# Developing Computer Security Regulations for Radioactive Material and Associated Facilities

F.A. morris

Pacific Northwest National Laboratory

Seattle, WA, United States of America

Email: fa.morris@pnnl.gov

r.a. weise

Pacific Northwest National Laboratory

Seattle, WA, United States of America

d.a. donnelly

Pacific Northwest National Laboratory

Seattle, WA, United States of America

**Abstract**

Radioactive material and associated facilities are vulnerable to cyberattack. Possible adversary scenarios include disabling or spoofing computer-based security systems to gain unauthorized access to radioactive material, to an associated facility, or to security-sensitive information; compromise of computer-based accounting and inventory systems to mask theft or diversion of radioactive material by insiders; and sabotage of computer-based safety or operational systems in order to cause the release of radiation. To counter such scenarios, many regulatory bodies are developing or considering the development of regulatory requirements for computer security, as recommended by current and forthcoming International Atomic Energy Agency (IAEA) guidance.

The paper presents a framework that regulatory bodies could use to undertake this process. The framework consists of a series of questions that the regulatory body could address in deciding whether and how to develop regulatory requirements for computer security, as well considerations that would go into addressing those questions. The questions addressed include:

1. whether the regulatory body has the legal authority to impose computer security requirements;
2. where to locate computer security requirements within the regulatory structure for nuclear security – e.g., as part of general nuclear security regulations or as separate requirements;
3. what other competent authorities may need to be involved in the development and implementation of computer security requirements;
4. whether to use a performance based, prescriptive or combined approach to computer security requirements;
5. what types of targets the computer security measures implemented by licensees should protect;
6. what basic content the regulation should include;
7. whether to vary the requirements based on practices (e.g., teletherapy versus industrial irradiator) or keep them generally applicable to all practices;
8. whether to develop implementing guidance, and if so, how to allocate topics between the regulation and guidance; and
9. how the licensee will be directed to document compliance with the resulting requirements, for example in the licensee’s security plan or in a separate computer security plan.

The paper also provides example regulatory provisions for different regulatory approaches to computer security. The result is a tool that can be used by regulatory bodies directly, in bilateral or multilateral regulatory development workshops, and in training on this topic.

## INTRODUCTION

Security of radioactive material and associated facilities is a relatively new topic. The *Code of Conduct on the Safety and Security of Radioactive Sources* (Code or Code of Conduct) [1], approved by the IAEA Board of Governors in 2003, was the first international instrument to call for the protection of radioactive material against malicious acts, through an effective national legislative and regulatory system of control. Interim IAEA guidance on the security of radioactive sources was issued that same year [2]. The first IAEA Nuclear Security Series (NSS) guidance on the security of radioactive material, including guidance on developing a regulatory programme, was published in 2009 [3].

Computer security,[[1]](#footnote-2) as it relates to nuclear security, is an even newer subject, addressed briefly in *Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities* *(INFCIRC/225/Revision 5)* (2011) [4] and more fully in *Computer Security at Nuclear Facilities* (2011) [5]. No current NSS publication specifically addresses computer security for radioactive material and associated facilities, although an implementing guide covering computer security throughout the nuclear security regime [6] will soon be published and more detailed guidance focused on computer security for radioactive material, associated facilities, and associated activities is in preparation [7].

In the absence of specific international guidance, the radiological security community has nonetheless recognized the importance of computer security. In the United States, the Nuclear Regulatory Commission (NRC)/ Agreement State Byproduct Materials Cyber Security Working Group recently assessed strategies for preventing and mitigating computer security vulnerabilities for Category-1 and 2 radioactive sources. While NRC decided not to develop new regulatory requirements for protection of radioactive material against cyber threats, it issued an Information Notice describing best practices that radioactive material licensees can use to protect their digital assets [8]. Similarly, the National Nuclear Security Administration (NNSA) Office of Radiological Security (ORS) has issued the publication *Cybersecurity Best Practices for Users of Radioactive Sources* [9].

