2002, the scope of nuclear security has been broadened to cover other aspects of the security of nuclear material and nuclear facilities, such as material accounting and control and computer security, the security of other radioactive material and associated facilities and activities, and security for nuclear and other radioactive material out of regulatory control (including, for example, measures against illicit trafficking). The terminology used in such guidance has expanded correspondingly, and has been documented progressively in individual guidance publications in the IAEA Nuclear Security Series, through glossaries, footnotes and

[1] INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Forensics Support, Technical Guidance, IAEA Nuclear Security Series No. 2, IAEA, Vienna (2006).

[2] INTERNATIONAL ATOMIC ENERGY AGENCY, Preventive and Protective Measures against Insider Threats, Implementing Guide, IAEA Nuclear Security Series No. 8, IAEA, Vienna (2008).

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

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

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

[3] INTERNATIONAL ATOMIC ENERGY AGENCY, Educational Programme in Nuclear Security, Technical Guidance, IAEA Nuclear Security Series No. 12, IAEA, Vienna (2010).

[4] INTERNATIONAL ATOMIC ENERGY AGENCY, Computer Security at Nuclear Facilities, Technical Guidance, IAEA Nuclear Security Series No. 17, IAEA, Vienna (2011).

descriptions in the text. This is the first attempt to compile the terminology and definitions in one place, both as a resource for drafters and reviewers to improve consistency as further guidance is developed, and as a basis to consider possible improvements to terminology and definitions in future revisions of guidance.

Some of the terminology documented in two other glossaries — the IAEA Safety Glossary [46] and the IAEA Safeguards Glossary [47] — may be of relevance to nuclear security, particularly when there are interfaces between security and safety and between security and safeguards. Where it is considered necessary to avoid confusion, or to discourage unjustified proliferation of different terminology and definitions, reference is made to these other glossaries to clarify commonalities and differences. The relationship between the safety and security glossaries is discussed in more detail below.

GENERAL REMARKS

Purpose

The IAEA Nuclear Security Glossary serves a number of different purposes:

(a) To explain the meanings of technical terms that may be unfamiliar to the reader;

(b) To explain any special meanings ascribed to common words or terms (since words can have several different meanings, it may be necessary to clarify which meaning is intended, in particular for non-native English speakers);

(c) To define precisely how terms — whose general meaning may be clear to readers — are used in a particular publication or set of publications, in order to avoid ambiguity concerning some important aspect(s) of their meaning;

(d) To explain the connections or differences between similar or related terms, or the specific meanings of the same technical term in different contexts;

(e) To clarify and, if possible, reconcile differences in the usage of specialized terms in different subject areas, since such differences in usage may be potentially misleading;

(f) To recommend terms that should be used in IAEA publications and documents (and identify those that should not), and provide the definitions that should be ascribed to them;

(g) To facilitate the translation of IAEA Nuclear Security Series publications.

Definitions of the type used in legal texts such as the CPPNM [45] and its 2005 Amendment [48], or the International Convention for the Suppression of Acts of Nuclear Terrorism (ICSANT) [49], are intended primarily for purpose (c) and, in some cases, do not serve the other purposes at all. Furthermore, definitions of this nature tend to be tailored to the needs of the specific text to which they relate, and hence are often not generally applicable. The ‘definitions’ included in nuclear security guidance publications are, however, less easily classified, tending towards a mixture of definition and explanation and of context specific and generally applicable definitions and/or explanations.

It should be note that a glossary is not the place to specify guidance. The definition of a term should contain the conditions that must be met in order for the term to be applicable, but not other conditions. This is best illustrated by an example. *Sensitive information* is defined as information, in whatever form, including software, the unauthorized disclosure, modification, alteration, destruction, or denial of use of which could compromise nuclear security. It is obvious from this definition that sensitive information is also information that needs to be kept secure — and protecting the confidentiality of sensitive information is specified in the Nuclear Security Fundamentals to be essential to a nuclear security regime — and it may be tempting to add words to that effect to the definition. However, fundamentally it is the consequences of misuse of the information that define it as sensitive, not the need for security measures.

Scope

The IAEA Nuclear Security Glossary comprises a compilation of terminology, definitions and explanations used in publications in the IAEA Nuclear Security Series:

- The main text includes terms that are defined in existing publications in the IAEA Nuclear Security Series, except for specialized technical terms defined only in Technical Guidance publications. As such, the main text is intended to include the main terminology of the IAEA Nuclear Security Series as a whole.
- The Appendix lists definitions of specialized technical terms that are defined only in Technical Guidance publications and address a level of detail beyond that covered in the higher level guidance.
- The Annex provides explanations of other terms used in IAEA Nuclear Security Series publications but not explicitly defined there. These explanations are not approved definitions and are intended only to assist readers' understanding of the text of nuclear security guidance: in the event of any conflict, the approved definitions in the main text and Appendix take precedence. In some cases, the explanations in this Annex take the form of short narrative texts indicating the meaning of a number of related terms and the relationships between them, rather than separate stand-alone explanations for each term.

The scope of the IAEA Nuclear Security Glossary is necessarily limited, and is intended to focus on the key terms that are specific to, or that are used in a specific way in, nuclear security, and in particular those defined and used in IAEA Nuclear Security Series publications. A number of general categories of terms that may be used in security related publications have been specifically excluded from the IAEA Nuclear Security Glossary (except where a specific point needs to be made about a specific term). These groups of excluded terms include:

(a) Basic terms from radiation and nuclear physics that are not specific to nuclear security (e.g. alpha particle, decay, fission, radionuclide). An understanding of these terms is assumed.

(b) Terminology from safety and safeguards that is addressed in the IAEA Safety Glossary [46] or IAEA Safeguards Glossary [47]. Such terms and definitions may in some cases be referred to or discussed in the IAEA Nuclear Security Glossary, but the other glossaries should be consulted where they are the appropriate authorities.

(c) The specialized terminology of fields other than nuclear security (e.g. criminology, intelligence, detection instrumentation or computing), except where such terms have a special meaning or usage in nuclear security. The basic definition of such terms is left to the experts in the relevant fields, and the IAEA Nuclear Security Glossary addresses only any additions or adaptations specific to the nuclear security context.

(d) Highly detailed, specialized terminology from a specific field within security (e.g. the detailed technical terminology of nuclear forensics techniques or performance testing of equipment, or operational details of response force procedures). If necessary, such terminology can be defined in the specialized publications to which it is relevant. In cases where such terms are included in IAEA Nuclear Security Series publications, they are listed in the Appendix of this publication.

Referencing

To help the reader, reference numbers for publications in the IAEA Nuclear Security Series match the publication's number in that series. In a few cases, terms defined in particular IAEA Nuclear Security Series publications, in particular the basic radiological and nuclear terms explained in Ref. [6], are not included because the definition of such basic terms is outside the scope of the Nuclear Security Series. Where a reference is marked with an asterisk (e.g. [13*, 14]), this indicates that the definition so marked is identical to that listed except for the term "nuclear security" being replaced by "physical protection", and/or references to radioactive material and/or associated facilities being replaced by nuclear material

and nuclear facilities. In these cases, the essential meaning of the term is considered to be the same, but different terminology has been used due to a different context.

Where terms the same as or similar to those used in IAEA Nuclear Security Series publications are also used in other key nuclear security documents, such as Conventions and UN Security Council Resolutions, or in IAEA safety standards (and therefore appear in the IAEA Safety Glossary [46]), the other usage (and any difference in definition) is noted for information.

Some other brief explanations have been added where they appear necessary, particularly where there are multiple definitions of the same term or where different terms are used for what appears to be the same concept, but in general no extensive commentary is provided on the terms and definitions listed.

USE OF THE IAEA NUCLEAR SECURITY GLOSSARY

Choosing between multiple definitions

The entry for each term starts with one or more definition(s). Alternative definitions are given:

(a) If different definitions are given in current IAEA Nuclear Security Series publications. In some cases, there are obvious reasons for the differences – for example, if the publications deal with the security of different types of material – but in other cases it is not clear why definitions have been changed or new ones introduced; or

(b) If the term is used in two or more distinct security related contexts; or

(c) If it is necessary to include in the IAEA Nuclear Security Glossary an established definition that is still needed but is not considered suitable as a general definition (for example, some of the definitions from INFCIRC/225 [13] may need to be retained in supporting publications but would not be the preferred general definitions); or

(d) To include definitions of which drafters and reviewers of IAEA publications should be aware, even though they are unlikely to be used in IAEA publications (definitions in the main security related conventions are an important example of this group).

Different definitions for a given term are numbered and referenced.

Unless otherwise specified, preferred definitions are listed first. If a preferred definition is indicated, this should be used unless there is a compelling reason why this is not possible.

If a preferred definition is not indicated, then unless otherwise specified in the text, drafters should use the most appropriate existing definition for their purposes. In particular:

- Preference should normally be given in Implementing Guides and Technical Guidance to definitions from the 'parent' Recommendations[5] or Implementing Guide.
- For guidance on cross-cutting topics, preference should be given to definitions from the Fundamentals [20].
- Otherwise, as a general guide, preference should be given to definitions from publications higher in the hierarchy of the IAEA Nuclear Security Series and/or published more recently. Therefore, for example, definitions from early Technical Guidance publications [1, 3–6] should only be used if there is no other source in the IAEA Nuclear Security Series.

In some cases, the definition(s) is/are followed by further information as appropriate, such as:

(a) Particular notes of caution (indicated by the symbol **!**), such as terms that do not mean what they might appear to mean (e.g. *out of regulatory control*), or potential conflicts with other safety or security related terminology;

[5] i.e. Ref. [13] for nuclear material and nuclear facilities; Ref. [14] for other radioactive material and associated facilities; or Ref. [15] for nuclear and other radioactive material out of regulatory control.

(b) Notes of information (indicated by the symbol ⓘ), such as:

- Explanation of the context(s) in which the term is normally used (and, in some cases, contexts in which it should not be used);
- Reference to related terms: synonyms, terms with similar but not identical meanings, 'contrasting' terms;
- Miscellaneous information: for example, the units in which a quantity is normally measured, recommended parameter values, references.

(c) A special type of information note (indicated by the symbol §) to make the reader aware where there are terms or definitions in the IAEA Safety Glossary [46] that might appear similar or related, to provide clarification of the relationship between the term and/or definitions.;

This supplementary information is not part of the definition, but it is included to assist drafters and reviewers in understanding how to use (or not to use) the term in question.

Use of the Glossary by drafters and reviewers of IAEA Nuclear Security Series publications

Beginning with the preparation of a document preparation profile (DPP) and throughout the development process, drafters of nuclear security guidance publications should, as far as possible, use the terms in the IAEA Nuclear Security Glossary with the meanings given, as described above. Terms should also be used consistently. Every time a different term or form of words is used, the reader may be unsure whether a different meaning is intended. Unnecessary variety of expression should therefore be avoided if there is any possibility of causing confusion or ambiguity, or if in doubt. Terms that are not listed in the IAEA Nuclear Security Glossary may be used, provided that there is no suitable alternative term listed in the IAEA Nuclear Security Glossary.

A publication may contain a list of key terms used in that publication and their definitions, i.e. a glossary for that publication. However, the first question concerning the inclusion of the definition of any term in a publication should always be whether the term actually needs to be defined. Terms should be defined explicitly in a publication only if a definition is essential to the correct understanding of that publication. If the term is used with its normal dictionary meaning, or if its meaning in a particular publication will be obvious to the reader from its dictionary meaning and the context, then there should be no need for a definition. A term whose meaning is imprecise may need to be defined, if the imprecision actually detracts from a correct understanding of the text; in many cases, however, the precise meaning of a term will not be essential for the purposes of a given publication. Similarly, obvious derivatives of a defined term need not themselves be defined unless there is some specific ambiguity that needs to be addressed.

If it is considered necessary to include a term in the list of definitions in an individual publication, the preferred or existing definition should be used wherever possible. If that definition is not suitable (e.g. if the subject of the publication falls outside the scope of the existing definition), the wording of the definition may be modified, but its meaning should not be changed. The technical officer responsible for the IAEA Nuclear Security Glossary should be informed of any such modifications to the wording of definitions.

Similarly, definitions for any additional — usually more specialized — terms needed in a specific publication can be provided by the drafters or the technical officer responsible for the document, and included either in the text (in the main body of the text or footnotes) or in a list of definitions. Such definitions should be copied for information to the technical officer responsible for the IAEA Nuclear Security Glossary.

The technical officer for a publication is responsible for ensuring that any definitions given in that publication are in accordance with these rules.

Reviewers should consider whether each term included in a list of definitions in an individual publication really needs to be defined, and if so whether a list of definitions (as opposed to the text or a

footnote) is the most appropriate place for the definition. (Reviewers should also consider whether any terms not defined in the publication need to be defined.)

If the glossary in a draft publication gives a definition different from the preferred or existing in the IAEA Nuclear Security Glossary, reviewers should check:

(a) That the preferred or existing definition in the IAEA Nuclear Security Glossary could not reasonably have been used;

(b) That the definition given in the draft publication reflects essentially the same meaning as the preferred or existing definition.

Reviewers should make any appropriate recommendations to the technical officer responsible for the publication.

A

access control

See Appendix.

access delay

The element of a *physical protection system* designed to increase *adversary penetration time* for entry into and/or exit from the *nuclear facility* or *transport*. [13]

ⓘ Access delay can be accomplished by physical barriers, activated delays, complexity and/or personnel.

! Note that this is not the whole delay to which an adversary is subject, as it excludes the time needed to complete a malicious act after reaching the target.

administrative control measures

See Appendix.

adversary

Any individual performing or attempting to perform a *malicious act*. [8, 25]

! Where the term *threat* is used in the specific sense of an individual or group of individuals, an adversary is a person or group actually attempting to carry out a *malicious act*, whereas a *threat* is a postulated *adversary* against whom security measures are designed.

alarm threshold value

See Appendix.

area

hazard control area*:* A designated geographical area, representing the maximum extent of all hazards within a *radiological crime scene*, into which, within and from which access is controlled. [22]

inner area: An area with additional protection measures inside a *protected area*, where *Category I nuclear material* is used and/or stored. [13]

limited access area: Designated area containing a *nuclear facility* and *nuclear material* to which access is limited and controlled for physical protection purposes. [13]

operational control area: A designated geographical area, representing the maximum extent of the area needed to support the management of a *radiological crime scene*, into and from which access is controlled. [22]

protected area: Area inside a *limited access area* containing *Category I or II nuclear material* and/or *sabotage* targets surrounded by a *physical barrier* with additional *physical protection measures*. [13, 16, 26]

vital area: Area inside a *protected area* containing equipment, systems or devices, *or nuclear material*, the *sabotage* of which could directly or indirectly lead to *high radiological consequences*. [13, 16]

! Reference [4] gives the definition: "An area inside a protected area containing equipment, systems or devices, or nuclear material, the sabotage of which could directly or indirectly lead to unacceptable radiological consequences. A protected area is an area under surveillance containing category I or II nuclear material and/or vital areas surrounded by a physical barrier." The definition in Ref. [13] is preferred.

associated activity

The possession, production, processing, use, handling, storage, disposal or transport of *nuclear material* or *other radioactive material.* [14, 20, 24, 37, 38]

! Although the wording does not explicitly exclude malicious activities conducted by *adversaries*, this term is presumably intended to refer only to authorized activities.

§ This term is broadly equivalent to an 'activity' in the general term "facilities and activities" used in safety standards [46].

associated facility

A facility (including associated buildings and equipment) in which *nuclear material* or *other radioactive material* is produced, processed, used, handled, stored or disposed of and for which an *authorization* is required. [20, 24, 37, 38]

ⓘ This includes *nuclear facilities* and any other facilities holding significant amounts of *radioactive material*.

§ This term is broadly equivalent to a 'facility' in the general term "facilities and activities" used in safety standards [46].

attack

See Appendix.

authorization

1. The granting by a *competent authority* of written permission for operation of an *associated facility* or for carrying out an *associated activity*, or a document granting such permission. [20, 24, 37]

2. The granting by a c*ompetent authority* of written permission for operation of an *associated facility* or for carrying out an *associated activity*. [14, 15]

§ The same term is used in safety standards with substantially the same meaning: "The granting by a regulatory body or other governmental body of written permission for a person or organization (the operator) to conduct specified activities." [46]

authorized person

A natural or legal person that has been granted an *authorization*. An *authorized person* is often referred to as a "licensee" or "operator". [14, 15, 20]

! The term "licensee" has essentially the same meaning (and is often used when the authorization is called a licence), whereas "operator" is sometimes used in a broader sense that can also include an organization or person applying for *authorization* [46].

