

**INTERNATIONAL ATOMIC ENERGY AGENCY**

DIVISION OF NUCLEAR SECURITY

**Nuclear Security Series Glossary  
Version 1.1 (May 2014)**

DRAFT

DRAFT FOR USE BY TECHNICAL OFFICERS AND DRAFTERS  
AND FOR COMMENT

## INTRODUCTION

### Background

This Glossary comprises a compilation of terminology, definitions and explanations given in existing publications in the Nuclear Security Series. Reference numbers match the publication numbers in the Nuclear Security Series. For ease of reference, each reference number has an associated letter indicating the category of the publication: F for the Nuclear Security Fundamentals [20F]; R for the Recommendations [13R, 14R, 15R]; G for Implementing Guides and T for Technical Guidance publications. In a few cases, terms defined in particular Nuclear Security Series publications, in particular the basic radiological and nuclear terms explained in [6T], 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. [13R\*, 14R]), 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 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), the other usage (and any difference in definition) is noted for information.

Some brief explanations have been added where they appear necessary, but in general no commentary is provided on the terms and definitions listed. It is proposed that a next step could be to annotate this compilation with commentary on the terms and definitions, particularly where there are multiple definitions of the same term or where different terms are used for what appears to be the same concept. Such annotations could form the basis for discussions and proposals for harmonizing terminology and definitions. However, it remains to be decided whether this second, more analytical step should be initiated immediately or should be deferred until the first iteration of a suite of Nuclear Security Series publications, and therefore the set of terms and definitions pertinent to those publications, is largely complete.

### Scope

The scope of the Nuclear Security Series 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 Nuclear Security Series publications. A number of general categories of terms that may be used in security related publications have been specifically excluded from this 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 (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 or IAEA Safeguards Glossary. Such terms and definitions may in some cases be referred to or discussed in this Nuclear Security Series 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, radiation detection instrumentation or computing). This terminology may be used in security contexts, but the definition of such terms is left to the experts in the relevant fields.
- (d) Very specialized terminology from a specific field within security (e.g. the detailed terminology of nuclear forensics or detection systems). If necessary, such terminology can be defined in the specialized publications to which it is relevant.

## Use of this Glossary

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

- (a) If different definitions are given in current 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 this 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 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 indicated in the text, drafters should use the most appropriate definition for their purposes. In particular:

- Preference should be given in guidance documents to definitions from the ‘parent’ Recommendations<sup>1</sup> or Implementing Guide.
- For guidance on cross-cutting topics, preference should be given to definitions from the Fundamentals [20F].
- Otherwise, as a general guide, preference should be given to definitions from publications higher in the hierarchy of Nuclear Security Series and/or published more recently. Therefore, for example, definitions from early Technical Guidance publications [1T–6T] should only be used if there is no other source in the 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;
- (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, and terms that supersede or are superseded by the term being described;
  - Miscellaneous information: for example, the units in which a quantity is normally measured, recommended parameter values, references, etc.

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.

Drafters of nuclear security guidance publications should, as far as possible, use the terms in this Glossary with the meanings given. Terms should also be used consistently, especially in guidance. Variety of expression — a virtue in most forms of writing — should be avoided if there is any possibility of causing confusion or ambiguity. Terms that are not listed in this Glossary may be used, provided that there is no suitable alternative term listed.

---

<sup>1</sup> i.e. [13R] for nuclear material and nuclear facilities; [14R] for other radioactive material and associated facilities; or [15R] for nuclear and other radioactive material out of regulatory control.

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 meaning, or if its meaning in a particular publication will be obvious to the reader from 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 matter 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 recommended definition should be used wherever possible. If the recommended 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 Nuclear Security Series 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 Nuclear Security Series 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, of course, whether any terms not defined in the publication need to be defined.)

If the glossary in a draft publication gives a definition different from that recommended in the Nuclear Security Series Glossary, reviewers should check:

- (a) That the definition recommended in the Nuclear Security Series Glossary could not reasonably have been used;
- (b) That the definition given in the draft publication reflects essentially the same meaning as the recommended definition.

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

# A

## **access control**

Means to ensure that access to assets is authorized and restricted based on business and security requirements. [17T – from ISO]

## **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*. [13R]

- ① Access delay can be accomplished by physical barriers, activated delays, and/or personnel.