Recognizing the growing threat and in anticipation of specific IAEA guidance, regulatory bodies around the world are considering whether and how to develop computer security regulations for radioactive material and associated facilities. The remainder of the paper presents a framework that regulatory bodies could use to undertake this process.

## framework for developing computer security regulations

The framework consists of a series of questions that the regulatory body could address as it develops regulatory requirements for computer security, as well considerations that would go into addressing those questions.

### Legal authority

Typically, regulations are developed by the regulatory body; depending on the national legal system, regulations may be adopted by the executive, the legislature, or the regulatory body itself. Regardless of the process, the imposition of enforceable requirements in a given field must be authorized by primary legislation (law). Thus, the regulatory body will need to determine whether there is adequate legal authority for the development and adoption of computer security requirements for radioactive material and associated facilities. This determination may not be straightforward. At one extreme, the national nuclear law or perhaps a national computer security law might specifically authorize the development of such requirements. But unless the law has been very recently enacted, it is unlikely to include a specific computer security provision. The law is more likely to authorize the imposition of information security requirements or indicate that security requirements must be based on countering the threat. Because computer security is a subset of information security [6] and the threat can include cyberattack scenarios, such provisions could be viewed as providing the necessary “hook” for computer security requirements, even if the law does not mention computer security. At the other extreme, the law may simply authorize the development of security requirements, without reference to specific subtopics. Ultimately, determining whether the necessary legal authority exists will be a matter of judgment for the regulatory body and its lawyers. If they determine that the necessary legal authority is lacking, the regulatory body might choose to issue non-mandatory guidance, until such time as the law might be amended to grant the necessary authority.

### Regulatory structure

Subject to any constraints posed by primary legislation, the regulatory body is likely to have some flexibility in determining how to incorporate computer security requirements within its regulatory structure. For example, it could establish computer security requirements as a stand-alone regulation, separate from nuclear security regulations addressing other topics, such as physical protection or nuclear material accounting and control (NMAC). Alternatively, the regulatory body could amend existing nuclear security regulations to include computer security as an additional topic that licensees must address. Often, there are separate nuclear security regulations for nuclear material and nuclear facilities and for radioactive material and associated facilities, sometimes with a set of general requirements applicable to both. In this case, the regulatory body could add appropriate computer security requirements to each of these regulations. While there is no single best approach, incorporating computer security requirements into existing nuclear security regulations has the advantage of facilitating the integration of computer security into the licensee’s overall nuclear security program. Such integration is especially important for topics where computer security and physical protection or NMAC intersect – e.g., information protection, access control, security plans. Ultimately, the regulatory body will need to decide how to incorporate computer security into its regulatory structure in the most practical and effective manner, given prevailing national practices and circumstances.

### Involvement of other competent authorities

In most countries, the regulatory body for nuclear security is likely to be responsible for developing regulations for radioactive material and associated facilities, although in some countries responsibility for issuing computer security regulations might be assigned to a competent authority with general responsibility for computer security across multiple domains, including but not limited to radiological security. In the former case, the regulatory body should involve other competent authorities with perceived interest in computer security in the development of its regulations. Similarly, in the latter case, competent authority for computer security should involve the regulatory body. In both cases, there are likely to be other competent authorities with interests and expertise in computer security that should also be consulted. These could include intelligence services and other authorities responsible for threat assessment; the ministry of interior, national police, and other security agencies; and the authorities responsible for emergency preparedness, planning, and response. Such involvement will improve the technical quality of the resulting computer security requirements and may also help to secure the buy-in of the participating agencies.

### Regulatory approach

In developing computer security requirements, the regulatory body may use the prescriptive approach, the performance-based approach, or the combined approach. Using the prescriptive approach, the regulatory body would establish a set of specific computer security measures that it has determined provide an acceptable level of performance to address the national threat. The advantage of the prescriptive approach is simplicity of implementation, for both the regulatory body and the licensee. The disadvantage is a lack of flexibility to address circumstances specific to the licensee where the required measures are impractical or ineffective. Using the performance-based approach, the regulatory body would establish overall objectives and require the licensee to identify and implement a set of computer security measures that meet the objectives. The advantage of the performance-based approach is in enabling the licensee to employ computer security measures that are well-suited to its distinctive operations. The disadvantage is the relatively high level of expertise needed by both the regulatory body and the licensee in order to implement this approach. Using the combined approach, the regulatory body would incorporate both prescriptive and performance-based elements. For example, the regulation might include prescriptive measures but allow the licensee to propose alternative measures that it can demonstrate are equally effective.