§ The term "authorized party" is used in safety standards with a more detailed but broadly similar definition: "The person or organization (the operator) responsible for an authorized facility or an authorized activity that gives rise to radiation risks who has been granted written permission (i.e. authorized) by a regulatory body or other governmental body to conduct specified activities." [46]

availability

The property of being accessible and usable upon demand by an authorized entity. [23]

§ In safety standards, the term is used with a general sense of being in a state to perform a required function under given conditions [46]

B

blended attack

A malicious act involving the coordinated use of both *cyber-attack* and physical attack. [17, 42]

book inventory

See *inventory*.

bulk analysis

The analysis of either an entire sample or a portion of the sample to determine the average properties of the measured portion. [2]

C

candidate vital area set

See Appendix.

capacity

See Appendix.

capacity evaluation

See Appendix.

carrier

Any person, organization or government undertaking the carriage of *nuclear material* by any means of transport. The term includes both carriers for hire or reward (known as common or contract carriers in some States) and carriers on own account (known as private carriers in some States). [26]

§ Definition (and explanatory second sentence) are taken from the Transport Regulations [50], modified to refer only to nuclear material, and to refer to “States” instead of “countries”.

central alarm station

An installation which provides for the complete and continuous alarm monitoring, assessment and communication with *guards*, facility management and *response forces*. [13]

chain of custody

The procedures and documents that account for the integrity of physical evidence by tracking its handling and storage from its point of collection to its final disposition. [2, 22]

ⓘ Other terms for this process are ‘chain of evidence’, ’chain of physical custody’ and ’chain of possession’. [2, 22]

ⓘ UNODC definition taken from Ref. [51].

characterization

Determination of the nature of the radioactive material and associated evidence. [2]

§ The term is used in a variety of contexts in safety standards with the similar broad meaning of determining the nature and activity of radionuclides present in a specified place.

class characteristic

An attribute or feature shared by all members of a class of people or items. [2]

competent authority

A governmental organization or institution that has been designated by a State to carry out one or more *nuclear security* functions. [13–15, 23, 25, 26, 38]. [For example, *competent authorities* may include *regulatory bodies*, law enforcement, customs and border control, intelligence and security agencies or health agencies, etc. [2, 14, 15, 19–22, 24, 37]

§ In safety standards, this term is used only in the specific context of the Transport Regulations [50], with a definition similar to definition 2; in other safety contexts the term 'regulatory body' (implying the regulatory body for the relevant area(s) of safety) is used.

compromise

The accidental or deliberate violation of *confidentiality*, loss of *integrity*, or loss of *availability* of an *information object*. [23]

ⓘ The verb is also used more generally in various publications, without specific definition, to describe security (or some other desirable characteristic) being degraded in some way.

computer-based systems

Technologies that create, provide access to, process, compute, communicate or store digital information, or perform, provide or control services involving such information. [17, 42]

ⓘ These technologies may be physical or virtual. They may include but are not limited to: desktop, laptop, tablet and other personal computers; smart phones; mainframe computers; servers; virtual computers; software applications; databases; removable media; digital instrumentation and control devices; programmable logic controllers; printers; network devices; and embedded components and devices.

computer security

A particular aspect of *information security* that is concerned with the protection of *computer-based systems* against compromise.[17, 42]

computer security incident

An occurrence that actually or potentially jeopardizes the confidentiality, integrity or availability of a computer-based system (including information), or that constitutes a violation or imminent risk of violation of security policies. [17, 42] computer security level

The strength of protection required to meet computer security requirements for a function related to nuclear security, safety, nuclear material accounting and control and/or *sensitive information* management. [17, 42]

computer security measures

Measures intended to prevent, detect or delay, respond to, and mitigate the consequences of malicious acts or other acts that could compromise computer security. [17, 42]

computer security programme

A plan for the implementation of the computer security strategy specifying organizational roles, responsibilities and procedures. The programme specifies and details the means for achieving the computer security goals and is a part of (or linked to) the overall security plan. [17, 42]

computer security risk management

See Appendix.

computer security zone

A group of systems having common physical and/or logical boundaries — and, if necessary, arranged using additional criteria — that is assigned a common computer security level to simplify the administration, communication and application of computer security measures. [17, 42]

confidentiality

The property that information is not made available or disclosed to unauthorized individuals, entities, or processes. [23]

configuration management

The process of identifying and documenting the characteristics of a facility's physical protection system — including computer systems and software — and of ensuring that changes to these characteristics are properly developed, assessed, approved, issued, implemented, verified, recorded and incorporated into the facility documentation [13, 25]

§ The term is used in safety standards with a similar meaning of identifying and documenting the characteristics of a facility's structures, systems and components [46].

containment

Structural elements (cans, gloveboxes, storage cabinets, rooms, vaults, etc.), which are used to establish the physical integrity of an area or items and to maintain the continuity of knowledge of *nuclear material*. [25]

§ In safety standards, the term 'containment' is used to refer to "Methods or physical structures designed to prevent or control the release and the dispersion of radioactive substances."

contingency plan

Predefined sets of actions for response to unauthorized acts indicative of attempted *unauthorized removal* or *sabotage*, including threats thereof, designed to effectively counter such acts. [13, 19, 26, 37]

ⓘ This is normally understood to be an operator's plan for response within a facility or at the site of an activity. A State's plan may be referred to as a national response plan.

control (of nuclear material)

Activities, devices, systems and procedures that ensure that the continuity of knowledge (e.g. location, quantitative measurements) about *nuclear material* is maintained. [25]

ⓘ This specific meaning relates to nuclear material accounting and control. The term 'control' is used more generally in safety and nuclear security to refer to the function, power or means of directing, regulating or restraining.

conveyance

For *transport* (a) by road or rail: any vehicle used for carriage of *nuclear material* cargo; (b) by water: any seagoing vessel or inland waterway craft, or any hold, compartment, or defined deck area of a seagoing vessel or inland waterway craft used for carriage of *nuclear material* cargo; and (c) by air: any aircraft used for carriage of *nuclear material* cargo. [13, 26]

§ Definition derived from the Transport Regulations [50], modified to refer to nuclear material cargo.

crime scene

A site containing records of activities, alleged to be a crime. [22]

ⓘ UNODC definition taken from Ref. [49].

radiological crime scene: A *crime scene* at which a criminal act or intentional unauthorized act involving nuclear or other radioactive material has taken place or is suspected. [2, 22]

crime scene operations

The procedures that aim to control access at a *crime scene*, to document the scene as it was first encountered, and to recognize, collect, package and remove from the scene all relevant evidence. [22]

ⓘ UNODC definition taken from Ref. [51].

criminal act

See *malicious act*.

criminal or intentional unauthorized act

See *malicious act*.

cyber-attack

A malicious act with the intention of stealing, altering, preventing access to or destroying a specified target through unauthorized access to (or actions within) a susceptible *computer-based system*. [17, 42]

ⓘ Such an act is characterized as a *cyber-attack* because it is directed at or exploits a *computer-based system*. The means by which that system is attacked may be electronic or physical.

D

defence in depth

1. The combination of multiple layers of systems and measures that have to be overcome or circumvented before *nuclear security* is compromised. [9, 13*, 14, 25, 26]

2. The combination of successive layers of systems and measures for the protection of *targets* from *nuclear security threats*. [20]

3. The combination of multiple layers of systems and measures for the protection of *targets* from nuclear security *threats*. [15]

§ The term "defence in depth" is widely used in safety standards. While the general concept is similar, the safety definition of "defence in depth" [46] is too complex and specific to be directly adapted for security. When it is necessary to refer to defence in depth in both security and safety senses in the same nuclear security guidance publication (e.g. when describing security measures against sabotage that use (security) defence in depth to protect structures, systems and components that contribute towards (safety) defence in depth at a nuclear facility), the latter

should be referred to as “safety defence in depth”, and a footnote provided to indicate that, while the security and safety concepts are essentially similar, different formal definitions are used.

defensive computer security architecture

See Appendix.

design basis threat (DBT)

The attributes and characteristics of potential *insider* and/or *external adversaries*, who might attempt *unauthorized removal* or *sabotage*, against which a *physical protection system* is designed and evaluated. [4, 10, 13, 16, 17, 26]

designated nuclear forensic laboratory

A laboratory that has been identified by a State as being capable of accepting or analysing samples of nuclear and/or other radioactive material for the purpose of supporting nuclear forensic examinations. [2]

detection [of a nuclear security event]

1. A process in a *physical protection system* that begins with sensing a potentially malicious or otherwise unauthorized act and that is completed with the assessment of the cause of the alarm. [13, 17, 26]

§ In safety, the term detection normally refers strictly to the detection of radiation by an instrument, which is often taken to imply ‘detection’ of the presence of radioactive material (e.g. in the form of contamination). In nuclear security, detection of a nuclear security event may follow an alarm indicating ‘detection’ by instruments of the presence either of radioactive material or of other material (e.g. shielding material) that may indicate the presence of radioactive material, or of an unauthorized person or act, but may also follow receipt of an information alert based on intelligence indicating that a malicious act may be intended. In either case, detection of a nuclear security event also requires assessment of the alarm or alert to determine whether there is in fact a nuclear security event.

2. Awareness of *criminal act(s)* or *unauthorized act(s)* with *nuclear security* implications or measurement(s) indicating the unauthorized presence of *nuclear material*, or *other radioactive material* at an *associated facility* or an *associated activity* or a *strategic location*. [15, 19 with “Means of attaining…” at beginning, 21]

3. Awareness of a *criminal or unauthorized act* with *nuclear security* implications or measurement(s) indicating the unauthorized presence of nuclear and other radioactive material at an *associated facility* or *associated activity* or a *strategic location*. [18]

detection instrument

A complete functional system, being a combination of hardware and software (or firmware) supported by procedures for installation, calibration, maintenance and operation, used for detecting *nuclear material* or *other radioactive material*. [21]

detection measure

Measures intended to detect a criminal or unauthorized act with nuclear security implications. [15, 18, 21]

! The exact wording above, taken from [18], should be used. The definitions in Refs [15] and [21] read “…a criminal or an unauthorized act…” [emphasis added], which is ambiguous.

detection system

Integrated set of *detection measures* including capabilities and resources necessary for *detection* of a criminal act or an unauthorized act with nuclear security implications. [15, 18 – with "criminal or unauthorized act", 21]

deterministic safety assessment

See Appendix.

device

[The term is used without definition in the following terms and their definitions.]

improvised nuclear device: A device incorporating radioactive materials designed to result in the formation of a nuclear-yield reaction. Such devices may be fabricated in a completely improvised manner or may be an improvised modification to a nuclear weapon. [21, 22, 24]

ⓘ Ref. [13] uses the term ***nuclear explosive device*** without an explicit definition, indicating that such a device could be produced using *nuclear material* obtained by *unauthorized removal*, i.e. improvised. The term *improvised nuclear device* is used particularly to refer to a device built or adapted by a non-State actor using material *out of regulatory control*, which may also be indicative of likely characteristics of the device, but such a device is a *nuclear explosive device*.

radiation exposure device: A device with radioactive material designed to intentionally expose members of the public to radiation. [21, 22, 24, 37]

radiological dispersal device: A device to spread radioactive material using conventional explosives or other means. [21, 22, 24, 37]

ⓘ ICSANT [46] defines a "device" in this sense as: "Any nuclear explosive device; or any radioactive material dispersal or radiation-emitting device which may, owing to its radiological properties, cause death, serious bodily injury or substantial damage to property or to the environment."

! A "device" is defined, with a different meaning, in Ref. [5] (see Appendix).

digital assets

Computer-based systems (or parts thereof) that are associated with or within a State's nuclear security regime. [42]

ⓘ See also *sensitive digital assets*.

dispersal or release

See Appendix.

! The term "dispersal" should be used to describe the spreading of radionuclides or radioactive material into or within the public domain as a result of explosion or other mechanical means, fire, nuclear chain reaction or dissolution in a solvent (e.g. a water supply). The term "release" should only be used in a general sense to refer to radioactive material entering the public domain by dispersal or authorized discharge.

! "Dispersion" is a specific process that may contribute to the dispersal of radioactive material. It should not be used in the general sense of *dispersal*.

E

emergency

A non-routine situation or event that necessitates prompt action, primarily to mitigate a hazard or adverse consequences for human life and health, property and the environment. [37]

ⓘ This includes nuclear and radiological emergencies and conventional emergencies such as fires, release of hazardous chemicals, storms or earthquakes.

ⓘ This includes situations for which prompt action is warranted to mitigate the effects of a perceived hazard.

§ Definition from Safety Requirements for emergency preparedness and response. [52]

nuclear or radiological emergency An *emergency* in which there is, or is perceived to be, a hazard due to:

(a) The energy resulting from a nuclear chain reaction or from the decay of the products of a chain reaction; or

(b) Radiation exposure. [37]

§ Definition from Safety Requirements for emergency preparedness and response. [52]

emergency response

The performance of actions to mitigate the consequences of an *emergency* for human life and health, property and the environment. [37]

ⓘ The *emergency response* also provides a basis for the resumption of normal social and economic activity.

ⓘ Definition from Safety Requirements for emergency preparedness and response [52].

examination

A procedure used to obtain information from evidence in order to reach conclusions concerning the nature of and/or associations related to evidence. [2]

ⓘ Should not normally need a definition: if used, the text should make clear the specific meaning in the context of the publication.

external adversary

An *adversary* other than an *insider*. [8]

F

facility function

See Appendix.

false alarm

An alarm found by subsequent assessment not to have been caused by the presence of *nuclear or radioactive material*. [21]

force-on-force exercise

A *performance test* of the *physical protection system* that uses designated trained personnel in the role of an adversary force to simulate an attack consistent with the *threat* or the *design basis threat*. [13, 26]

front line system

See Appendix.

G

graded approach

1. The application of *nuclear security measures* proportionate to the potential consequences of a *malicious act*. [13*, 14, 25, 26]

! [13*], [14] and [25] use the word "proportional", which has a similar sense but implies too precise a relationship.

2. The application of *nuclear security measures* proportionate to the potential consequences of criminal or intentional unauthorized acts involving or directed at *nuclear material*, *other radioactive material*, associated facilities or associated activities or other acts determined by the State to have an adverse impact on nuclear security. [15 with "proportional" instead of "proportionate", 20, 24, 37]

§ The same term is used in safety standards, but defined explicitly to mean applying measures commensurate with the likelihood and possible consequences of, and the level of risk associated with, a loss of control.

guard

A person who is entrusted with responsibility for patrolling, monitoring, assessing, escorting individuals or *transport*, controlling access and/or providing initial response. [13, 26]

ⓘ People carrying out one of these tasks, e.g. escorting an individual, are not necessarily *guards*.

H

hazard control area

See *area*.

high confidence of low probability of failure (HCLPF)

See Appendix.

human factor

See Appendix.

I

improvised nuclear device

See *device*.

incident

ⓘ Several types of *incident* are defined as a basis for categorizing entries in the Agency's Incident and Trafficking Database (ITDB) [53].