## **adversary**

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

- ! There is some overlap between the use in different publications of the terms *adversary* and *threat* to describe such individuals.

## **alarm threshold value**

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

## **area**

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

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

***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*. [13R, 16T]

***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. [13R, 16T]

## **associated activity**

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

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

## **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. [20F]

- ① This includes *nuclear facilities* and any other facilities holding significant amounts of *radioactive material*.

## **attack**

An attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an asset. [17T – from ISO]

### **authentication**

The provision of assurance that a claimed characteristic of an entity is correct. [17T – from ISO]

### **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. [20F]
2. The granting by a *competent authority* of written permission for operation of an *associated facility* or for carrying out an *associated activity*. [14R, 15R]
3. A permission granted in a document by a regulatory body to a person who has submitted an application to manage a radioactive source. The authorization can take the form of a registration, a licence or alternative effective legal control measures which achieve the objectives of the Code of Conduct. [11G – taken from Code of Conduct]

### **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". [20F, 14R, 15R]

- ! The term “operator” is sometimes used in a broader sense to refer also to an organization or person applying for *authorization* [IAEA Safety Glossary].

### **availability**

The property of being accessible and usable upon demand by an authorized entity. [17T – from ISO]

## **B**

### **[border crossing point]**

See *point of [exit and] entry*.

- ! Sometimes used in older documents, with the same meaning as *point of entry* (or *point of exit or entry*) and the same distinction between designated and undesignated points, but now superseded.

## **C**

### **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*. [16T]

### **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. [4T]

**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. [4T]

**categorization**

A process performed to address the threat posed by a specific incident, with the goal of identifying the risk to the safety of first responders, law enforcement personnel and the public and determining if there is criminal activity or a threat to national security. [2T]

**central alarm station**

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

**characterization**

A process performed to determine the nature of the radioactive and associated evidence [in a *nuclear security event*]. [2T]

**competent authority**

1. A governmental organization or institution that has been designated by a State to carry out one or more *nuclear security* functions. [13R, 14R, 15R]. [For example, *competent authorities* may include *regulatory bodies*, law enforcement, customs and border control, intelligence and security agencies or health agencies, etc. [20F, 14R, 15R, 19G f/n]
2. Any national authority or authorities designated or otherwise recognized as such for any purpose relevant to this guide. [9G f/n]

**computer security**

A particular aspect of information security that is concerned with computer based systems, networks and digital systems. [17T]

**computer security incident**

An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of a computer based, networked or digital information system or the information that the system processes, stores, or transmits or that constitutes a violation or imminent risk of violation of security policies, security procedures, or acceptable use policies. [17T]

**computer security perimeter**

The logical border around a network to which critical assets are connected and to which access is controlled. [17T]

**computer security policy**

Aggregate of directives, regulations, rules and practices that prescribes how an organization manages and protects computers and computer systems. [17T]

**confidentiality**

The property that information is not made available or disclosed to unauthorized individuals, entities, or processes. [17T – from ISO]

### **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 [13R]

### **contingency plan**

1. 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. [13R, 19G f/n]
2. A part of the security plan or a stand-alone document that identifies reasonably foreseeable security events, provides initial planned actions, (including alerting appropriate authorities) and assigns responsibilities to appropriate operator personnel and response personnel. [11G definition of “security contingency plan”]

### **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. [13R]

- ① An adapted definition from the IAEA Transport Regulations.

### **countermeasure**

An action taken to counteract a *threat*, or to eliminate or reduce vulnerabilities. [17T]

- ! In safety, the term “countermeasure” is specifically reserved for actions aimed at alleviating the radiological consequences of an accident.

### **criminal act**

See *criminal or unauthorized acts*.

### **criminal or [intentional] unauthorized acts**

A general term encompassing *malicious acts* and any other intentional acts or omissions contrary to national law or regulations and having *nuclear security* implications.