While each of these approaches is potentially applicable to computer security requirements for radioactive material and associated facilities, most regulatory bodies seem likely to conclude that purely performance-based requirements would require an unrealistic level of computer security expertise on the part of both its own staff and licensees. But at the same time, the rapid evolution of both hardware and software as well as a changing threat environment, could quickly render highly prescriptive requirements obsolete. As a result, computer security requirements that are largely prescriptive but stated generally enough to allow for adaptation seem likely to be the preferred approach in most instances. Regulatory bodies should avoid naming specific types of technology, software, or hardware in the regulations, as they are likely to go out-of-date quickly.

### Target identification

A fundamental principle of nuclear security holds that targets are identified and assessed to determine if they require protection from nuclear security threats [10]. This principle applies to a regulatory body developing computer security requirements for radioactive material and associated facilities, which should identify the types of radiological targets potentially subject to cyberattack in its country. For example, the NRC/Agreement State Byproduct Materials Cyber Security Working Group’s evaluation of the potential consequences that could occur if the availability, integrity, or confidentiality of data or systems associated with Category-1 and 2 quantities of radioactive material were compromised by a cyberattack. The Working Group considered the following types of digital assets as potential targets:

* Digital/microprocessor-based systems and devices that support the physical security of the licensee's facilities, including access control systems, physical intrusion detection and alarm systems, video camera monitoring systems, digital video recorders, door alarms, motion sensors, key card readers, and biometric scanners;
* Equipment and devices with software-based control, operation, and automation features, such as panoramic irradiators and stereotactic radiosurgery devices;
* Computers/systems used to maintain source inventories, audit data, and records necessary for compliance with security requirements and regulations; and
* Digital technology used to support incident response communications/coordination such as digital packet radio systems, digital repeater stations, and digital trunk radio systems [11].

This list would be a useful starting point for regulatory bodies developing computer security requirements for radioactive material and associated facilities.

### Regulation content

In the absence of a model regulation or even examples, a regulatory body developing computer security requirements for radioactive material and associated facilities faces both an opportunity and a challenge in defining the overall content. While resolution of several of the questions discussed above (location of computer security requirements in the regulatory structure, regulatory approach, targets to be protected) may determine some of the content, the regulatory body will have considerable flexibility in defining other aspects of the requirements. The following could serve as a starting point:

* **General provisions.** These provisions would address such topics as purpose and scope, definitions, basic requirement of compliance, computer security event reporting, and administrative matters such as records and records retention. The exact framing of these provisions would depend on whether the computer security requirements were included in a stand-alone regulation, as a subchapter within an existing nuclear security regulation, or inserted as amended provisions within an existing nuclear security regulation.
* **Targets to protect.** These provisions would identify the targets that the licensee must protect, as discussed above in 2.5.
* **Malicious acts to protect against.** These provisions would describe the types of cyberattacks that the licensee’s computer security measures must counter. Such provisions could be based on soon-to-be-published IAEA guidance, which indicates that computer security measures should protect against criminal or intentional unauthorized acts directed at or affecting computer-based systems with the intent of achieving or facilitating the theft, alteration, prevention of access, to or destruction of sensitive information or sensitive information assets by compromising the confidentiality, integrity, availability or a combination of these properties, of the sensitive information within a sensitive digital asset (SDA), or of the SDA itself [6].
* **Level of protection to provide.** These provisions would define the degree of protection that the licensee’s computer security measures must provide. According to the IAEA, the required degree of protection should be proportionate to the potential consequences of a successful cyberattack. One way to implement such an approach is to group computer-based systems and the associated SDAs into zones. The required level of protection would then correspond to the consequences of a successful cyberattack on the zone. Alternatively, the regulatory body could simply specify the overall degree of protection required. While these provisions are clearly central to a performance-based regulation, they are also essential for a prescriptive regulation, where they provide a means of evaluating whether the prescriptive requirements have been adequately implemented.
* **Required security measures.** These provisions determine the types of computer security measures that the licensee must implement. A performance-based regulation would identify such measures in general terms and specify how the licensee must demonstrate that the measures it selects meet the applicable performance requirement. A prescriptive regulation would identify specific measures that the licensee must implement. As discussed above, these measures should be sufficiently general that the licensee can adapt them to its own circumstances and adjust them to reflect changes in technology and the threat environment. A regulation based on the combined approach could take many forms. One example is NRC’s requirements for computer security at nuclear power plants which prescribes the process that the licensee must follow in order to develop the necessary security measures and identifies in general terms the licensee’s security program must meet [12].