§ In safety standards, the term 'incident' is used with the particular meaning: "Any unintended event, including operating errors, equipment failures, initiating events, accident precursors, near misses or other mishaps, or unauthorized act, malicious or non-malicious, the consequences or potential consequences of which are not negligible from the point of view of protection and safety" [46]. In the IAEA Nuclear Security Series the term 'incident' is used only with its general dictionary meaning.

incident commander (IC)

The person in charge of the *nuclear security event*. The IC commands the entire *response* and directs all those supporting the *response*. The IC may delegate authority for performing certain activities to others as required, e.g. to on-scene controller, the public information officer/team. [18]

individualization

The ability to associate a forensic result or a set of results uniquely with a single source, such as a person, place or production process. [2]

information alert

Time sensitive reporting that could indicate a *nuclear security event*, requiring assessment, and may come from a variety of sources, including operational information, medical surveillance, accounting and consigner/consignee discrepancies, border monitoring, etc. [15, 18, 21, 22]

information object

Knowledge or data that have value to the organization. [23]

information security

The preservation of the *confidentiality*, *integrity* and *availability* of information. [17, 23, 42]

initial assessment

The process of analysing systematically and evaluating an *information alert* or an *instrument alarm* to determine whether a *nuclear security event* has occurred. [22]

initial entry

The first controlled entry made into a *crime scene*, conducted for the purpose of gathering data regarding the nature and extent of on-scene hazards. [22]

initiating event

See Appendix.

inner area

See *area*.

innocent alarm

An alarm found by subsequent assessment to have been caused by *nuclear or other radioactive material* under *regulatory control* or exempt or excluded from *regulatory control*. [22]

ⓘ It is therefore a valid alarm: the system indicated the presence of material as it was designed to do, but the subsequent analysis showed that the material was not of security concern. However, this definition is for use in relation to detection of material out of regulatory control.

insider

1. An individual with authorized access to *associated facilities* or *associated activities* or to *sensitive information* or *sensitive information assets*, who could commit, or facilitate the commission of criminal or intentional unauthorized acts involving or directed at *nuclear material*, *other radioactive material*, *associated facilities* or *associated activities* or other acts determined by the State to have an adverse impact on nuclear security. [8, 17, 20]

2. One or more individuals with authorized access to *nuclear facilities* or *nuclear material* in *transport* who could attempt *unauthorized removal* or *sabotage*, or who could aid an *external adversary* to do so. [13, 25, 26]

3. An individual with authorized access to *associated facilities* or *associated activities* or to *sensitive information* or *sensitive information assets*, who could commit, or facilitate the commission of a *malicious act*. [14]

! In general, an insider is somebody with the relevant access, but not necessarily any motivation or intent to commit *malicious acts*.

insider adversary

An *insider* that commits malicious activities with awareness, intent and motivation. [8]

institutional control

Regulatory control or control by any institution that has a role in the investigation, prosecution, extradition or other proceedings of a State related to the location, seizure or recovery of *nuclear or other radioactive material*. [19]

§ The term institutional control is used in some safety standards to indicate a type of largely passive control measures (e.g. restrictions on land use or access) that might be assumed to continue — particularly at a disposal facility for radioactive waste or a contaminated site after remediation — in the long term future after active regulatory control can no longer be assumed to be maintained.

instrument alarm

Signal from instruments that could indicate a *nuclear security event*, requiring assessment. An *instrument alarm* may come from devices that are portable or deployed at fixed locations and operated to augment normal commerce protocols and/or in a law enforcement operation. [15, 18, 21 with "a detection instrument or set of such instruments", 22]

integrity

The property of accuracy and completeness of information [23]

inventory

book inventory: The algebraic sum of the previous *physical inventory* (as determined at a physical inventory taking) and any subsequent inventory changes (as reflected in the inventory change reports). [25]

physical inventory: The sum of all the measured or derived estimates of batch quantities of *nuclear material* physically present at a given time within a *material balance area*, obtained by a facility operator in accordance with specified procedures. [25]

§ The term *inventory* is widely used in safety, especially in radioactive waste safety, to refer to the total amount of radioactive material or radioactive waste within a certain specified area or intended to be managed in a certain specified way (or a breakdown of the characteristics of the material or waste within that total amount, for example the total activity of each radionuclide present). The definitions in Ref. [25] are considered to be consistent with that general concept of *inventory*.

irradiated

! This term (or its opposite, unirradiated) may be used with its normal dictionary meaning. However, the table used to define *nuclear material* in Ref. [13] uses the term "unirradiated"

with a different, specific meaning. Implicitly, "irradiated" material in this context would be material that does not meet the definition of *unirradiated material*.

unirradiated material: Material not irradiated in a reactor or material irradiated in a reactor but with a radiation level equal to or less than 1 Gy/h (100 rad/h) at 1 m unshielded. [13]

ⓘ This definition appears as a footnote to the table defining categories of *nuclear material*.

irregularity

An unusual observable condition which might result from *unauthorized removal* of *nuclear material*, or which restricts the ability of the facility operator to draw the conclusion that *unauthorized removal* has not occurred. [25]

L

limited access area

See *area*.

logic model

See Appendix.

M

major public event

1. A high-profile event that a State has determined to be a potential *target*. [15, 20, 21]

2. A high profile event that a State has determined to be a potential *target* to include, for example, sporting, political, and religious gatherings involving large numbers of spectators and participants. [18]

! This refers to a different type of "event" from a *nuclear security event*.

ⓘ In publications not specifically addressing security for major public events, it should not normally be necessary to give a definition.

malicious act

An act or attempt of *unauthorized removal* of *radioactive material* or *sabotage*. [13*, 14, 26*]

ⓘ A 'criminal act' is normally covered by criminal or penal law in a State, whereas an 'unauthorized act' is typically the subject of administrative or civil law. In addition, criminal acts involving nuclear or other radioactive material may constitute offences related to acts of terrorism[, including those set out in the Convention on the Physical Protection of Nuclear Material and its Amendment and the International Convention for the Suppression of Acts of Nuclear Terrorism, all of] which, in some States, are subject to special legislation. Unauthorized acts with nuclear security implications could include both intentional and unintentional unauthorized acts as determined by the State. Examples of a criminal act or an unauthorized act with nuclear security implications could, if determined by the State, include: (1) the undertaking of an unauthorized activity involving radioactive material by an authorized person; (2) the unauthorized possession of radioactive material by a person with the intent to commit a criminal or unauthorized act with such material, or to facilitate the commission of such acts; or (3) the failure of an authorized person to maintain adequate control of radioactive material, thereby making it accessible to persons intending to commit a criminal or an unauthorized act, using such material. [15, 19 with square bracketed text]

margin

See Appendix.

material balance area (MBA)

An area in a *nuclear facility* designated such that: (a) the quantity of *nuclear material* in each movement into or out of each MBA can be determined; and (b) the *physical inventory* of *nuclear material* in each MBA can be determined when necessary, in accordance with specified procedures, in order that the material balance can be established. [25, in text]

minimal cut set

See Appendix.

N

national nuclear forensics library

An administratively organized collection of information on nuclear and other radioactive material produced, used or stored within a State. [2]

need to hold

Rule by which individuals are permitted to have in their physical possession only the information assets that are necessary to conduct their work effectively. [23]

need to know

1. Rule by which individuals, processes, and systems are granted access to only the information, capabilities and assets which are necessary for execution of their authorized functions. [23]

2. A principle under which users, processes and systems are granted access to only the information, capabilities and assets which are necessary for execution of their authorized functions. [19]

nuclear attribution

See Appendix.

nuclear explosive device

See *device*.

nuclear facility

1. A facility (including associated buildings and equipment) in which *nuclear material* is produced, processed, used, handled, stored or disposed of and for which an *authorization* or licence is required. [20, 37]

2. A facility (including associated buildings and equipment) in which *nuclear material* is produced, processed, used, handled, stored or disposed of and for which a specific licence is required. [13, 25, 26]

- ⓘ The 2005 CPPNM Amendment [48] defines a nuclear facility as a facility (including associated buildings and equipment) in which *nuclear material* is produced, processed, used, handled, stored or disposed of, if damage to or interference with such facility could lead to the release of significant amounts of radiation or radioactive material.
- ⓘ ICSANT [49] defined a nuclear facility as any nuclear reactor, including reactors installed on vessels, vehicles, aircraft or space objects for use as an energy source in order to propel such vessels, vehicles, aircraft or space objects or for any other purpose; or any plant or conveyance being used for the production, storage, processing or transport of radioactive material.

§ Safety standards use the term ‘nuclear installation’, defined as “Any nuclear facility subject to authorization that is part of the nuclear fuel cycle, except facilities for the mining or processing of uranium ores or thorium ores and disposal facilities for radioactive waste” [46]. This definition thus includes: nuclear power plants; research reactors (including subcritical and critical assemblies) and any adjoining radioisotope production facilities; storage facilities for spent fuel; facilities for the enrichment of uranium; nuclear fuel fabrication facilities; conversion facilities; facilities for the reprocessing of spent fuel; facilities for the predisposal management of radioactive waste arising from nuclear fuel cycle facilities; and nuclear fuel cycle related research and development facilities. The term nuclear facility is not specifically defined for safety standards, and since the basis for the definition of nuclear installation refers to the function of the facility rather than the material held and handled there, there is no automatic relationship with the definition of nuclear facility in nuclear security guidance.

nuclear forensic interpretation

The process of correlating sample characteristics with existing information on types of material, origins and methods of production of nuclear and other radioactive material, or with previous cases involving similar material. [2]

nuclear forensic science or **nuclear forensics**

A discipline of forensic science involving the examination of nuclear or other radioactive material, or of other evidence that is contaminated with radionuclides, in the context of legal proceedings. [2]

nuclear material

1. Material listed in the table on the categorization of nuclear material, including the material listed in its footnotes, in Section 4 of IAEA Nuclear Security Series No. 13, Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5). [13, 14, 26] (Table is reproduced below)

2. Any material that is either *special fissionable material* or *source material* as defined in Article XX of the IAEA Statute. [15, 20, 21, 23–25, 37]

ⓘ For practical purposes, both definitions of “nuclear material” are assumed to refer to broadly the same range of material.

Category I/II/III nuclear material: See table below.

Table "Categorization of Nuclear Material", reproduced from Ref. [13]

Material	Form	Category I	Category II	Category III[c]
1. Plutonium[a]	Unirradiated[b]	2 kg or more	Less than 2 kg but more than 500 g	500 g or less but more than 15 g
2. Uranium-235 (^{235}U)	Unirradiated[b] — Uranium enriched to 20% ^{235}U or more — Uranium enriched to 10% ^{235}U but less than 20% — Uranium enriched above natural, but less than 10% ^{235}U	5 kg or more	Less than 5 kg but more than 1 kg 10 kg or more	1 kg or less but more than 15 g Less than 10 kg but more than 1 kg 10 kg or more
3. Uranium-233 (^{233}U)	Unirradiated[b]	2 kg or more	Less than 2 kg but more than 500 g	500 g or less but more than 15 g
4. Irradiated fuel (The categorization of irradiated fuel in the table is based on international transport considerations. The State may assign a different category for domestic use, storage and transport taking all relevant factors into account.)			Depleted or natural uranium, thorium or low-enriched fuel (less than 10% fissile content)[d,e]	

[a] All plutonium except that with isotopic concentration exceeding 80% in plutonium-238.

[b] Material not irradiated in a reactor or material irradiated in a reactor but with a radiation level equal to or less than 1 Gy/h (100 rad/h) at 1 m unshielded.

[c] Quantities not falling in Category III and natural uranium, depleted uranium and thorium should be protected at least in accordance with prudent management practice.

[d] Although this level of protection is recommended, it would be open to States, upon evaluation of the specific circumstances, to assign a different category of physical protection.

[e] Other fuel which by virtue of its original fissile material content is classified as Category I and II before irradiation may be reduced one category level while the radiation level from the fuel exceeds 1 Gy/h (100 rad/h) at 1 m unshielded.

nuclear or radiological emergency

See *emergency*.

nuclear security

1. The prevention of, detection of, and response to, criminal or intentional unauthorized acts involving or directed at nuclear material, other radioactive material, associated facilities, or associated activities. [14, 15, 20 (in text)]

2. The prevention and detection of and response to, theft, sabotage, unauthorized access, illegal transfer or other malicious acts involving nuclear material, other radioactive substances or their associated facilities. It should be noted that 'nuclear security' includes 'physical protection', as that term is understood from consideration of the Physical Protection Objectives and Fundamental Principles, the CPPNM and the Amendment to the CPPNM. [7]

ⓘ The first part of this definition is taken from the second Nuclear Security Plan (GOV/2005/50).

nuclear security culture

The assembly of characteristics, attitudes and behaviours of individuals, organizations and institutions which serves as a means to support, enhance and sustain *nuclear security*. [4, 7 (without "sustain"), 13–15, 20, 26, 38]

§ The IAEA Safety Glossary [46] defines safety culture as "The assembly of characteristics and attitudes in organizations and individuals which establishes that, as an overriding priority, protection and safety issues receive the attention warranted by their significance."

nuclear security culture coordinator

See Appendix.

nuclear security culture enhancement group

See Appendix.

nuclear security culture enhancement programme

See Appendix.

nuclear security culture indicator

See Appendix.

nuclear security detection architecture

The integrated set of nuclear security systems and measures as defined in the IAEA Nuclear Security Recommendations on Nuclear and Other Radioactive Material out of Regulatory Control [15] based on an appropriate legal and regulatory framework needed to implement the national strategy for the detection of nuclear and other radioactive material out of regulatory control. [19, 21]

nuclear security event

1. An event that has potential or actual implications for nuclear security that must be addressed. [15, 17–22, 24, 26, 37, 38]

ⓘ Reference [37] describes three types of nuclear security event:

- Type 1: A *criminal or intentional unauthorized act* leading to dispersal of *nuclear material* or *other radioactive material*, or harmful energy release from a nuclear reaction, or harmful radiation exposure of people due to *nuclear material* or *other radioactive material*. This type of *nuclear security event* is always a *nuclear or radiological emergency*.
- Type 2: A *criminal or intentional unauthorized act* in which there is the confirmed unauthorized presence at a known location, of *nuclear material* and/or *other radioactive material*, but without dispersal of the material, or without uncontrolled energy release from a nuclear reaction, or without uncontrolled radiation exposure. This type of *nuclear security event* is likely to be also a *nuclear or radiological emergency*.
- Type 3: Information alerts are assessed to indicate a credible possibility of a *criminal or intentional unauthorized act*, but the location of the *nuclear material* or *other radioactive material* or *sabotage*, or any planned target, may not be known. In some cases, this type of *nuclear security event* may also be a *nuclear or radiological emergency*.

2. An event that is assessed as having implications for *nuclear security*. [13*, 14, 19*]

ⓘ Ref. [19] refers to this definition (with "physical protection" in place of "nuclear security") as particular to the context of *physical protection*.

nuclear security measures

1. Measures intended to prevent a nuclear security threat from completing criminal or intentional unauthorized acts involving or directed at *nuclear material*, *other radioactive material*, *associated facilities*, or *associated activities* or to detect or respond to *nuclear security events*. [15, 17, 18, 20, 21 in singular form, 24]

2. Measures intended to prevent a *threat* from completing a *malicious act* or to *detect* or respond to *nuclear security events*. [14]

nuclear security regime

1. A regime comprising:

- The legislative and regulatory framework and administrative systems and measures governing the nuclear security of *nuclear material*, *other radioactive material*, *associated facilities*, and *associated activities*,
- The institutions and organizations within the State responsible for ensuring the implementation of the legislative and regulatory framework and administrative systems of nuclear security;
- *Nuclear security systems* and *nuclear security measures* for the prevention of, detection of, and response to, *nuclear security events*. [14, 15, 17, 20, 37, 38]

2. The *nuclear security regime* comprises:

- The legislative and regulatory framework and administrative systems and measures governing the nuclear security of nuclear and other radioactive material, *associated facilities* and *associated activities*;
- The institutions and organizations within the State responsible for ensuring the implementation of the legislative and regulatory framework and administrative systems of nuclear security;
- *Nuclear security systems* and *nuclear security measures* at the facility level, transport level and activity level for *detection* of, and *response* to, *nuclear security events*. [18]

nuclear security system

An integrated set of *nuclear security measures*. [14, 15, 17, 18, 20, 21, 24, 38]

nuclear security threat

See *threat*.

O

operational control area

See *area*.

operator

1. Any person, organization, or government entity licensed or authorized to undertake the operation of an *associated facility* or to perform an *associated activity*. [20, 26, 37, 38]

2. Any person, organization, or government entity licensed or authorized to undertake the operation of a *nuclear facility*. [13, 25]

ⓘ Also used in Ref. [14], with "associated facility" in place of "nuclear facility".

3. Any person, organization, or government entity licensed or authorized to undertake the operation of a *nuclear facility*, an *associated facility* or an *associated activity* such as transport of *nuclear or other radioactive material*. The term therefore includes *shippers/consignors* and *carriers*. [19]

4. An entity (person or organization) authorized to operate a nuclear or radiological facility or authorized to use, store or transport nuclear material and/or radioactive material. Such an entity would normally hold a licence or other document of authorization from a competent authority or be contractors of a holder of such an authorization. [8]

§ This is essentially the same as the definition of 'operator' in the IAEA Safety Glossary [46]. In the safety standards use of the synonymous term 'operating organization' is generally preferred.

other radioactive material

Any *radioactive material* that is not *nuclear material*. [14, 20, 23, 24, 37]

out of regulatory control

See *regulatory control*.