- ① 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. [15R, 19G f/n with square bracketed text]

# D

## **defence in depth**

1. The combination of successive layers of systems and measures for the protection of *targets* from *nuclear security threats*. [20F, 17T]
2. The combination of multiple layers of systems and measures that have to be overcome or circumvented before *nuclear security* is compromised. [13R\*, 14R]
3. The combination of multiple layers of systems and measures for the protection of *targets* from nuclear security *threats*. [15R]
4. Implementing several layers of defence, including both administrative aspects (procedures, instructions, sanctions, access control rules, confidentiality rules) and technical aspects (multiple layers of protection together with measures for detection and delay) that adversaries would have to overcome or circumvent to achieve their objectives. [9G f/n]

! The term “defence in depth” is widely used in safety standards. While the general concept is similar, the safety definition of “defence in depth” is too complex and specific to be directly adapted for security.

## **design basis threat**

1. 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. [13R, 4T, 16T]
2. A description of the attributes and characteristics of potential *insider/external* adversaries who might attempt *unauthorized removal* of nuclear material or radioactive material or *sabotage*, against which a *physical protection system* is designed and evaluated. [9G f/n]
3. A comprehensive description of the motivation, intentions and capabilities of potential adversaries against which protection systems are designed and evaluated. [10G, 11G]

## **detection**

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. [13R]
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*. [15R, 19G f/n with “Means of attaining...” at beginning, 21G]
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*. [18G]

## **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*. [21G]

## **detection measure**

Measures intended to detect a criminal or an unauthorized act with nuclear security implications. [15R, 18G – with “criminal or unauthorized act”, 21G]

### **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. [15R, 18G – with “criminal or unauthorized act”, 21G]

### **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. [16T]

### **device**

1. [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. [21G]

***radiation exposure device***: A device with radioactive material designed to intentionally expose members of the public to radiation. [21G]

***radiological dispersal device***: A device to spread radioactive material using conventional explosives or other means. [21G]

① ICSANT 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.”

2. 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. [5T]

! Clearly this is a different type of “device” from those listed under definition 1. The term should therefore only be used with definition 2 in contexts in which there is no risk of confusion, and then with great care.

### **direct dispersal or release**

See *dispersal or release*.

### **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. [16T]

***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. [16T]

### **disused source**

A radioactive source which is no longer used, and is not intended to be used, in facilities and activities for which authorization has been granted [11G, attributed to Safety Glossary].

## F

### **false alarm**

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

### **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*. [13R]

### **front line system**

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

## G

### **graded approach**

1. The application of *nuclear security measures* proportional to the potential consequences of a *malicious act*. [13R\*, 14R]
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. [20F, 15R with “proportional” instead of “proportionate”]
3. An approach or process by which the scope, depth and rigour of the management and engineering control measures (such as physical protection system) are commensurate with the evaluation of the threat and the magnitude of any hazard involved with the failure of the item or process concerned. [9G f/n]

### **guard**

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

## H

### **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. [4T]

## **improvised nuclear device**

See *device*.

## **incident**

- ① Several types of *incident* are defined as a basis for categorizing entries in the Agency's Incident and Trafficking Database (ITDB).

## **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. [18G]

## **indirect dispersal or release**

See *dispersal or release*.

## **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. [15R, 18G, 21G]

## **information security**

The preservation of the confidentiality, integrity and availability of information. Note: In addition, other properties such as authenticity, accountability, non-repudiation and reliability can also be involved. [17T – from ISO]

## **initiating event**

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

- ① Sometimes referred to as a postulated initiating event. [16T]

## **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*. [16T]

## **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*.

## **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. [20F]

2. An *adversary* with authorized access to a nuclear facility, a transport operation or sensitive information. [8G]
3. 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. [13R]
4. 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*. [14R]

#### **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*. [19G f/n]

#### **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. [15R, 18G, 21G with “a detection instrument or set of such instruments”]

#### **integrity**

The property of protecting the accuracy and completeness of assets. [17T – from ISO]

## L

#### **limited access area**

See *area*.

#### **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. [16T]

***sabotage logic model:*** A *logic model* that documents the malicious events or combinations of malicious events that could lead to *unacceptable radiological consequences*. [16T]

***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*. [16T]

## M

#### **major public event**

1. A high-profile event that a State has determined to be a potential *target*. [20F, 15R, 21G]
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. [18G]

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

### **malicious act**

1. An act or attempt of *unauthorized removal* of *radioactive material* or *sabotage*. [13R\*, 14R]
2. A wrongful act or activity intentionally done or engaged in without legal justification or excuse (e.g. smuggling) or an act or activity intended to cause death or physical injury to any person, material damage to any person (e.g. theft) or damage to property or to the environment. [11G]

① This definition is taken from GOV/2002/10.