### General versus practice-specific requirements

Radioactive material, specifically radioactive sources, are found in a wide range of medical, industrial, educational, research, and other applications, and as a result regulatory bodies may wish to create different computer security requirements depending on the type or use of the radioactive source. Category-1 radioactive sources are used to treat cancer patients with conventional teletherapy devices as well as with fixed, multi-beam (gamma knife) units, to sterilize a variety of products in large industrial irradiators, and to conduct research and treat blood prior to transfusion in smaller self-shielded irradiators. Category-2 radioactive sources are used in industrial radiography devices to perform imaging for non-destructive testing and to treat cancer patients with high and medium dose rate brachytherapy. Category-3 radioactive sources are used to perform thickness, density, and level measurements with fixed industrial gauges and to perform geophysical measurements with well-logging gauges. While all radioactive material and associated facilities are potentially vulnerable to cyberattack, they are not all vulnerable to the same degree, or in the same ways, or with the same consequences if a cyberattack were successful. For example, devices in fixed locations, such as teletherapy units or self-shielded irradiators, have physical protection systems, including access control, intrusion detection, and alarm assessment systems, all of which are digitally controlled and thus capable of defeat through cyberattack. In contrast, the security of an industrial radiography unit in the field may depend on simple physical control. As another example, some practices, such as teletherapy units and industrial irradiators employ software-based safety or operational control systems which could be disabled or manipulated in a way that may jeopardize patient or operator safety, while in other practices such systems are absent. Or to take yet another example, the consequences of a cyber-enabled malicious act – such as sabotage or unauthorized removal and use in a radiological dispersal device – would differ depending on the category of the radioactive material involved.

A regulatory body could choose to impose a single set of computer security requirements for all radioactive material and associated facilities or take these differences into account through various means. For example, there could be a separate set of requirements for each practice (or perhaps for each group of practices with common vulnerabilities). Or there could be a general set of requirements common to all practices, supplemented by specific requirements for practices with distinct vulnerabilities, such as those using software-based safety or operational control systems. The regulatory body might also choose to define the required degree of protection against cyberattack based on the category of the radioactive material, as a means of applying the graded approach to computer security based on the potential consequences of a malicious act. The regulatory body’s choices in this regard are likely to depend on the size and diversity of the country’s radioactive material inventory and the trade-offs between simplicity and customized requirements.

### Regulatory guidance

Regulatory bodies often complement regulations with implementing guidance. Such guidance documents are most often based on a regulation, providing non-mandatory advice on how to comply with the regulation. In some States, guidance creates a “safe harbor” – if the licensee follows the guidance, it will be considered in compliance, but generally following guidance is not the only way to comply. Regulatory bodies may find the issuance of guidance on computer security for radioactive material and associated facilities to be an effective regulatory tool for several reasons. First, as previously noted, including highly detailed prescriptive requirements in a regulation may impede use of the specific computer security measures best suited to a licensee’s own operations as well as adaptation of those measures to changing technologies and threats. Keeping the regulatory requirements reasonably general and putting the detail in guidance will better allow for necessary flexibility. Second, in most States guidance may be more easily and quickly revised than regulations. Thus, the guidance itself can be modified periodically to keep it current. Third, if the regulatory body decides not to develop a regulation, either because legal authority is found to be lacking or for other reasons, the regulatory body can use guidance to encourage licensees to improve computer security on a voluntary basis.