P

performance testing

Testing of the *physical protection measures* and the *physical protection system* to determine whether or not they are implemented as designed; adequate for the proposed natural, industrial and threat environments; and in compliance with established performance requirements. [13, 26]

physical barrier

A fence, wall or similar impediment which provides *access delay* and complements access control. [13]

§ In safety standards, the term 'barrier' is used to mean "A physical obstruction that prevents or inhibits the movement of people, radionuclides or some other phenomenon (e.g. fire), or provides shielding against radiation" [46].

physical control measures

See Appendix.

physical inventory

See *inventory*.

physical protection

ⓘ The preferred approach, in cases where the term physical protection is still used (i.e. primarily in guidance supporting [13]), is to use it without explicit definition, making its meaning clear from the context and the measures described.

ⓘ A footnote in Ref. [13] effectively defines *physical protection* as the nuclear security of nuclear material and nuclear facilities. Hence, when the context is clearly *nuclear material* and *nuclear facilities*, *physical protection* and *nuclear security* may be considered synonymous. However, the term physical protection is sometimes understood to exclude 'non-physical' security measures, such as computer security or nuclear material accounting and control, so the preference is to avoid explicit definitions.

! Ref. [16] gives an explicit definition: "Measures (including structural, technical and administrative protective measures) taken to prevent an adversary from achieving an undesirable consequence (such as radiological sabotage, or the unauthorized removal of nuclear or other radioactive material in use, storage or transport) and to mitigate or minimize the consequences if the adversary initiates such a malicious act." This should not be used in other publications.

physical protection measures

The personnel, procedures, and equipment that constitute a *physical protection system*. [13, 26]

physical protection regime

A State's regime including:

- the legislative and regulatory framework governing the physical protection of *nuclear material* and *nuclear facilities*;
- the institutions and organizations within the State responsible for ensuring implementation of the legislative and regulatory framework;

- facility and transport *physical protection systems*. [13, 26]

ⓘ Because this is an established term, it may be used where essential for consistency with [13], with the understanding that a physical protection regime is that part of a State's nuclear security regime intended to counter unauthorized removal and sabotage of nuclear material and sabotage of nuclear facilities. However, guidance should not normally refer to a "regime" covering a part of nuclear security (e.g. a transport security regime): the convention is that a State has one national nuclear security regime, which includes elements relating to particular areas of nuclear security.

physical protection system

An integrated set of *physical protection measures* intended to prevent the completion of a *malicious act*. [13, 26]

point of [exit or] entry

designated point of exit or entry: An officially designated place on the land border between two States, seaport, international airport or other point where travellers, means of transport, and/or goods are inspected. Often, customs and immigration facilities are provided at these points of exit and entry. [15, 18, 21]

undesignated point of exit or entry: Any air, land and water crossing point between two States that is not officially designated for travellers and/or goods by the State, such as green borders, sea shores and local airports. [15, 18, 21]

ⓘ Sometimes referred to as border crossing points.

! These terms imply entry to and exit from a State and should not be confused with checkpoints or access control points that might operate at points of entry to and exit from a site, a facility or a designated area.

prevention set

See Appendix.

probabilistic safety assessment

See Appendix.

protected area

See *area*.

R

radiation exposure device

See *device*.

radiation search

The set of activities to detect, and identify suspicious nuclear or other *radioactive material out of regulatory control* and to determine its location. [15, 18, 21]

radiation survey

Activities to map the radiation background of natural and human made *radioactive material* in an area or to facilitate later search activities. [15, 18, 21]

§ The term ‘radiological survey’ is defined in the IAEA Safety Glossary as “An evaluation of the radiological conditions and potential hazards associated with the production, use, transfer, release, disposal or presence of radioactive material or other sources of radiation” [46].

radioactive material

1. Any material designated in national law, regulation, or by a *regulatory body* as being subject to *regulatory control* because of its radioactivity. [14, 15, 21, 23] In the absence of such a designation by a State, any material for which protection is required by the current version of the International Basic Safety Standards. [20, 24, 37]

ⓘ If an explicit definition is considered necessary, the second sentence should be included for the avoidance of doubt.

ⓘ The current version of the International Basic Safety Standards is Ref. [54].

§ The definition in safety standards is “Material designated in national law or by a regulatory body as being subject to regulatory control because of its radioactivity”, i.e. the first sentence of the above, but without “regulation” [46].

2. Nuclear material, as defined in the CPPNM; radioactive sources, as defined in the Code of Conduct for the Safety and Security of Radioactive Sources and other radioactive substances containing nuclides which undergo spontaneous disintegration (a process accompanied by the emission of one or more types of ionizing radiation, such as alpha and beta particles, neutrons and gamma rays). [7]

radioactive source

Radioactive material that is permanently sealed in a capsule or closely bonded, in a solid form and which is not exempt from *regulatory control*. It also means any *radioactive material* released if the *radioactive source* is leaking or broken, but does not mean material encapsulated for disposal, or *nuclear material* within the nuclear fuel cycles of research and power reactors. [14]

ⓘ The full definition is from the Code of Conduct on the Safety and Security of Radioactive Sources [55].

! Reference [5] gives a definition: “A means of containment of radioactive material such that the radioactive material remains protected in a leaktight capsule but the radiation is allowed to be emitted for its intended purpose. Also known as a sealed source or source. Radioactive sources are manufactured in accordance with international law for integrity.” This definition should not be used.

§ The preferred definition in the safety standards is more general: “A source [i.e. anything that can cause radiation exposure and can be treated as a single entity for purposes of protection and safety] containing radioactive material that is used as a source of radiation” [46].

radioactive substance

! Stated or implied in some IAEA Nuclear Security Series publications (e.g. Refs [13] and [14]) to be synonymous with *radioactive material*, in order to confirm consistency with the 2005 CPPNM Amendment [45]. In contexts related to the CPPNM Amendment, the terms are synonymous, but in general they may have different meanings – see the entry in the IAEA Safety Glossary [46].

radiochronometry

The use of measurements of radioactive decay products in a sample of material to determine the time elapsed since the last separation of progeny from the parent material (and thus, the ‘age’ of the material in the measured sample). [2]

radiological assessor

A person who, at a *radiological crime scene*, assists by performing radiation surveys, performing dose assessments, assisting with the control of radionuclide contamination, ensuring the radiation protection of *crime scene* personnel and formulating recommendations on protective actions. [22]

radiological crime scene

See *crime scene.*

radiological dispersal device

See *device*.

regulatory authority

ⓘ May be used, with definition 1 of *regulatory body*, to avoid confusion in nuclear security contexts in which the term *regulatory body* might be assumed by readers to imply only the *regulatory body* for safety. (See, for example, Ref. [19]). The term "competent authority with regulatory responsibility" is also used in Ref. [15] for this purpose.

regulatory body

One or more authorities designated by the government of a State as having legal authority for conducting the regulatory process, including issuing *authorizations*. [20]

! Ref. [5] gives a definition from safety: "An organization designated by a national government as having legal authority for regulating nuclear, radiation, radioactive waste and transport safety." This should not be used in security publications.

regulatory control

1. Any form of institutional control applied to *nuclear material* or *other radioactive material*, *associated facilities*, or *associated activities* by any *competent authority* as required by the legislative and regulatory provisions related to safety, security, or safeguards. Explanation: The phrase 'out of regulatory control' is used to describe a situation where *nuclear* or *other radioactive material* is present in sufficient quantity that it should be under *regulatory control*, but control is absent, either because controls have failed for some reason, or they never existed. [15, 20–22, 24, 37]

! ***out of regulatory control*** refers to the absence of the direct control over material by an *authorized person* that is or would be mandated by *regulatory control* for such material. Material might therefore be designated as *out of regulatory control* even when some aspects of *regulatory control* are in place.

2. Any form of institutional control applied to *nuclear material* or *other radioactive material*, *associated facilities*, or *associated activities* by any *competent authority* as required by the legislative and regulatory provisions related to safety, security, or safeguards. Explanation: The phrase 'out of regulatory control' is used to describe a situation where *nuclear* or *other radioactive material* is present without an appropriate *authorization*, either because controls have failed for some reason, or they never existed. [14, 19]

§ The term is used in safety standards with a broadly similar definition: "Any form of control or regulation applied to facilities and activities by a regulatory body for reasons relating to nuclear safety and radiation protection or to nuclear security" [46].

response

All of the activities by a State that involve assessing and responding to a *nuclear security event*. [15, 18, 19, 21]

§ In safety, 'response' normally refers to response to a *nuclear or radiological emergency*, i.e. to the consequences for the safety of people and the environment of an accident or a *nuclear*

security event. In security, 'response' normally refers to response to a *nuclear security event* itself, including identifying, pursuing and interdicting the cause of the event.

response forces

Persons, on-site or off-site, who are armed and appropriately equipped and trained to counter an attempted *unauthorized removal* or an act of *sabotage*. [13, 26]

response measure

A measure intended to assess an alarm/alert and to respond to a *nuclear security event*. [15, 18, 21, 22]

response system

An integrated set of *response measures* including capabilities and resources necessary for assessing the alarms/alerts and *response* to a *nuclear security event*. [15, 21, 22]

risk

The potential for an unwanted outcome resulting from a *nuclear security event* as determined by its likelihood and the associated consequences. [24, 37]

! A number of IAEA Nuclear Security Series publications, notably Ref. [13], refer to different "types" of *risk* relevant to nuclear security, specifically: the risk of unauthorized removal of radioactive material (with possible subsequent dispersal or use to cause radiation exposure or, in the case of nuclear material, with the intent to construct a nuclear explosive device); and the risk of sabotage. This wording could be understood to be used in a loose and general way, but possibly more specifically to indicate that successful unauthorized removal of material or sabotage would itself be a "consequence", in which case the "risk" would be rather vaguely that to society or the world in general. The descriptions in the text, however, indicate that the "types" are actually the risk associated with unauthorized removal and the risk associated with sabotage, i.e. the risks to people who might be affected by a malicious act using removed material or releases from a sabotaged facility, which is more consistent with the normal IAEA usage of 'risk'.

§ The concept of risk is referred to extensively in safety. Depending on the context, it may be defined precisely, e.g. by a mathematical expression, or more generally [46]. However, it always refers to a combination of the likelihood or probability of something happening and the consequences if it does happen, as does the definition in Ref. [24]. In safety, quantitative probabilities (based on observed or modelled frequencies of random events) are often used to calculate risk: in security contexts, likelihoods are very unlikely to be quantifiable, as they usually depend on human decisions and actions rather than random processes.

risk assessment

The overall process of systematically identifying, estimating, analysing and evaluating *risk* for the purpose of informing priorities, developing or comparing courses of action, and informing decision making. [24, 37]

§ The same term is used in safety standards with a similar definition relevant for safety: "Assessment of the radiation risks and other risks associated with normal operation and possible accidents involving facilities and activities" [46].

S

sabotage

1. Any deliberate act directed against a *nuclear facility* or *nuclear material* in use, storage or transport which could directly or indirectly endanger the health and safety of personnel, the public or the environment by exposure to radiation or release of radioactive substances. [13, 16, 26]

! This definition of sabotage is of a technical nature and does not aim to provide a definition for the purpose of criminal law, such as those provided for in the relevant international instruments or national law of States. [13]

ⓘ The definition in Ref. [13] is the same as that in the 2005 CPPNM Amendment [48].

2. Any deliberate act directed against an *associated facility* or an *associated activity* that could directly or indirectly endanger the health and safety of personnel, the public, or the environment by exposure to radiation or release of *radioactive substances*. [14, 37]

- Reference [14] states in a footnote that *radioactive substances* and *radioactive material* have the same meaning. However, with the definition of radioactive material given in Ref. [14] (which does not include the sentence covering material that has not been designated radioactive material by an appropriate authority but should be so designated), this may defeat the purpose of the different wording. The purpose may have been to include, for example, fission products generated in a nuclear fission chain reaction, which are created during that reaction and so may not have been designated as "radioactive material" by an appropriate authority.

safety alarm

See Appendix.

safety alarm threshold value

See Appendix.

scenario

See Appendix.

screening

See Appendix.

self-assessment

See Appendix.

sensitive digital assets

Sensitive information assets that are (or are parts of) *computer-based systems*. [17, 42]

ⓘ Alternatively, these are *digital assets* that store, process, control or transmit *sensitive information*.

sensitive information

Information, in whatever form, including software, the unauthorized disclosure, modification, alteration, destruction, or denial of use of which could compromise nuclear security. [15, 17, 18, 20, 21, 23, 37, 42]

sensitive information assets

Any equipment or components that are used to store, process, control or transmit *sensitive information*. For example, sensitive information assets include control systems, networks, information systems and any other electronic or physical media. [17, 20, 23, 42]

shipment

The specific movement of a consignment (nuclear material) from origin to destination. [26]

§ Essentially the same definition is in the Transport Regulations: "The specific movement of a consignment from origin to destination" [50].

shipper

Any person, organization or government that prepares or offers a consignment of *radioactive material* for *transport* (i.e. the consignor). [13*, 14, 26*]

ⓘ As the parenthetical remark suggests, there are very strong similarities between a shipper and a consignor. The term "shipper" is used in safeguards, and therefore relates particularly to shipment of nuclear material. The only substantive difference between the terms appears to be that movements of nuclear material from one material balance area to another within a facility (transfers) have a shipper, whereas the term "consignor" necessarily implies transport of the material in the public domain. This difference does not appear sufficient to justify different terms, but the term "shipper" is retained for the time being where consistency with higher level guidance is necessary.

sigma multiplier

See Appendix.

signature

A characteristic or a set of characteristics of a given sample that enables that sample to be compared with reference materials. [2]

social engineering

See Appendix.

source material

Uranium containing the mixture of isotopes occurring in nature; uranium depleted in the isotope 235; thorium; any of the foregoing in the form of metal, alloy, chemical compound, or concentrate; any other material containing one or more of the foregoing in such concentration as the Board of Governors shall from time to time determine; and such other material as the Board of Governors shall from time to time determine; but not including ore or ore residue. [20]

ⓘ Taken from the IAEA Statute, as amended by INFCIRC/153 [56].

source term

The amount and isotopic composition of radioactive material released (or postulated to be released) following *sabotage*. [26]

special fissionable material

Plutonium-239; uranium- 233; *uranium enriched in the isotopes 235 or 233*; any material containing one or more of the foregoing; and such other fissionable material as the Board of Governors shall from time to time determine; but not including *source material*. [20]

ⓘ Taken from the IAEA Statute [56].

stand-off attack

An attack, executed at a distance from the target *nuclear facility* or *transport*, which does not require adversary hands-on access to the target, or require the adversary to overcome the *physical protection system*. [13]

standard gamma ray background

See Appendix.

standard neutron background

See Appendix.

standard neutron source configuration

See Appendix.

strategic location

1. A location of high security interest in the State which is a potential *target* for terrorist attacks using *nuclear material* or *other radioactive material*, or a location at which *nuclear material* or *other radioactive material* that is *out of regulatory control* is located. [20, 21, 24 with "nuclear or other radioactive material out of regulatory control", 37]

2. A location of high security interest in the State which is a potential *target* for terrorist attacks using *nuclear and other radioactive material* or a location for *detection* of *nuclear and other radioactive material* that is out of *regulatory control*. [15, 18]

success criteria

See Appendix.

success path

See Appendix.

support system

See Appendix.

surveillance

The collection of information through devices or direct observation to detect unauthorized movements of *nuclear material*, tampering with *containment* of *nuclear material* or falsification of information related to location and quantities of *nuclear material*. [25]

§ The same term is used in safety standards to mean "A type of inspection to verify the integrity of a facility or structure" [46].

system for nuclear material accounting and control

An integrated set of measures designed to provide information on, control of and assurance of the presence of *nuclear material*, including those systems necessary to establish and track nuclear material inventories, control access to and detect loss or diversion of *nuclear material*, and ensure the integrity of those systems and measures. [13 (with "accountancy"), 25]

T

target

Nuclear material, *other radioactive material*, *associated facilities*, *associated activities*, or other locations or objects of potential exploitation by a *nuclear security threat*, including *major public events*, *strategic locations*, *sensitive information*, and *sensitive information assets*. [15, 20, 21, 37]

ⓘ In most cases, this should not need definition, as the general meaning is consistent with the normal dictionary meaning and the context should make clear the specific meaning.

threat

A person or group of persons with motivation, intention and capability to commit a *malicious act*. [4, 13, 16, 26]

! While this is the definition given in Ref. [13], the word threat is used in the text of Ref. [13] in various ways, some of which are not consistent with this definition.