3. A deliberate act to remove radioactive material from authorized control (theft) or an act directed against radioactive material (e.g. sabotage) that could endanger workers, the public and the environment by exposure to radiation or the release or dispersal of radioactive material, including the deliberate dispersion of radioactive material to cause economic and social disruption. [9G f/n]

### **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. [4T]

*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. [4T]

### **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. [16T]

## **N**

### **need to know**

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. [17T, 19G f/n]

### **nuclear attribution**

The process of identifying the source of nuclear or radioactive material used in illegal activities, to determine the point of origin and routes of transit involving such material, and ultimately to contribute to the prosecution of those responsible. [2T]

### **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. [20F, 17T]
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. [13R]

① The 2005 CPPNM Amendment 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.

- ① ICSANT 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.

### nuclear forensic interpretation

The process of correlating the material characteristics [of nuclear or radioactive material] with the production history. [2T]

### nuclear forensics

The analysis of intercepted illicit nuclear or radioactive material and any associated material to provide evidence for *nuclear attribution*. [2T]

### 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). [13R, 14R] (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. [20F, 15R, 21G]

3. Plutonium except that with isotopic concentration exceeding 80% in plutonium-238; uranium-233; *uranium enriched in the isotope 235 or 233*; uranium containing the mixture of isotopes as occurring in nature other than in the form of ore or ore-residue; any material containing one or more of the foregoing. [9G f/n, 12T f/n]

- ① This definition is used in the CPPNM and ICSANT.

- ① For practical purposes, the three definitions of “nuclear material” all 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. [13R]

Material	Form	Category I	Category II	Category III <sup>c</sup>
1. Plutonium <sup>a</sup>	Unirradiated <sup>b</sup>	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 ( <sup>235</sup> U)	Unirradiated <sup>b</sup> <ul style="list-style-type: none"> <li>— Uranium enriched to 20% <sup>235</sup>U or more</li> <li>— Uranium enriched to 10% <sup>235</sup>U but less than 20%</li> <li>— Uranium enriched above natural, but less than 10% <sup>235</sup>U</li> </ul>	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 ( <sup>233</sup> U)	Unirradiated <sup>b</sup>	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) <sup>d,e</sup>	

---

<sup>a</sup> All plutonium except that with isotopic concentration exceeding 80% in plutonium-238.

<sup>b</sup> 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.

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

<sup>d</sup> 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.

<sup>e</sup> 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 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. [14R, 15R f/n]

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. [9G f/n, 11G, 12T f/n] 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. [7G f/n]

① The first part of this definition is taken from GOV/2005/50.

## **nuclear security culture**

1. The assembly of characteristics, attitudes and behaviours of individuals, organizations and institutions which serves as a means to support, enhance and sustain *nuclear security*. [20F, 13R, 14R, 15R, and 4T, 7G without “sustain”]

2. The characteristics and attitudes in organizations and of individuals which establish that security issues receive the attention warranted by their significance. [11G]

① The IAEA Safety Glossary 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 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 [15R] and is based on an appropriate legal and regulatory framework needed to implement the national strategy for the detection nuclear and other radioactive material out of regulatory control. [19G f/n]

## **nuclear security event**

1. An event that has potential or actual implications for nuclear security that must be addressed. [20F, 15R, 18G, 19G f/n, 21G]

2. An event that is assessed as having implications for *nuclear security*. [13R\*, 14R, 19G\* f/n]

① [19G] 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 *threat* from completing a *malicious act* or to *detect* or respond to *nuclear security events*. [14R]

2. 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. [20F, 15R, 21G in singular form]

3. Measures intended to prevent a nuclear security threat from completing criminal or intentional unauthorized acts involving or directed at nuclear and other radioactive material, associated facilities, or associated activities or to detect or respond to nuclear security events. [18G]

### **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*. [20F, 14R, 15R]
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*. [18G]

### **nuclear security system**

An integrated set of *nuclear security measures*. [20F, 14R, 15R, 18G, 21G]

### **nuclear security threat**

See *threat*.