### Documentation of compliance

The IAEA recommends that the regulatory body require licensees to document their compliance with computer security requirements in a computer security plan [6]. Such a plan provides a means both of demonstrating to the regulatory body that the licensee has properly implemented computer security requirements and of providing an internal reference for the licensee’s staff on its computer security program, including roles and responsibilities, policies and procedures, and internal requirements. The computer security regulation should specifically require preparation of a computer security plan, either as part of the licensee’s overall security plan or as a separate document including arrangements for responding to a cyberattack. The elements of such a plan could be specified in the body of the regulation or in an annex and should be required to address at least the following topics:

* Organization and responsibilities
* Asset management
* Risk, vulnerability, and compliance assessment
* System security design and configuration management
* Operational security procedures
* Personnel management
* Response to a computer security event

The regulation should require the licensee to review its computer security plan at specified intervals and update it to reflect new technologies used in computer-based systems, as well as newly identified threats and vulnerabilities.

## example regulatory provisions

As a basis for discussion, the following are example provisions that could be included in a regulation on computer security for radioactive material and associated facilities. These provisions are presented as if they were a chapter of a regulation with other, existing chapters on other nuclear security topics, such as physical protection. They are for illustrative purposes only. Depending on how a regulatory body chooses to address the questions presented in Section 2 above, the provisions could look quite different. Because of space limitations, some provisions are less detailed than what would likely be included in an actual regulation.

### Purpose

This chapter establishes requirements for protecting the confidentiality, integrity and availability of electronic data and computer systems and processes whose compromise could have an adverse impact on safety or nuclear security functions.

### Scope

This chapter applies to licensees of Category 1 and 2 radioactive material.

### Basic requirement

No person or entity may use or store Category-1 or 2 radioactive material or operate an associated facility except in conformance with the requirements of this chapter.

### Definitions

* **Computer security.** The aspect of information security that is concerned with computer-based systems, networks and digital systems.
* **Computer-based systems.** The computation, communication, instrumentation and control devices that make up functional elements of a facility or activity, including desktop computers, mainframe systems, servers and network devices, as well as lower level components such as embedded systems and programmable logic controllers.
* **Computer security plan (CSP).** A plan for the implementation of the computer security policy specifying organizational roles, responsibilities and procedures.
* **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.
* **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.
* **Cyberattack.** A malicious act that targets sensitive information, sensitive information assets, sensitive digital assets, or other computer-based systems with the intent of compromising the safety or security of radioactive material or an associated facility.
* **Information security.** The preservation of the confidentiality, integrity and availability of information.
* **Sensitive digital assets (SDAs).** Sensitive information assets that are computer-based systems.
* **Sensitive information.** Information, in whatever form, including software, the unauthorized disclosure, modification, alteration, destruction, or denial of use of which could compromise nuclear security.
* **Sensitive information assets.** Any equipment or components that are used to store, process, control, or transmit sensitive information, including control systems, networks, information systems and any other electronic or physical media

### Response to computer security incidents

The licensee must establish policies and procedures to:

* Maintain the capability for timely detection and response to computer security incidents and cyberattacks;
* Notify the Regulatory Body of any significant computer security incident or any actual or attempted cyberattack within 4 hours of discovery;
* Mitigate the consequences of computer security incidents or cyberattacks;
* Correct exploited vulnerabilities; and
* Restore affected systems, networks, and/or equipment affected by computer security incidents or cyberattacks

### Computer security plan

The licensee must document its compliance with the requirements of this chapter in a computer security plan, which may be a stand-alone document or incorporated in the applicable general security plan. The licensee must review its computer security plan at least annually and update it to reflect new technologies used in computer-based systems, as well as newly identified threats and vulnerabilities.