ⓘ In this usage, a *threat* is generally understood to be a postulated person or group against whose capabilities and intentions nuclear security measures are designed, whereas a real person or group who actually takes action to attempt a *malicious act* becomes an *adversary*. However, this distinction is not always maintained consistently, and in some cases it may be difficult to decide which term is more appropriate.

§ A relevant analogy in safety is the postulated initiating event, one of a set of hypothesized events against which safety systems are designed. In this case, however, if the event happens then it is an initiating event. Hence the relationship between the two terms is much clearer. An equivalent for security would be to refer to threats as postulated adversaries, which is a cumbersome term but does not have multiple possible meanings. The term threat could then be used more conceptually, alongside terms such as hazard and risk.

nuclear security threat: A person or group of persons with motivation, intention and capability to commit criminal or intentional unauthorized acts involving or directed at *nuclear material*, *other radioactive material*, *associated facilities* or *associated activities* or other acts determined by the State to have an adverse impact on nuclear security. [20, 24]

threat assessment

An evaluation of the *threats* — based on available intelligence, law enforcement, and open source information — that describes the motivation, intentions, and capabilities of these *threats*. [10, 13, 14, 17, 24 (with *nuclear security threats*), 26, 37]

2. The process of analysing systematically the hazards associated with facilities, activities or sources within or beyond the borders of a State in order to identify:

(a) Those events and the associated areas for which protective actions may be required within the State;

(b) The actions that would be effective in mitigating the consequences of such events.

The term threat assessment does not imply that any threat, in the sense of an intention and capability to cause harm, has been made in relation to such facilities, activities or sources. [4]

[threat beyond the DBT]

See Appendix.

threat statement

A description of credible adversaries (including attributes and characteristics) in the form of design basis threat or representative threat statement, developed on the basis of the national nuclear security threat assessment. [10]

[threat types 1 and 2 (TT-1 and TT-2)]

See Appendix.

technical control measures

See Appendix.

trace element

An element in a sample that has an average concentration of less than 1000 μg/g or 0.1% of the matrix composition. [2]

ⓘ This term is used in various areas of science with different numerical meanings. This definition is specific to *nuclear forensics*.

transport

International or domestic carriage of *nuclear material* by any means of transport, beginning with the departure from a *nuclear facility* of the *shipper* and ending with the arrival at a *nuclear facility* of the receiver. [13, 26]

§ The equivalent definition of the term 'transport' in the safety standards is more general: "The deliberate physical movement of radioactive material (other than that forming part of the means of propulsion) from one place to another" [46].

transport control centre

A facility which provides for the continuous monitoring of a *transport conveyance* location and security status and for communication with the *transport conveyance*, *shipper/*receiver, *carrier* and, when appropriate, its *guards*, and the *response forces*. [13, 26]

two-person rule

A procedure that requires at least two authorized and knowledgeable persons to be present to verify that activities involving *nuclear material* and *nuclear facilities* are authorized in order to detect access or actions that are unauthorized. [13, 25]

U

unacceptable radiological consequences

A level of radiological consequences, established by the State, above which the implementation of *nuclear security measures* is warranted. [4, 13*, 16*]

ⓘ It may sometimes be necessary to clarify that this is definition refers to hypothetical, potential consequences for the purposes of planning nuclear security measure; it does not refer to actual consequence that might be used as a basis for decisions on response actions.

unauthorized act

See *criminal or unauthorized act*.

unauthorized removal

The theft or other unlawful taking of *radioactive material*. [4, 13*, 25*, 26*]

unirradiated

See *irradiated*.

unwitting insider

An *insider* without the intent and motivation to commit a *malicious act* who is exploited by an *adversary* without the unwitting insider's awareness. [8]

uranium enriched in the isotope 235 or 233

Uranium containing the isotope 235 or 233 or both in an amount such that the abundance ratio of the sum of these isotopes to the isotope 238 is greater than the ratio of the isotope 235 to the isotope 238 occurring in nature. [20]

ⓘ Taken from the IAEA Statute [56]. Also used in CPPNM [45] and ICSANT [49].

V

venue

Any identified location (such as a building, stadium, open area/park, religious place) where a *major public event* actually takes place. A *venue* is considered to be a *strategic location*. [18]

ⓘ This term should not usually need explicit definition.

vital area

See *area*.

vulnerability

A physical feature or operational attribute that renders an entity, asset, system, network, facility, activity or geographic area open to exploitation or susceptible to a given threat. [24]

vulnerability assessment

A process which evaluates and documents the features and effectiveness of the overall security system at a particular target. [24]

W

walkdown

See Appendix.

APPENDIX
SPECIALIZED TECHNICAL TERMS DEFINED IN TECHNICAL GUIDANCE PUBLICATIONS

The main text contains the terms and definitions used broadly across the Nuclear Security Series, which represent the main terminology of nuclear security and its regulation. A key aim of the main text is to promote consistency in the use of this terminology in different publications.

This Appendix lists some more specialized technical terms that are defined and used only in a small number of IAEA Nuclear Security Series (typically Technical Guidance) publications providing detailed guidance on a specific aspect of nuclear security. Consistency between different IAEA Nuclear Security Series publications may be a lesser issue in relation to such terms, but they are recorded in this Appendix for completeness, and to promote consistency between the IAEA Nuclear Security Series publications and other documentation developed by the IAEA, such as more detailed technical publications outside the IAEA Nuclear Security Series and training materials.

administrative control measures

Policies, procedures and practices specifying permitted, necessary and forbidden actions to protect computer-based systems by providing instructions for actions of employees and of vendors, contractors and suppliers. [17]

alarm threshold value

Prescribed number of *sigma multipliers* above the background value [1].

candidate vital area set

A *prevention set* (complement cut set or minimal path set) for a *sabotage area logic model* that identifies a set of areas whose protection will prevent *malicious acts* leading to *unacceptable radiological consequences*. *Sabotage* cannot be accomplished unless the saboteur can enter at least one area in the *prevention set*. [16]

capacity

An ‘absolute’ measure of the robustness of SSCs subjected to a particular threat that can include physical, operational and administrative attributes. Capacity is defined relative to a specific metric. Code capacity is a measure of a plant design feature relative to the code. Failure capacity is a measure of the robustness of SSCs subjected to a particular threat. [4]

capacity evaluation

The process of establishing the capacity of SSCs, operational procedures, PPSs, etc., when subjected to a particular threat. An example is the establishment of the failure capacity, strength or robustness of structures and components to impact, impulse, explosion, vibration, steam and/or loading conditions. Capacity evaluation may identify vulnerabilities and systems interactions; items under evaluation are usually found to be considerably more robust than the design limits. [4]

computer security risk management

Assessment and management of the risks associated with possible cyber-attacks that have the potential to degrade nuclear safety or nuclear security. CSRM is conducted at a facility level and at a system level. [17]

defensive computer security architecture

Arrangement of computer-based systems according to design requirements, constraints and measures that are to be imposed during the lifecycle of a system, such that the systems performing identified facility functions having significance to the safety and security of the facility and assigned to computer security levels on the facility level have the required level of protection. [17]

deterministic safety assessment

A comprehensive, structured analysis that assesses the performance of the facility against a broad range of operating conditions, postulated initiating events, and other circumstances, demonstrating that normal operation can be carried out safely, in such a way that facility parameters do not exceed operating limits. [16]

§ This term is not defined in the safety standards; see the entry in the IAEA Safety Glossary for 'deterministic analysis' [46].

device

A piece of machinery or instrument in which a radioactive source is used, and which safely houses the source. The manufacture of devices generally conforms to national or international safety standards. [5]

! Clearly this is a different type of "device" from those listed in the main text. The term should therefore only be used with this definition in contexts in which there is no risk of confusion, and then with great care.

dispersal or release

direct dispersal or release: Dispersal or release of material by application of energy from an external source (for example, an explosive or incendiary device) on the material. [16]

indirect dispersal or release: Dispersal or release of material by utilizing the potential energy (i.e. heat or pressure) contained in the nuclear or radioactive material or in a process system to disperse the material. [16]

facility function

A coordinated set of actions, processes and operations associated with a nuclear facility. Their purpose may be, but is not limited to, performing functions important or related to nuclear safety, nuclear security, nuclear material accounting and control or sensitive information management. [17]

ⓘ Reference [17] uses the term *facility function* to refer to any security, safety or other function at a nuclear facility that computer security measures may be needed to protect. Ref. [42] uses the same concept of functions that need to be protected, but the scope of Ref. [42] is not limited to facilities, and therefore these functions are not described as *facility functions*.

§ A *safety function* is defined as: "A specific purpose that must be accomplished for safety for a facility or activity to prevent or to mitigate radiological consequences of normal operation, anticipated operational occurrences and accident conditions" [46]. In some cases (e.g. sabotage), a safety function may be performed by security measures, but the term is usually used only in the context of safety measures at nuclear installations or radioactive waste disposal facilities.

! A security measure (computer security or nuclear security) may have both a security function and a safety function (and possibly others), so the term "security function", analogous to "safety function", would be more difficult and complex to define. Definition of such a term could also cause confusion as the phrase "security function" is sometimes used without specific definition in other IAEA Nuclear Security Series publications.

front line system

A system that directly performs a facility safety function. See also the definition of *support system*. [16]

high confidence of low probability of failure (HCLPF)

The probabilistic definition of the HCLPF is 95% confidence of less than about a 5% probability of failure. HCLPF values can be estimated using probabilistic or deterministic techniques. The deterministic approach is preferred because, once rules governing the definition of demand and capacity are established, engineers without training in probabilistic methods can perform the evaluations. [4]

human factor

The complex of all individual and collective human physical, psychological and behavioural properties that interact with technological systems, management organizations and natural environments. [38]

initiating event

An event identified during design as capable of leading to anticipated operational occurrences or accident conditions. [16]

- In safety, this is essentially the definition of a 'postulated initiating event', an event against which safety features are designed [46]. It becomes an initiating event ("An identified event that leads to anticipated operational occurrences or accident conditions") if it happens.

initiating event of malicious origin

A maliciously initiated *initiating event*. A *malicious act* that upsets the operation in such a way that, if mitigation were unsuccessful, would lead to *unacceptable radiological consequences*. [16]

logic model

A statement, algebraic expression, or graphical representation that captures the combinations of item failures that lead to an undesired event or undesired system state. [16]

> ***sabotage logic model***: A *logic model* that documents the malicious events or combinations of malicious events that could lead to *unacceptable radiological consequences*. [16]
>
> ***sabotage area logic model***: A *sabotage logic model* that identifies the physical areas from which the malicious events can be performed. The *sabotage area logic model* can be analysed to identify the combinations of areas from which *sabotage* resulting in *unacceptable radiological consequences* can be committed and also the areas that should be protected to prevent *unacceptable radiological consequences*. [16]

margin

A relative measure of expected performance versus a specified criterion or metric. It can be measured and expressed deterministically or probabilistically. One measure of margin is the relationship between capacity and loading condition. For example, for a structural element, a ratio of blast pressure demand and pressure capacity to failure (D/C) of less than one indicates that there is margin to failure. [4]

> ***safety margin***: A measure of the expected performance of the plant as a system when measured against a safety metric and when subjected to a particular threat. Intermediate results include the expected performance of SSCs when subjected to a particular threat and can be defined as the minimum ratio of capacity to demand for SSCs on the success path. [4]
>
> - This term is not defined in the safety standards.

minimal cut set

A smallest set of events sufficient to cause the outcome of a *logic model*. For a fault tree, a minimal cut set is a smallest set of basic events that will cause the top event to occur. [16]

nuclear security culture coordinator

A person who is (or a group of people who are) officially appointed to lead the effort to enhance the *nuclear security culture*. [38]

nuclear security culture enhancement group

A group of representatives from the *nuclear security* stakeholders, as identified by the State or *competent authority*, that sets the strategy to enhance the *nuclear security culture* and provides high level oversight of the strategy's implementation. [38]

nuclear security culture enhancement programme

A systematic set of measures designed to continually enhance *nuclear security*. [38]

nuclear security culture indicator

A *nuclear security culture* characteristic that can be observed or measured and compared against criteria as a means of assessing the strength of the *nuclear security culture*. [38]

physical control measures

Physical barriers that protect instruments, computer-based systems and supporting assets from physical damage and prevent unauthorized physical access. [17]

prevention set

A smallest set of events that will prevent the outcome of a *logic model*. For a fault tree, a prevention set is a smallest set of basic events that should be prevented in order to prevent the top event. [16]

probabilistic safety assessment

A comprehensive, structured approach to identifying failure scenarios, constituting a conceptual and mathematical tool for deriving numerical estimates of risk. [16]

§ This definition is from the IAEA Safety Glossary [46].

safety alarm

Acoustic, visual or vibration signal produced when the radiation level exceeds the *safety alarm threshold value*. [1]

§ This term is not defined in the safety standards.

safety alarm threshold value

Absolute ambient dose equivalent rate (or absolute count rate) equivalent to the maximum permissible values (100 μSv h^{-1}). Exceeding of the safety alarm threshold requires immediate radiation safety measures. [1]

§ This term is not defined in the safety standards.

safety margin

See *margin*.

scenario

A postulated or assumed set of conditions and/or events. Most commonly used in analysis or assessment to represent possible future conditions and/or events to be modelled, such as possible accidents at a nuclear facility. A scenario may represent the conditions at a single point in time or a single event, or a time history of conditions and/or events (including processes). Safety analysts use accident scenarios to describe and model plant response to potential accidents. An accident scenario, which usually has an initiating event superimposed on a proposed plant configuration, can be used to model system response, including various operator actions as appropriate. [4]

threat scenario: A scenario whose initiating event is an act of sabotage. [4]

screening

A type of analysis aimed at eliminating from further consideration factors that are less significant for protection or safety, in order to concentrate on the more significant factors. This is typically achieved by consideration of very pessimistic hypothetical scenarios. Screening is done in various disciplines using a variety of tools:

(a) In threat assessment, screening is used to eliminate certain possible terrorist acts because of, for example, the existence of other State protective strategies, the perceived low capability level of the adversaries, strong protective forces and/or the low probability of the event.

(b) Site and plant screening may exclude certain threat scenarios because of, for example, site location or the inherent robustness of the design. [4]

§ The first part of this definition is from the IAEA Safety Glossary [46].

self-assessment

Referred to simply as 'assessment' in this report, self-assessment is the evaluation process performed by the operating organizations, with the assistance of external agencies and consultants as needed, to identify and correct safety and security problems that hinder the achievement of the organization's safety and security objectives. The end result of self-assessment activities may be risk reduction strategies that include changes and upgrades to the nuclear facility. This is considered to be the first step of a more formal review (e.g. regulatory review) by an external organization. [4]

§ In the safety standards this term has a broadly similar definition: "A routine and continuing process conducted by senior management and also by management at other levels to evaluate the effectiveness of performance in all areas of their responsibility."

sigma multiplier

The net signal count rate above background divided by the square root of the background count rate. [1]

standard gamma ray background

Ambient dose equivalent rate (dH*(10)/dt) of 0.1 μSv h^{-1} ±50% as measured by a legal dose rate meter with a wide energy range of 30 keV–3 MeV. [1, typos corrected]

standard neutron background

Value of the neutron flux outside and at sea level. This is approximately 0.015 n cm^{-2} s^{-1} (±30%). [1]

standard neutron source configuration

A ^{252}Cf source emitting a specified number of neutrons per second surrounded by 1 cm of lead. [1]

success criteria

The minimum system performance that will allow for performance of a system safety function under the specific conditions created by an *initiating event*. [16]

success path

A minimal set of components for a subset of plant systems — including safety systems, support systems, containment structures and operator actions — whose operability and survivability are sufficient to ensure the safe shutdown of a nuclear power plant, removal of residual heat, containment as required and the necessary continued control actions for the threat scenario under consideration. [4]

support system

A system required for the proper functioning of one or more *front line system(s)*. [16]

technical control measures

Hardware and/or software used to prevent, detect, mitigate the consequences of and recover from an intrusion or other *malicious act*. [17]

threat beyond the DBT

A threat identified in the assessment that, while not included in the DBT, remains credible. Threats beyond the DBT need to be taken into account to ensure the physical protection of nuclear facilities. [4]

! This should not be used as a defined term. If it is necessary to describe such threats and/or measures to counter them, the text should explain, rather than referring to a definition.

threat scenario

See *scenario*.

threat type 1 (TT-1)

A threat posed to the nuclear facility by insiders or by adversaries intending to intrude into the facility to commit their act (with or without insider assistance). In general, the PPS of the facility is designed to counter this type of threat. The DBT considers many threats of this type. [4]

threat type 2 (TT-2)

A threat posed to the nuclear facility initiated outside the plant boundary that does not require the presence of the adversaries onsite. Examples of this type of threat include standoff attacks such as shoulder launched missiles and malicious aircraft impacts. It is normally difficult for the facility's PPS to counter this type of attack, as it is not designed for this purpose. For many, but not all, nuclear facilities, a TT-2 is considered to be beyond the DBT. [4]

walkdown

Techniques to enable a team of experienced engineers, operators, security and safety personnel, and technicians to quickly understand plant configuration and procedures based on thorough in-plant inspections and the review of existing documents such as design drawings, operating procedures, safety analysis reports and PSA reports (e.g. level 1, level 2, level 3, fire PSA, seismic PSA, shutdown PSA). [4]

REFERENCES

[1] INTERNATIONAL ATOMIC ENERGY AGENCY, Technical and Functional Specifications for Border Monitoring Equipment, Technical Guidance, IAEA Nuclear Security Series No. 1, IAEA, Vienna (2006) (available on request from the IAEA Secretariat).