## **O**

### **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*. [20F]
2. Any person, organization, or government entity licensed or authorized to undertake the operation of a *nuclear facility*. [13R]
  - ① Also used in [14R], 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*. [19G f/n]
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. [8G, 9G f/n]

5. Any organization or person applying for authorization or authorized and/or responsible for nuclear, radiation, radioactive waste or transport safety when undertaking activities or in relation to any nuclear facilities or sources of ionizing radiation. This includes, inter alia, private individuals, governmental bodies, consignors or carriers, licensees, hospitals, self-employed persons, etc. [10G, 11G]

① This is the definition from the IAEA Safety Glossary.

#### **other radioactive material**

Any *radioactive material* that is not *nuclear material*. [20F, 14R]

#### **out of regulatory control**

See *regulatory control*.

#### **outsider**

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

## 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. [13R]

#### **physical barrier**

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

#### **physical protection**

1. The *nuclear security* of *nuclear material* and *nuclear facilities*.
  - ❖ A footnote in Ref. [13R] effectively defines *physical protection* in this way. Hence, when the context is clearly *nuclear material* and *nuclear facilities*, *physical protection* and *nuclear security* may be considered synonymous.
2. 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*. [16T]

#### **physical protection measures**

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

#### **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*. [13R]

### **physical protection system**

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

### **point of [exit or ]entry**

1. An officially designated point of exit or entry is a 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. An undesignated point of exit or entry is any air, land and water crossing point that is not officially designated for travellers and/or goods by the State, such as green borders, sea shores and local airports. [15R, 18G]

2. 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 POEs. An undesignated POE is any air, land or water crossing point that is not officially designated for travellers and/or goods by the State, such as green borders, sea-shores and local airports. [21G]

❖ See also *border crossing point*.

### **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. [16T]

### **probabilistic safety assessment**

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

① This definition is from the IAEA Safety Glossary.

### **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. [15R, 18G, 21G]

### **radiation survey**

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

! 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.”

### **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. [9G f/n, 14R, 15R, 21G] 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. [20F]

2. Nuclear material and other radioactive substances which contain nuclides which undergo spontaneous disintegration (a process accompanied by emission of one or more types of ionising radiation, such as alpha-, beta-, neutron particles and gamma rays) and which may, owing to their radiological and fissile properties, cause death, serious bodily injury, or substantial damage to property or to the environment. [12T f/n]

① This definition is used in the ICSANT.

3. 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). [7G f/n]

### **radioactive source**

1. *Radioactive material* that is permanently sealed in a capsule or closely bonded, in a solid form and which is not exempt from *regulatory control*. [9G f/n] 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. [11G, 12T f/n, 14R]

① The full definition is from the Code of Conduct.

2. 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. [5T]

### **radioactive substance**

! Stated or implied in some Nuclear Security Series publications (e.g. Refs [13R] and [14R]) to be synonymous with *radioactive material*, in order to confirm consistency with the 2005 CPPNM Amendment. 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.

### **radiological dispersal device**

See *device*.

### **regulatory authority**

① 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, [19G])

### **regulatory body**

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

2. An organization designated by a national government as having legal authority for regulating nuclear, radiation, radioactive waste and transport safety. [5T]

## **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. [20F, 15R, 21G]

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. [14R, 19G f/n]

- ! **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.

## **response**

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

- ! 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*. [13R]

## **response measure**

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

## **response system**

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

## **risk**

The potential that a given threat will exploit the vulnerabilities of an asset, or group of assets, and thereby cause harm to the organization. It is measured in terms of a combination of the likelihood of an event and the severity of its consequences. [17T]

## **risk assessment**

Overall process of systematically identifying, estimating, analysing and evaluating risk. [17T]

# 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. [13R, 16T]

! 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. [13R]

① The definition in [13R] is the same as that in the 2005 CPPNM Amendment.