[2] INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Forensics in Support of Investigations, Implementing Guide, IAEA Nuclear Security Series No. 2-G (Rev. 1), IAEA, Vienna (2015).

[3] INTERNATIONAL ATOMIC ENERGY AGENCY, UNIVERSAL POSTAL UNION AND WORLD CUSTOMS ORGANIZATION, Monitoring for Radioactive Material in International Mail Transported by Public Postal Operators, Technical Guidance, IAEA Nuclear Security Series No. 3, IAEA, Vienna (2006).

[4] INTERNATIONAL ATOMIC ENERGY AGENCY, Engineering Safety Aspects of the Protection of Nuclear Power Plants against Sabotage, Technical Guidance, IAEA Nuclear Security Series No. 4, IAEA, Vienna (2007).

[5] INTERNATIONAL ATOMIC ENERGY AGENCY, Identification of Radioactive Sources and Devices, Technical Guidance, IAEA Nuclear Security Series No. 5, IAEA, Vienna (2007).

[6] EUROPEAN POLICE OFFICE, INTERNATIONAL ATOMIC ENERGY AGENCY, INTERNATIONAL POLICE ORGANIZATION–INTERPOL AND WORLD CUSTOMS ORGANIZATION, Combating Illicit Trafficking in Nuclear and Other Radioactive Material, Technical Guidance, IAEA Nuclear Security Series No. 6, IAEA, Vienna (2007).

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

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

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

[10] INTERNATIONAL ATOMIC ENERGY AGENCY, National Nuclear Security Threat Assessment, Design Basis Threats and Representative Threat Statements, Implementing Guide, IAEA Nuclear Security Series No. 10 (Rev. 1), IAEA, Vienna (in preparation).

[11] INTERNATIONAL ATOMIC ENERGY AGENCY, Security of Radioactive Material in Use and Storage and of Associated Facilities, Implementing Guide, IAEA Nuclear Security Series No. 11 (Rev. 1), IAEA, Vienna (2019).

[12] INTERNATIONAL ATOMIC ENERGY AGENCY, Model Academic Curriculum on Nuclear Security, Technical Guidance, IAEA Nuclear Security Series No. 12 (Rev. 1), IAEA, Vienna (in preparation).

[13] 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).

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

[15] 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 AND 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).

[16] INTERNATIONAL ATOMIC ENERGY AGENCY, Identification of Vital Areas at Nuclear Facilities, Technical Guidance, IAEA Nuclear Security Series No. 16, IAEA, Vienna (2012).

[17] INTERNATIONAL ATOMIC ENERGY AGENCY, Computer Security Techniques for Nuclear Facilities, Technical Guidance, IAEA Nuclear Security Series No. 17 (Rev. 1), IAEA, Vienna (in preparation).

[18] INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Systems and Measures for Major Public Events, Implementing Guide, IAEA Nuclear Security Series No. 18, IAEA, Vienna (2012).

[19] INTERNATIONAL ATOMIC ENERGY AGENCY, Establishing the Nuclear Security Infrastructure for a Nuclear Power Programme, Implementing Guide, IAEA Nuclear Security Series No. 19, IAEA, Vienna (2013).

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

[21] INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Systems and Measures for the Detection of Nuclear and Other Radioactive Material out of Regulatory Control, Implementing Guide, IAEA Nuclear Security Series No. 21, IAEA, Vienna (2013).

[22] INTERNATIONAL ATOMIC ENERGY AGENCY, INTERNATIONAL CRIMINAL POLICE ORGANIZATION–INTERPOL AND UNITED NATIONS INTERREGIONAL CRIME AND JUSTICE RESEARCH INSTITUTE, Radiological Crime Scene Management, Implementing Guide, IAEA Nuclear Security Series No. 22-G, IAEA, Vienna (2014).

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

[24] INTERNATIONAL ATOMIC ENERGY AGENCY, Risk Informed Approach for Nuclear Security Measures for Nuclear and Other Radioactive Material out of Regulatory Control, Implementing Guide, IAEA Nuclear Security Series No. 24-G, IAEA, Vienna (2015).

[25] INTERNATIONAL ATOMIC ENERGY AGENCY, Use of Nuclear Material Accounting and Control for Nuclear Security Purposes at Facilities, Implementing Guide, IAEA Nuclear Security Series No. 25-G, IAEA, Vienna (2015).

[26] INTERNATIONAL ATOMIC ENERGY AGENCY, Security of Nuclear Material in Transport, Implementing Guide, IAEA Nuclear Security Series No. 26-G, IAEA, Vienna (2016).

[27] INTERNATIONAL ATOMIC ENERGY AGENCY, Physical Protection of Nuclear Material and Nuclear Facilities (Implementation of INFCIRC/225/Revision 5), Implementing Guide, IAEA Nuclear Security Series No. 27-G, IAEA, Vienna (2018).

[28] INTERNATIONAL ATOMIC ENERGY AGENCY, Self-assessment of Nuclear Security Culture in Facilities and Activities, Technical Guidance, IAEA Nuclear Security Series No. 28-T, IAEA, Vienna (2017).

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

[30] INTERNATIONAL ATOMIC ENERGY AGENCY, Sustaining a Nuclear Security Regime, Implementing Guide, IAEA Nuclear Security Series No. 30-G, IAEA, Vienna (2018).

[31] INTERNATIONAL ATOMIC ENERGY AGENCY, Building Capacity for Nuclear Security, Implementing Guide, IAEA Nuclear Security Series No. 31-G, IAEA, Vienna (2018).

[32] INTERNATIONAL ATOMIC ENERGY AGENCY, Establishing a System for Control of Nuclear Material for Nuclear Security Purposes at a Facility during Use, Storage and Movement, Technical Guidance, IAEA Nuclear Security Series No. 32-T, IAEA, Vienna (2019).

[33] INTERNATIONAL ATOMIC ENERGY AGENCY, Computer Security of Instrumentation and Control Systems at Nuclear Facilities, Technical Guidance, IAEA Nuclear Security Series No. 33-T, IAEA, Vienna (2018).

[34] INTERNATIONAL ATOMIC ENERGY AGENCY, Planning and Organizing Nuclear Security Systems and Measures for Nuclear and Other Radioactive Material out of Regulatory Control, Technical Guidance, IAEA Nuclear Security Series No. 34-T, IAEA, Vienna (2019).

[35] INTERNATIONAL ATOMIC ENERGY AGENCY, Security during the Lifetime of a Nuclear Facility, Implementing Guide, IAEA Nuclear Security Series No. 35-G, IAEA, Vienna (2019).

[36] INTERNATIONAL ATOMIC ENERGY AGENCY, Preventive Measures for Nuclear and Other Radioactive Material out of Regulatory Control, Implementing Guide, IAEA Nuclear Security Series No. 36-G, IAEA, Vienna (2019).

[37] INTERNATIONAL ATOMIC ENERGY AGENCY, Developing a National Framework for Managing the Response to Nuclear Security Events, Implementing Guide, IAEA Nuclear Security Series No. 37-G, IAEA, Vienna (2019).

[38] INTERNATIONAL ATOMIC ENERGY AGENCY, Enhancing Nuclear Security Culture In Organizations Associated With Nuclear and Other Radioactive Material, Technical Guidance, IAEA Nuclear Security Series No. 38-T, IAEA, Vienna (in preparation).

[39] INTERNATIONAL ATOMIC ENERGY AGENCY, Developing a Nuclear Security Contingency Plan for Nuclear Facilities, Technical Guidance, IAEA Nuclear Security Series No. 39-T, IAEA, Vienna (2019).

[40] INTERNATIONAL ATOMIC ENERGY AGENCY, Handbook on the Design of Physical Protection Systems for Nuclear Material and Nuclear Facilities, Technical Guidance, IAEA Nuclear Security Series No. 40-T, IAEA, Vienna (in preparation).

[41] INTERNATIONAL ATOMIC ENERGY AGENCY, Preparation, Conduct and Evaluation of Exercises for Detection of and Response to Acts Involving Nuclear and Other Radioactive Material out of Regulatory Control, Technical Guidance, IAEA Nuclear Security Series No. 41-T, IAEA, Vienna (in preparation).

[42] INTERNATIONAL ATOMIC ENERGY AGENCY, Computer Security for Nuclear Security, Implementing Guide, IAEA Nuclear Security Series No. 42-G, IAEA, Vienna (in preparation).

[43] INTERNATIONAL ATOMIC ENERGY AGENCY, Security Management and Security Plans for Radioactive Material and Associated Facilities, Technical Guidance, IAEA Nuclear Security Series No. 43-T, IAEA, Vienna (in preparation).

[44] INTERNATIONAL ATOMIC ENERGY AGENCY, Detection at State Borders of Nuclear and other Radioactive Material out of Regulatory Control, Technical Guidance, IAEA Nuclear Security Series No. 44-T, IAEA, Vienna (in preparation).

[45] The Convention on the Physical Protection of Nuclear Material, INFCIRC/274/Rev. 1, IAEA, Vienna (1980).

[46] INTERNATIONAL ATOMIC ENERGY AGENCY, IAEA Safety Glossary: Terminology Used in Nuclear Safety and Radiation Protection, 2018 Edition, IAEA, Vienna (2019).

[47] INTERNATIONAL ATOMIC ENERGY AGENCY, IAEA Safeguards Glossary: 2001 Edition, International Nuclear Verification Series No. 3, IAEA, Vienna (2002).

[48] Amendment to the Convention on the Physical Protection of Nuclear Material, in GOV/INF/2005/10-GC(49)/INF/6, IAEA, Vienna (2005).

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

[50] INTERNATIONAL ATOMIC ENERGY AGENCY, Regulations for the Safe Transport of Radioactive Material, 2018 Edition, IAEA Safety Standards Series No. SSR-6 (Rev. 1), IAEA, Vienna (2018).

[51] UNITED NATIONS OFFICE ON DRUGS AND CRIME, Crime Scene and Physical Evidence Awareness for Non-forensic Personnel, ST/NAR/39, UNODC, New York (2009).

[52] FOOD AND AGRICULTURE ORGANIZATION OF THE UNITED NATIONS, INTERNATIONAL ATOMIC ENERGY AGENCY, INTERNATIONAL CIVIL AVIATION ORGANIZATION, INTERNATIONAL LABOUR ORGANIZATION, INTERNATIONAL MARITIME ORGANIZATION, INTERPOL, OECD NUCLEAR ENERGY AGENCY, PAN AMERICAN HEALTH ORGANIZATION, PREPARATORY COMMISSION FOR THE COMPREHENSIVE NUCLEAR-TEST-BAN TREATY ORGANIZATION, UNITED NATIONS ENVIRONMENT PROGRAMME, UNITED NATIONS OFFICE FOR THE CO¬ORDINATION OF HUMANITARIAN AFFAIRS, WORLD HEALTH ORGANIZATION, WORLD METEOROLOGICAL ORGANIZATION, Preparedness and Response for a Nuclear or Radiological Emergency, IAEA Safety Standards Series No. GSR Part 7, IAEA, Vienna (2015).

[53] INTERNATIONAL ATOMIC ENERGY AGENCY, IAEA Incident and Trafficking Database (ITDB): Incidents of nuclear and other radioactive material out of regulatory control, 2015 Fact Sheet.

[54] EUROPEAN COMMISSION, FOOD AND AGRICULTURE ORGANIZATION OF THE UNITED NATIONS, INTERNATIONAL ATOMIC ENERGY AGENCY, INTERNATIONAL LABOUR ORGANIZATION, OECD NUCLEAR ENERGY AGENCY, PAN AMERICAN HEALTH ORGANIZATION, UNITED NATIONS ENVIRONMENT PROGRAMME, WORLD HEALTH ORGANIZATION, Radiation Protection and Safety of Radiation Sources: International Basic Safety Standards, IAEA Safety Standards Series No. GSR Part 3, IAEA, Vienna (2014).

[55] Code of Conduct on the Safety and Security of Radioactive Sources, IAEA/CODEOC/2004, IAEA, Vienna (2004).

[56] Statute of the International Atomic Energy Agency (As Amended), IAEA, Vienna (1989).

ANNEX
EXPLANATIONS OF TERMS NOT EXPLICITLY DEFINED

The explanations in this Annex are intended to help readers of the IAEA Nuclear Security Series to understand the text of the publications by indicating the meaning of terms that are used but not defined (particularly where this is a specialized meaning) and the similarities and differences between terms that may be used together or in related contexts. In some cases, the usage of the terms is explained by means of illustrative text rather than an explicit, discrete explanation. Particular attention is given to terms that might be confused with each other and usages that might not be expected from an understanding of everyday English. The entries in this Annex are not formal definitions and are not intended to define the terms precisely.

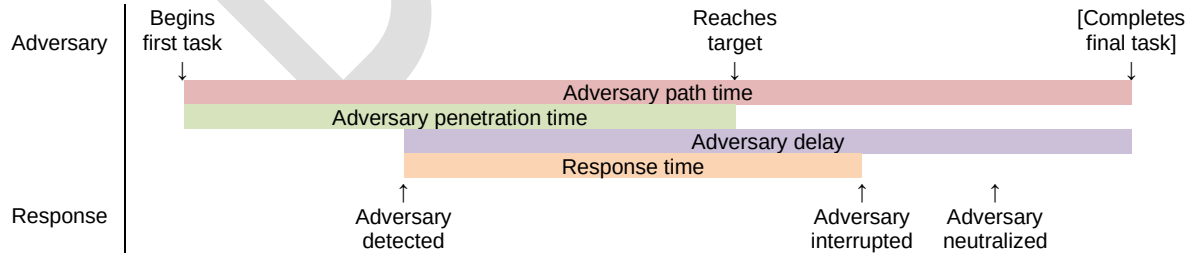
The explanations currently included are based primarily on consideration of terms appearing in the Nuclear Security Fundamentals and Recommendations [A-1–A-4].

adversary related terms:

adversary delay, adversary interruption, adversary neutralization, adversary path, adversary path time, adversary penetration time, adversary sequence diagram, adversary task

In order to commit a malicious act, an adversary will typically need to successfully complete a sequence of steps (sometimes called *adversary tasks*) to gain the access necessary to carry out the malicious act, to carry out the act itself (including, in the case of unauthorized removal of material, successfully getting the material out of the facility). The sequence of steps to carry out a specific malicious act in a specific way is sometimes called an *adversary path*, and the different adversary paths for different possible malicious acts at a particular facility or directed at a particular target, and/or different ways of committing them, can be presented schematically in an *adversary sequence diagram*. Each of the adversary tasks will take time — for example to move from one place to another, or to overcome or bypass a barrier or other nuclear security measure, or to carry out the malicious act itself. The total time assumed to be necessary for an adversary to reach the target of a specific adversary path is called the *adversary penetration time* for that path, and the total time to complete the whole adversary path is the *adversary path time*.