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*. [14R]

3. Any deliberate act directed against a nuclear or radiological facility or nuclear or radioactive material in use, storage or transport that could directly or indirectly endanger the health and safety of personnel, the public and the environment by exposure to radiation or release of radioactive substances. [10G, attributed to CPPNM]

4. Deliberate damage; sabotage in this context means deliberate damage to a radioactive source in use, storage or transport or to an associated facility. A deliberate act directed against a radioactive source in use, storage or transport could directly or indirectly endanger the health and safety of personnel, the public or the environment by exposure to radiation or release of radioactive material. [11G, “adapted from” INFCIRC/225 Rev 4]

5. Deliberate damage; sabotage in this context means deliberate damage to nuclear material or radioactive material in use, storage or transport or to an associated facility. A deliberate act directed against a nuclear facility or radioactive material in use, storage or transport could directly or indirectly endanger the health and safety of personnel, the public or the environment by exposure to radiation or release of radioactive material. [9G f/n, “adapted from” INFCIRC/225 Rev 4]

- [14R] states in a footnote that *radioactive substances* and *radioactive material* have the same meaning.

## **sabotage area logic model**

See *logic model*.

## **sabotage logic model**

See *logic model*.

## **safety alarm**

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

## **safety alarm threshold value**

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

## **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. [4T]

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

## **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. [4T]

## **security plan**

A document — prepared by the operator and possibly required to be reviewed by the regulatory body — that presents a detailed description of the security arrangements in place at a facility. [11G]

## **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. [4T]

## **sensitive information**

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

## **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. [20F]

## **shipper**

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

① The term *shipper* seems to be more commonly used in security in relation to the transport of *nuclear material*, whereas *consignor* is more commonly used in safety and security in the context of *radioactive material*.

**sigma multiplier**

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

**social engineering**

A non-technical form of information gathering or attack that relies on human interaction to manipulate people into inadvertently breaking security procedures, for example disclosing information or performing other actions with a security impact. [17T]

**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. [20F]

① Taken from the IAEA Statute, as amended by INFCIRC/153.

**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*. [20F]

① Taken from the IAEA Statute.

**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*. [13R]

**standard gamma ray background**

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

**standard neutron background**

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

**standard neutron source configuration**

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

**storage**

The holding of radioactive sources in a facility that provides for their containment with the intention of retrieval. [11G]

**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. [20F, 21G]

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*. [15R, 18G]

**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*. [16T]

**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. [4T]

**support system**

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

**system for nuclear material accountancy 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. [13R]

## 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*. [20F, 15R, 21G, 12T]

**threat**

1. A person or group of persons with motivation, intention and capability to commit a *malicious act*. [13R, 4T, 16T]
2. A likely cause of harm to people, damage to property or harm to the environment by an individual or individuals with the motivation, intention and capability to commit a malicious act. [8G]
3. An entity with motivation, intention and capability to commit a malicious act. [10G]
4. A characterization of an adversary capable of causing undesirable consequences, including the objectives, motivation and capabilities, e.g. number of potential attackers, equipment, training and attack plan. [9G f/n]
5. Potential cause of an unwanted incident, which may result in harm to a system or organization. [17T – from ISO] Note: In other IAEA Nuclear Security Series publications, ‘threat’ is typically defined as ‘a person or group of persons with motivation, intention and capability to commit a malicious act’. However, this publication [17T] uses the term in the computer security context, where a threat is not necessarily a person or persons.

***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. [20F]

### **threat assessment**

1. 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*. [13R, 14R]
2. An evaluation of the existing threats, usually including intelligence assessments, which describe the motivation, intentions, and capabilities of these threats to commit malicious acts. [10G]
3. An analysis that documents the credible motivations, intentions and capabilities of potential adversaries that could cause undesirable consequences with regard to radioactive material in use or storage and its associated facilities. [9G f/n, 11G]
4. 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. [4T]

### **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. [4T]

### **threat scenario**

See *scenario*.

### **threat statement**

A document that summarizes the threat assessment and has been modified to account for policy considerations. The DBT is an example of a threat statement. [10G]

### **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. [4T]

### **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. [4T]

### **transport**

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

### **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*. [13R]

### **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. [13R]

## U

### **unacceptable radiological consequences**

1. A level of radiological consequences, established by the State, above which the implementation of *nuclear security measures* is warranted. [13R\*, 4T, 16T\*]
2. A threshold of consequence that a State decides is so severe as to justify that resources be expended to prevent its occurrence. The resources are expended by those organizations responsible for providing the protection. [10G]

### **unauthorized act**

See *criminal or unauthorized act*.