Response forces will aim to interrupt (*adversary interruption*) or stop (*adversary neutralization*) the adversary's progress within the adversary path time, i.e. before completion of the malicious act, and preferably during the adversary penetration time, i.e. before the adversary reaches the target. However, they can only start to respond after the adversary has been detected, and therefore nuclear security measures are designed to detect adversaries as early as possible in the adversary penetration time, and to maximize the *adversary delay*, which is the remaining adversary penetration time after detection.



alarms and alerts:

alarm assessment, false alarm, information alert, innocent alarm, instrument alarm, nuisance alarm

The first indication of a possible nuclear security event will be an alarm or an alert. An alarm is usually an *instrument alarm*, generated when some type of equipment senses something that meets predefined criteria (e.g. a radiation monitor recording a dose rate exceeding a predefined value, indicating the

possible presence of radioactive material). An *information alert* is generated by a person or organization based on observation of or intelligence about something that could indicate intentions or preparations for a malicious act.

Alarm assessment is the process of determining whether the alarm was a *nuisance alarm* (a false alarm or an innocent alarm), in which case there is no nuclear security event and no response is initiated, or indicates a nuclear security event requiring response. An alarm that should not have been generated (e.g. one caused by an equipment fault, or human error such as incorrect calibration) is a *false alarm*. If the alarm was correctly generated, but the cause is subsequently determined not to be of nuclear security concern (e.g. a worker inadvertently activating a perimeter intruder detection system when performing maintenance, or an alarm indicating the presence of radioactive material that is subsequently found to be under regulatory control or of no security concern), then it is an *innocent alarm*.

Similarly, an information alert needs to be assessed to determine whether the information is correct and whether it indicates a credible possibility that a malicious act is being planned or attempted or has been carried out. If the information is not correct, then it may be considered a false alert, or if it is correct but found not to be of concern, then it may be considered an innocent alert: in either case, there is no nuclear security event and no response.

assessment, evaluation

Although it is not explicitly stated and not applied universally, the terms assessment and evaluation appear often to be used differently. Assessment is typically used to describe processes supporting the design and implementation of nuclear security measures, such as threat and consequence assessment as a basis for designing physical protection measures and assessment of alarms and alerts as a basis for initiating (or not) response measures. Evaluation is typically used to describe processes for measuring or checking the performance or effectiveness of the designed measures.

attractiveness (of material)

Materials and other potential targets are sometimes described in nuclear security contexts as more or less *attractive*. This refers to their potential *attractiveness* to an adversary as targets for *unauthorized removal* or *sabotage*, or as tools for *criminal or intentional unauthorized acts* involving material *out of regulatory control*. The attractiveness of a target to an adversary is assumed to relate to its inherent potential to cause harm, i.e. the potential to cause severe and/or widespread consequences (or fear of consequences). It therefore typically depends upon:

- The types (nuclear or other radioactive) and amounts of material present; and/or
- The type of facility or activity (e.g. sabotage of an operating nuclear facility may have more severe consequences than sabotage of such a facility after it is shut down).

In the case of material, attractiveness may also relate to the ease or difficulty with which it could be handled or used for malicious purposes. For example, conditioned radioactive waste may be in very large packages that are difficult to move and in a physical form that is very difficult to disperse.

Attractiveness of material is always relative, compared to other possible targets, but the term "relative attractiveness" is sometimes used to emphasize this.

Attractiveness does not, however, depend on the extent to which the target is protected by nuclear security measures, which is described in terms of *vulnerability*. Nuclear security should aim to make more attractive targets less vulnerable.

attributes, characteristics

A design basis threat (or other threat statement) describes the "attributes and characteristics" of potential adversaries, but the distinction between attributes and characteristics is not explicitly stated (and is not obvious from the normal English meaning of the two words). In this formulation, "attributes" appear to be broader or higher level characteristics of a potential adversary — such as motivations, intentions and capabilities — whereas "characteristics" are more specific details, such as skills, tactics and tools.

availability, accessibility (of material)

These terms are both used in relation to the vulnerability of radioactive material to unauthorized removal. Although the distinction may not be strict, "accessibility" refers to how easily an adversary could reach the material, whereas "availability" refers to how easily an adversary could remove and subsequently move the material. Therefore, for example, a radioactive source in a carrying case, in a locked safe in a secure room with video surveillance may be relatively inaccessible but relatively available if accessed, whereas a large, heavy canister of cemented radioactive waste in a warehouse with only a padlock on the door may be relatively accessible but much less available.

capability, capacity, competence

These terms are used to describe the extent to which an individual, an organization or a State can meet its nuclear security responsibilities. Although specialized publications addressing topics such as human resource development may attach specific meanings to these terms, in general the distinction between the two is as follows. Capability typically refers to an individual, organization or State having the knowledge, skills and resources (including financial and human resources, and any necessary tools) to meet a particular responsibility, whereas capacity refers more broadly to the overall collective ability, for example of a State, to meet its full range of responsibilities.

conditions (of authorization)

There may occasionally be potential confusion between conditions of an authorization – meaning any provision specified in the authorization with which the authorization holder must comply, and hence on which the authorization is conditional – and conditions in the sense of an environment or a state, such as operating conditions, or the conditions (e.g. temperature, protection from fire or radiation, security) in which material or equipment must be stored.

constraints, limitations (of detection instruments)

There appears not to be a fully established distinction between these two terms in this context, and there may be cases in which they are used interchangeably. However, where both are used in a way that implies that they are distinct, constraints typically relate to constraints on the conditions under which the instrument can be used (e.g. how wet or how dusty an environment it will work in, maximum or minimum operating temperature), whereas limitations typically relate to limitations on the performance of the instrument (e.g. its sensitivity, whether it provides continuous measurement or discrete measurements with 'dead time').

current threat

In principle this term could describe the threat at any given time. However, it is typically used when the threat is considered to have changed but the national threat assessment or design basis threat (or the physical protection system designed to address it) has not yet been updated, and compensatory measures may be needed to address the *current threat* where it exceeds or differs in nature from the threat against which the system was designed.

cyber-attack, cyber-threat, cyber-security

Although the term *computer security* is used in the IAEA Nuclear Security Series rather than other commonly used terms such as cyber-security and IT security (which are considered to be synonymous with *computer security*), the specific term *cyber-attack* is used to refer to malicious acts involving computer systems. Such acts may include: information gathering attacks aimed at planning and executing further malicious acts; attacks disabling or compromising the attributes of one or several computers crucial to facility security or safety; or compromise of one or several computers combined with other concurrent modes of attack, such as physical intrusion to target locations [A-5].

The term *cyber-threat* may also be used in a general descriptive sense to refer to the potential for such attacks, but is not clearly defined (e.g. it is not defined as a type of *nuclear security threat*), and therefore more precisely defined terms should be used in specific guidance.

declared content

The amount and nature of radioactive material stated by a consignor or shipper in relevant formal documentation to be in a package or shipment.

delay

In general, delay is a function of a physical protection system or other nuclear security measures, occurring between *detection* and reaching the target. It may be loosely used to refer to any measure that impedes or slows the progress of an adversary, but more specifically refers to those measures that adversaries are expected to encounter after their presence has been detected, as it is this delay that allows time for response forces to take action to intercept the adversary. The specific term *adversary delay* is used to refer to a more precisely defined measure of delay.

deterrence

Deterrence implies discouraging a potential adversary, by inspiring fear, from following a particular course of action. This may be fear of the consequences, particularly those for the adversary, of attempting the course of action, or fear of failure, i.e. attempting the course of action but being unsuccessful in achieving its objective. Potential consequences that might have a deterrent effect include the possibility of injury to the adversary while attempting the course of action (e.g. that resulting from high doses of radiation from handling radioactive material, or from action by response forces against the adversary), or the possibility of prosecution and punishment afterwards (sometimes referred to as "deterrence by punishment"). Fear of the possibility of failure may be achieved (sometimes referred to as "deterrence by denial") by creating a perception (in potential adversaries) that multiple effective security measures are in place and would be difficult to defeat or bypass. This perception may be created through the actual success or reputation of effective security measures, through providing particularly visible security measures, and/or by deception.

As the likelihoods of these three possibilities increase, it may generally be expected that the likelihood of an adversary attempting a malicious act will decrease. However, not all potential adversaries will be deterred by all of these possibilities: indeed some adversaries may be encouraged by measures intended to deter.

drill, exercise

These are both ways of testing arrangements for response. A drill is a test of a specific response action, whereas an exercise is a test of a coordinated or integrated set of such actions, including the coordination between those actions.

entry point, access point, point of potential access, point of entry,

These terms may be indistinguishable in many languages, and conceptually they have the same meaning. However, in English texts the terms *entry point*, *access point* and *point of potential access* are used to refer to a place at which entry is possible into an area with a higher security classification, for example into a limited access area or a radiological crime scene, whereas "point of entry" is used (usually as part of the term "point of exit or entry") to refer to a place at which entry is possible into a State (such as a border crossing).

escort

Used to refer to somebody who accompanies somebody who needs to be accompanied. The latter may need to accompanied for their own protection (in which case the escort will be a *guard*), or because they are not allowed unaccompanied access to a particular area (in which case the escort may be a *guard*), or because the two-person rule is being applied (in which case the escort is probably not a *guard*).

framework, regime, infrastructure, architecture, systems and measures

IAEA terminology refers to a *global nuclear security framework*, which comprises:

- An *international legal framework* of binding (e.g. Conventions, UN Security Council Resolutions) and non-binding (e.g. Codes of Conduct, IAEA guidance) instruments;
- A framework of *international cooperation and assistance*, with the IAEA playing a central role but including other international organizations and initiatives, non-governmental organizations and bilateral, multilateral and regional agreements and arrangements; and
- *National nuclear security regimes*.

A *national nuclear security regime* reflects the *national nuclear security strategy*, and also interfaces with (and may make use of) elements of the *national security regime*. It is defined in Ref. [A-1] as comprising:

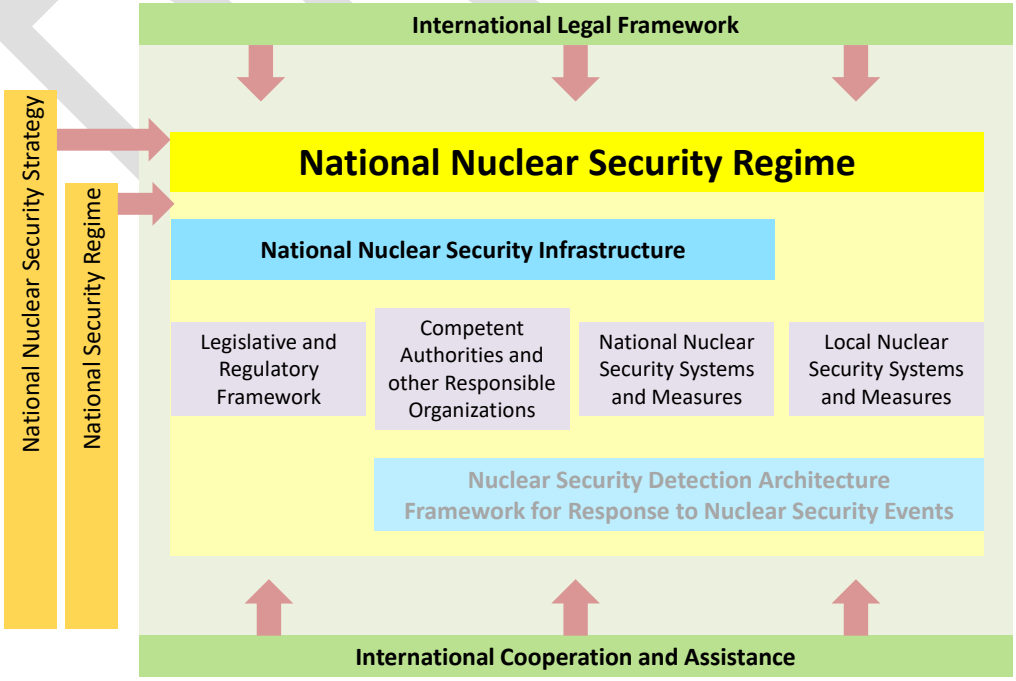
- The *legislative and regulatory framework* and administrative systems and measures governing the nuclear security of *nuclear material*, *other radioactive material*, *associated facilities* and *associated activities*;
- The institutions and organizations within the State responsible for ensuring the implementation of the legislative and regulatory framework and administrative systems of nuclear security (referred to in the figure below as *competent authorities and other responsible organizations*);
- *Nuclear security systems* and *nuclear security measures* for the prevention of, detection of and response to *nuclear security events*.

The systems and measures described in the last bullet include *national systems and measures*, designed and implemented by the State, and *local systems and measures* at the level of facilities and activities, designed and operated by the operator.

Reference [A-6] refers to a *national nuclear security infrastructure*, which is defined to include the first and second bullets and *national systems and measures*.

Reference [A-7] refers to a *nuclear security detection architecture*, which, in the specific context of detection of nuclear security events, includes the second and third bullets and is based on the first bullet. Reference is also sometimes made to *nuclear security response architecture*, a corresponding concept for response, but the Implementing Guide in this area describes a "framework" for managing response to nuclear security events.

These concepts and their interrelationship are summarized in the figure below.



hoax, scam

Both terms are used to describe cases involving intentional deception, typically in the context of nuclear security the pretended presence of nuclear material or other radioactive material or of a malicious act involving or directed at such material (or associated facilities or activities).

- A hoax is usually understood to be an intentionally false claim or pretended action intended to provoke unwarranted fear or other reaction, as a practical joke[6] or as a tactic to gain an advantage. For example, a false claim that an RDD has been left in an airport, timed to detonate, might simply be a joke to amuse the hoaxer, or a trick to cause disruption and possible loss to the airport operator or airlines due to an unnecessary evacuation, or a tactic to divert attention and response resources away from a malicious act being committed elsewhere.
- A scam is usually understood to be an actual or intended transaction in which one party intentionally deceives the other to gain an advantage. For example, sale of material claimed to be, but not in fact, nuclear material may be intended simply for financial advantage; however, the advantage sought might be to test the effectiveness of security arrangements.

In a nuclear security context, hoaxes and scams have in common the characteristic that the directly threatened consequences do not in fact materialize. However, as indicated by the examples, they might nevertheless be of nuclear security concern, and might need to be considered as malicious acts or nuclear security events.

interdiction

This is sometimes used as a generic term referring to a range of response actions that may be used in the course of stopping an adversary from completing a malicious act. It may include actions such as intercepting an adversary en route to a target, interrupting an adversary engaged in sabotaging a target or removing material, disarming or disabling an adversary, rendering a device safe or preventing material or equipment from being moved. Actions taken at the end of the response, such as apprehending an adversary, or seizing material or equipment, are usually considered not to be part of interdiction but rather to follow it.

intrusion

Often used to describe a step in an adversary's attempt to reach a target to commit a malicious act, namely attempting unauthorized entry into an area with a higher security classification. An intrusion is often assumed to be physical, but the term may also be used figuratively to refer to an attempt to gain access to sensitive information or a sensitive computer-based system during a cyber-attack.

§ The term "human intrusion" is used in waste safety to refer specifically to actions that humans might take in the future that could directly disrupt or adversely affect the performance of a waste disposal facility. In such cases, unless otherwise specified, "human intrusion" is assumed to be "inadvertent" in the sense that it is an intentional action, but one taken without knowledge or understanding of the presence of radioactive waste.

inventory, accounting (of radioactive material)

An inventory is a current list of all radioactive material, its basic characteristics (including radionuclide(s) and activity) and its authorized location. Typically an inventory would include all of the radioactive material in a particular facility or that a particular operator is authorized to possess. Accounting for radioactive material is a more active process of verifying, at prescribed intervals, that all material in the inventory is where it should be (its authorized location).

[6] Such a joke, if intended to disturb (rather than amuse) the person or people against whom it is directed, may be described as "malicious", but this is not necessarily the meaning of "malicious" implied by the term "malicious act".

! "Inventory" is sometimes used as a verb to describe the process of compiling or updating an inventory. This is acceptable in everyday English usage, but may be confusing in normative publications, so the more explicit term "inventory taking" is preferred to describe this process.

irregularity abnormality, anomaly discrepancy

Various terms are used to describe things that may be observed to be unusual, and that could be indications that a malicious act is being planned or attempted (or might be entirely innocent occurrences), but have not been investigated sufficiently to determine whether they are. Terms such as *irregularity*, *abnormality* and *anomaly* may be used to describe such observations that have not (yet) been determined to be of any nuclear security concern. The term irregularity is used specifically in relation to nuclear material accounting and control, but could be used in other contexts, provided that the essential meaning is the same.

The word "discrepancy" is used in safeguards when it has been confirmed that some material is unaccounted for. Since its precise meaning is connected with quantities of material that are of interest for safeguards purposes, the term should be avoided in nuclear security contexts.

lost, missing, stolen, unaccounted for (of material)

In the course of inventory taking, or other forms of material accounting, an *irregularity* (i.e. something that is not correct) may be observed. If further investigation indicates that the irregularity is not the result of a mistake in accounting or some normal random variation, it may be designated as *material unaccounted for,* indicating that material has been confirmed not to be where it should be (or to be where it should not be). After further investigation, it may be considered to be:

- *missing*, if there is considered to be some likelihood that it may be found, especially if it is suspected that it may not have left the facility or site;
- *lost*, if it is not expected to be found in the facility or on-site, but there is no evidence of an adversary having removed it;
- *stolen*, if there is credible evidence that it has been removed by or is in the possession of an adversary (even if such evidence might not be sufficient to prove theft).

Similar terminology of "lost, missing or stolen" is used more generally in relation to the security of nuclear and other radioactive material, with essentially the same meanings.

manipulation, falsification

These terms are used to refer to potential misuse of electronic data or other information for malicious purposes. While there is substantial overlap between the meanings of the terms, manipulation is potentially broader in scope: falsification necessarily implies adding, removing or modifying data or other information to make it incorrect or misleading (e.g. deleting records of nuclear material to conceal its unauthorized removal); manipulation could include this, but could also include changing the use or context of data or other information to achieve different effects from those intended (e.g. changing the software controlling a drone to make it attack the facility it is intended to defend).

mitigate, minimize (radiological consequences of sabotage)

Both terms are used in the objectives of a State's physical protection regime in Ref. [A-2], reflecting the wording of the obligations set out in the CPPNM Amendment [A-8]. The two words are not explained, but both imply reducing the potential or actual consequences of an act of sabotage. It may reasonably be assumed that one refers to measures applied to the material or facility in advance that will reduce the consequences if sabotage occurs, such as reducing the amount of material in one place, making it very difficult to disperse or strengthening containment, and that the other refers to measures to be taken after sabotage has occurred to reduce the consequences (which are planned in advance but only implemented after sabotage). However, it is not entirely clear which term is intended to convey which meaning: normal English usage would suggest that the former is minimization and the latter mitigation, but this may not always be the understanding in this context.

mobile, portable (radioactive sources)

These terms are both used to describe sources that can be used in the field, i.e. they can readily be moved to different locations as necessary. No fundamental distinction between the terms is applied with any consistency, but "portable" suggests that moving the source may be a little easier than "mobile". The term "portable" more specifically suggests something that a person can carry (e.g. an industrial radiography source used in the field). The term "mobile" might be more suggestive of something that can be transported by a vehicle, but it could also mean something very similar to "portable".

mobile, relocatable, fixed (of detection equipment)

Both "mobile" and "relocatable" are used to refer to equipment that can be moved from place to place as needed. The terms are not precisely defined, but the distinction is broadly as follows. Mobile equipment is intended to be used in temporary locations and moved frequently, and is therefore largely self-contained (often supported by its means of transport; for example, mounted in a vehicle) and easy to set up and calibrate. Relocatable equipment is equipment installed in semi-permanent locations and is intended to be moved only occasionally. Fixed equipment is equipment installed in a permanent location, from which it is not intended to be moved (although it would, of course, be possible to move it).

national response plan

The Recommendations for material out of regulatory control [A-4] specifically recommend the development, maintenance, exercising and implementation (when needed) of a national plan for response to nuclear security events. In these Recommendations, this *national response plan* relates to material out of regulatory control, and therefore by implication is a plan for the State's response (since in this case there is no operator). In the context of regulated facilities and activities, there is also a need for a plan for the State's response to a nuclear security event (which may also be the *national response plan*), but in this case this should be coordinated or integrated with the operator's *contingency plan* for nuclear security events. In general terms, the contingency plan may be expected to focus on on-site response actions and the national response plan on the off-site response, but the extent to which this distinction applies will depend on the arrangements in the State, e.g. some States may use 'off-site' responses forces also for all response on-site.

In all cases, the national response plan for nuclear security events needs to be coordinated or integrated, as appropriate, with other national plans for emergencies, including particularly emergency plans for response to a nuclear or radiological emergency.

A national response plan describes the practical implementation of national systems and measures within the national framework for managing the response to nuclear security events referred to in the entry for "framework, regime, infrastructure, architecture, systems and measures" above.

objective, goal

There is no generally accepted order of hierarchy between these terms, i.e. some people consider that a broad objective might be pursued via a number of narrower goals, others may think of a goal as something higher or broader than on objective. However, the IAEA convention is that objectives are higher level and/or broader than goals, e.g. objectives may be strategic and pursued through tactical goals.

personnel security, physical security

These terms are sometimes used to describe different groups of nuclear security measures of different types, but both are confusing terms and should be avoided where possible:

- The term "personnel security measures" is used to describe nuclear security measures relating to the control of personnel, such as recruitment and deployment policies, trustworthiness checks and monitoring of personnel behaviour. However, the term itself may be confused with measures for the security of personnel, such as body armour or armoured vehicles: these may

be referred to as "personal security", but the difference in terms may not be very clear, particularly to non-native English speakers.

- The term "physical security measures" is used to describe conventional physical measures to restrict access or actions (sometimes referred to as "gates, guards and guns"). However, there is an obvious potential for confusion with "physical protection measures".

§ In addition, some languages already use an adjective meaning "physical" to distinguish between safety and security, so adding another "physical" is likely to be confusing.

procedures, protocols

These terms are sometimes used together in describing administrative measures for nuclear security or for managing other nuclear security measures. Although the distinction is not precisely defined, a procedure is typically broader in scope: a procedure is a set of instructions for carrying out certain types of work or performing certain tasks, whereas a protocol is typically a more specific and detailed set of 'rules' or instructions for using a specific technique.

recommended requirements

The IAEA Nuclear Security Series specifies no "requirements". Requirements for nuclear security may be specified by a State or a competent authority (especially a regulatory body), in legislation or in regulations. An operator must meet those requirements where relevant, and particularly when they are specified or referred to in their authorizations, and in doing so may specify, through contractual conditions, "requirements" to be met by staff, vendors, contractors or suppliers. Some legal and regulatory requirements may also apply directly to staff, vendors, contractors or suppliers.

Ref. [A-2] explicitly specifies "recommended requirements", meaning that the IAEA recommends that States or their competent authorities impose these requirements on operators, and on others as appropriate (for States Parties to the CPPNM and its Amendment [A-8, A-9], they may also be required of the State as part of its Convention obligations). The other Nuclear Security Recommendations publications [A-3, A-4] explicitly specify "recommendations". In some cases these recommendations may be less specific and explicit than the recommended recommendations in Ref. [A-2], but they have essentially the same status of IAEA recommendations on the requirements that States or their competent authorities should impose within their jurisdiction.

recovery, seizure (of material)

Both terms may be used to describe taking into authorized possession (by a competent authority or other authorized person) nuclear or other radioactive material that was out of regulatory control.

- The term recovery is usually used in cases where the material is discovered of unknown origin or after being lost or abandoned (occasionally referred to as "discovered material"), and is taken into authorized possession primarily in order simply to secure it and bring it under regulatory control. The material is then referred to as "recovered material".

- The term seizure is usually used in cases where the material is taken from a person who has it in their unauthorized possession, or is removed when being used in an unauthorized way (e.g. in a malicious act). In such cases, the material is taken into authorized possession in order to secure it and bring it under regulatory control, but may also subsequently be treated as evidence related to a malicious act. The material is then referred to as "seized material". The terms "interdicted material" (when the adversary's control over the material is interrupted or constrained) and "detained material" (when an adversary has lost physical control of the material and the State is determining its nature and the necessity of measures to secure it) are sometimes used to refer to temporary steps that may be involved in taking control of the material.

security management

Ref. [A-3] indicates that this term specifically refers to measures taken by an operator to address: access control; trustworthiness; information protection (meaning information security); security plan; training and qualification; (material) accounting; inventory; and nuclear security event reporting.

State authorities, legitimate national authority

The term "State authority" is sometimes used to describe organizations that have assigned responsibilities of some relevance to nuclear security but that are not considered to meet the definition of a competent authority, for example because their responsibilities are much broader and nuclear security is just one area in which they are applied. (Ref. [A-3] uses "legitimate national authority" for a similar purpose.) For example, a national security agency might be considered a State authority, and have responsibilities relevant to nuclear security (e.g. advising on the development of design basis threats), but another organization with more direct responsibility specifically for nuclear security might be considered to be the competent authority.

tamper proof, tamper resistant, tamper indicating

The verb "tamper" is used in relation to material accounting to describe actions in which an adversary attempts to obtain or facilitate unauthorized access to the place (e.g. the building, room or container) in which nuclear material or other radioactive material is stored, with the presumed ultimate aim of unauthorized removal. In such cases, seals or other devices are used on points of access (e.g. doors) or containers themselves to indicate whether an unauthorized person has opened or attempted to open them. Such devices may also be not intended to help prevent access, but they are at least intended to indicate whether access has been obtained or attempted, or whether the device itself has been tampered with to conceal such an action or to otherwise mislead (e.g. by switching devices between containers). A *tamper indicating* device (TID) is, as the name suggests, intended primarily to indicate any tampering, not directly to prevent it. The term *tamper resistant* (or possibly *tamper proof*, which indicates a degree of confidence that is unlikely to be warranted) implies that part of such a device's purpose is intended to be preventive (although such a device would also be expected to be tamper indicating).

theft, robbery, unlawful taking

In some jurisdictions, the term *theft* necessarily implies an intent that might not always be present in cases that would be of nuclear security concern. Similarly the definition of *robbery* might not be applicable. The term unlawful taking is used as a more general term in the CPPNM Amendment [A-8] to ensure that all acts of this nature that could be of nuclear security are included: the term *unauthorized removal* is used for the same purpose in the Nuclear Security Series.

> ***protracted theft***: Unauthorized removal of nuclear material in a series of small quantities removed over a period of time. This may be a way of avoiding detection; if the amount removed each time is small enough to be easily concealed and/or too small for its loss to be noticed promptly, a more significant quantity may be acquired by accumulating a number of such small amounts. In principle, this could be done with any material, but is only likely to be worthwhile for nuclear material.

threshold, threshold level

Used in a number of contexts to indicate a level of some measurable (or otherwise assessable) quantity such that, if that level is exceeded, something happens.

- The threshold level for a detection instrument is a level of the measured quantity (for example, of dose rate) that, if exceeded, triggers the instrument to generate an alarm. Such a threshold level is set by the user of the instrument at the lowest level that might indicate some form of malicious act.
- The activity levels by which radioactive sources and nuclear material are categorized as Category 1–5 sources or Category I–III material are sometimes referred to as thresholds.

- The threshold levels for unacceptable radiological consequences (URC) and high radiological consequences (HRC) are levels of potential radiological impact from hypothetical acts of sabotage such that requirements for nuclear security measures against acts leading to consequences above the threshold level are significantly more stringent than for those below. For acts that could cause impacts greater than URC, specific nuclear security measures need to be designed and implemented to protect the targets of those acts; for acts that could cause impacts greater than HRC, the relevant targets need to be designated as vital areas and protected accordingly. The threshold levels are typically set by the State on the basis of judgements about the acceptability of risk, and are usually expressed in terms of a relatively simple indicator of radiological impact, such as the potential dose to an individual at the site fence.

transport related terms:

cargo, carriage, carrier, consignee, consignment, consignor, conveyance, package, packaging, receiver, receiving State, shipment, shipper, shipping State, transit site, transit State

Radioactive material for transport is placed by (or on behalf of) the *consignor* in *packaging* to create a *package*. The package, or the set of packages to be transported together, make up a *consignment*. The consignor employs a *carrier* to make a *shipment*, that is for *carriage* of the consignment as *cargo*, on the carrier's *conveyance*[7], to a *consignee*. If the shipment is not continuous, it may stop temporarily (e.g. overnight) at a *transit site*.

The CPPNM [A-9] addresses the international transport of nuclear material, and uses the terms *shipper* and *receiver*, the terms used in safeguards for consignor and consignee. IAEA Nuclear Security Series publications therefore often use the term shipper and receiver, especially with reference to the transport of nuclear material. For international transport, the terms *shipping State*, *transit State* and *receiving State* are used, corresponding to the shipper, transit site and receiver.

Consignment and shipment are therefore not synonyms. However, consignor and shipper are synonymous, as are consignee and receiver.

In all of the above, the term "transport" is used only when the shipment passes through the public domain; the movement of radioactive material entirely within a licensed site is not considered to be "transport", and no consignor/shipper or consignee receiver is involved in such cases. However, in the specific case of the transfer of nuclear material between material balance areas (MBAs) on the same site, the safeguards terms "shipping MBA" and "receiving MBA" are used.

trustworthiness, integrity, reliability

In nuclear security, trustworthiness has essentially its dictionary meaning. However, the specific context implies that the concern is whether a person might, by act or omission, commit, facilitate or otherwise assist in the commission of a *malicious act*. The concern relates to acts or omissions that the person might commit intentionally, but "intentionally" may include acts or omissions committed with or without a significant degree of understanding of an ultimate purpose and potential consequences. This could include:

- Knowing participation in a malicious act by or on behalf of a directly motivated adversary;
- Participation in or facilitation of, with or without full understanding, a malicious act in return for a personal benefit (e.g. payment);
- Participation in or facilitation of, with or without full understanding, a malicious act under duress (e.g. blackmail or other threat).

Trustworthiness checks for people with nuclear security responsibilities might therefore need to consider factors that could contribute towards any of the above. Trustworthiness includes an

[7] A conveyance is a vehicle (for transport by land) or a vessel (by water) or an aircraft (by air).

individual's integrity — and "integrity" is occasionally used as an approximate synonym for trustworthiness — but this excludes consideration of another aspect of trustworthiness, namely the likelihood and likely strength of an individual's exposure to temptation or coercion (their ability to withstand such temptation or coercion would partly, but not entirely, reflect their integrity).

Errors and other inadvertent acts or omissions are normally considered to be primarily safety concerns. However, trustworthiness checks may also need to give some consideration to characteristics of an individual's behaviour that might increase their likelihood of unintentional acts or omissions that could facilitate malicious acts by others, such as unwitting facilitation of cyber-attack by victims of 'social engineering'. An individual's likely ability to avoid such acts or omissions (e.g. through strict adherence to procedures, or high levels of alertness) is sometimes referred to as "reliability". However, care should be taken to avoid any confusion with the use of "reliability" in safety to refer to a characteristic of a system.

REFERENCES FOR ANNEX

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

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

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

[A-4] INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Recommendations on Nuclear and Other Radioactive Material out of Regulatory Control, IAEA Nuclear Security Series No. 15, IAEA, Vienna (2011).

[A-5] INTERNATIONAL ATOMIC ENERGY AGENCY, Computer Security Techniques for Nuclear Facilities, Technical Guidance, IAEA Nuclear Security Series No. 17 (Rev. 1), IAEA, Vienna (in preparation).

[A-6] INTERNATIONAL ATOMIC ENERGY AGENCY, Establishing the Nuclear Security Infrastructure for a Nuclear Power Programme, Implementing Guide, IAEA Nuclear Security Series No. 19, IAEA, Vienna (2013).

[A-7] INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Systems and Measures for the Detection of Nuclear and Other Radioactive Material out of Regulatory Control, Implementing Guide, IAEA Nuclear Security Series No. 21, IAEA, Vienna (2013).

[A-8] Amendment to the Convention on the Physical Protection of Nuclear Material, in GOV/INF/2005/10-GC(49)/INF/6, IAEA, Vienna (2005).

[A-9] The Convention on the Physical Protection of Nuclear Material, INFCIRC/274/Rev. 1, IAEA, Vienna (1980).