### **unauthorized removal**

1. The theft or other unlawful taking of *radioactive material*. [13R\*, 4T]
2. The theft or other unlawful taking of *radioactive sources*. [11G]

### **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. [20F]

- ① Taken from the IAEA Statute. Also used in CPPNM and ICSANT.

## 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*.

### **vital area**

1. 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. [13R]
2. 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. [4T]

### **vulnerability**

Weakness of an asset or control that can be exploited by a threat. [17T – from ISO]

**vulnerability assessment**

A process which evaluates and documents the features and effectiveness of the overall security system at a particular facility. [11G]

## W

**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). [4T]

DRAFT

## REFERENCES

- [1T] INTERNATIONAL ATOMIC ENERGY AGENCY, Technical and Functional Specifications for Border Monitoring Equipment, Technical Guidance, Nuclear Security Series No. 1, IAEA, Vienna (2006).
- [2T] INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Forensics Support, Technical Guidance, Nuclear Security Series No. 2, IAEA, Vienna (2006).
- [3T] INTERNATIONAL ATOMIC ENERGY AGENCY, Monitoring for Radioactive Material in International Mail Transported by Public Postal Operators, Technical Guidance, Nuclear Security Series No. 3, IAEA, Vienna (2006).
- [4T] INTERNATIONAL ATOMIC ENERGY AGENCY, Engineering Safety Aspects of the Protection of Nuclear Power Plants against Sabotage, Technical Guidance, Nuclear Security Series No. 4, IAEA, Vienna (2007).
- [5T] INTERNATIONAL ATOMIC ENERGY AGENCY, Identification of Radioactive Sources and Devices, Technical Guidance, Nuclear Security Series No. 5, IAEA, Vienna (2007).
- [6T] INTERNATIONAL ATOMIC ENERGY AGENCY, Combating Illicit Trafficking in Nuclear and Other Radioactive Material, Technical Guidance, Nuclear Security Series No. 6, IAEA, Vienna (2007).
- [7G] INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Culture, Implementing Guide, IAEA Nuclear Security Series No. 7, IAEA, Vienna (2008).
- [8G] INTERNATIONAL ATOMIC ENERGY AGENCY, Preventive and Protective Measures against Insider Threats, Implementing Guide, IAEA Nuclear Security Series No. 8, IAEA, Vienna (2008).
- [9G] INTERNATIONAL ATOMIC ENERGY AGENCY, Security in the Transport of Radioactive Material, Implementing Guide, IAEA Nuclear Security Series No. 9, IAEA, Vienna (2008).
- [10G] INTERNATIONAL ATOMIC ENERGY AGENCY, Development, Use and Maintenance of the Design Basis Threat, Implementing Guide, IAEA Nuclear Security Series No. 10, IAEA, Vienna (2009).
- [11G] INTERNATIONAL ATOMIC ENERGY AGENCY, Security of Radioactive Sources, Implementing Guide, IAEA Nuclear Security Series No. 11, IAEA, Vienna (2009).
- [12T] INTERNATIONAL ATOMIC ENERGY AGENCY, Educational Programme in Nuclear Security, Technical Guidance, Nuclear Security Series No. 12, IAEA, Vienna (2010).
- [13R] 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).
- [14R] INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Recommendations on Radioactive Material and Associated Facilities, IAEA Nuclear Security Series No. 14, IAEA, Vienna (2011).
- [15R] 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).
- [16T] INTERNATIONAL ATOMIC ENERGY AGENCY, Identification of Vital Areas at Nuclear Facilities, Technical Guidance, Nuclear Security Series No. 16, IAEA, Vienna (2012).
- [17T] INTERNATIONAL ATOMIC ENERGY AGENCY, Computer Security at Nuclear Facilities, Technical Guidance, Nuclear Security Series No. 17, IAEA, Vienna (2011).

- [18G] INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Systems and Measures for Major Public Events, Implementing Guide, IAEA Nuclear Security Series No. 18, IAEA, Vienna (2012).
- [19G] 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).
- [20F] 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).
- [21G] 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).

DRAFT