[*Recommended topics to be included in computer security plans to be specified in regulatory guidance.*]

### Systems and devices to be protected

The licensee must protect:

* Computer-based systems that support physical protection systems;
* Equipment and devices with software-based control, operation, and automation features, whose compromise could facilitate sabotage or unauthorized removal;
* Computer-based systems used to maintain radioactive material inventories, audit data, and records necessary for compliance with nuclear security requirements; and
* Computer-based systems used to support incident response communications and coordination.

### Malicious acts to be countered

The licensee must protect the systems and devices specified in 3.6 against adversaries attempting to:

* Use a cyberattack to override the licensee’s network controls and security measures, allowing them to facilitate a physical attack, which could result in unauthorized and/or undetected access to radioactive material;
* Exploit security equipment to gain access to the licensee’s network to carry out a cyberattack, such as installing ransomware or stealing proprietary or other sensitive information;
* Use a cyberattack to manipulate or sabotage equipment and processes that use radioactive sources; or
* Use social engineering to exploit insiders to gain access to physical protection systems, networks, and related subsystems.

### Degree of protection required

In implementing the requirements of this chapter, the licensee must provide reasonable assurance that the systems and devices specified in 3.6 are adequately protected against the malicious acts specified in 3.7.

### Computer security management

The licensee must:

* Designate an individual responsible for computer security;
* Establish acceptable use policy for employee use of computer resources;
* Establish and implement plans, processes, and procedures for recovery and full restoration, in a timely manner, of any capabilities or services that are impaired due to a cyber event; and
* Establish and implement a security awareness program for all employees.

### Network policies and procedures

The licensee must establish policies and procedures to manage its digital networks in a secure manner.

[*Recommended topics for network policies and procedures to be specified in regulatory guidance.*]

### Network design and operations

The licensee must design and operate its digital networks in a manner that reduces their vulnerability to the malicious acts specified in 3.7.

[*Recommended practices for network design and operations to be specified in regulatory guidance.*]

### Hardware and software acquisition

The licensee must adopt a systematic approach for acquiring hardware and software that reduces their vulnerability to the malicious acts specified in 3.7.

[*Recommended practices for hardware and software acquisition to be specified in regulatory guidance.*]

### Computer security measures

The licensee must implement measures to reduce the vulnerability of the systems and devices specified in 3.6 to the malicious acts specified in 3.7.

[*Recommended computer security measures to be specified in regulatory guidance.*]

## Conclusions

Radioactive material and associated facilities are vulnerable to cyberattack. As a result, many regulatory bodies are developing or considering the development of regulatory requirements for computer security. The framework presented in the paper can help regulatory bodies undertake the process of regulatory development in a systematic manner. The example regulatory provisions presented can serve as a tool for use by regulatory bodies directly, in bilateral or multilateral regulatory development workshops, and in training on this topic.

References

1. INTERNATIONAL ATOMIC ENERGY AGENCY, Code of Conduct on the Safety and Security of Radioactive Sources, IAEA/CODEOC/2004, IAEA, Vienna (2004).
2. INTERNATIONAL ATOMIC ENERGY AGENCY, Security of radioactive sources, Interim guidance for comment, IAEA-TECDOC-1355, IAEA, Vienna (2003).
3. INTERNATIONAL ATOMIC ENERGY AGENCY, Security of Radioactive Sources, IAEA Nuclear Security Series No. 11, IAEA, Vienna (2009).
4. INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5), Nuclear Security Series No. 13, IAEA, Vienna (2011)
5. INTERNATIONAL ATOMIC ENERGY AGENCY, Computer Security at Nuclear Facilities, IAEA Nuclear Security Series No. 17, IAEA, Vienna (2011).
6. INTERNATIONAL ATOMIC ENERGY AGENCY, Computer Security for Nuclear Security, IAEA NST045, IAEA, Vienna (forthcoming).
7. HERDES, G., Apogee Group LLC, personal communication, 2019.
8. UNITED STATES NUCLEAR REGULATORY COMMISSION, Effective Cyber Security Practices to Protect Digital Assets of Byproduct Materials Licensees, NRC Information Notice 2019-04 (2019).
9. NATIONAL NUCLEAR SECURITY ADMINISTRATION, OFFICE OF RADIOLOGICAL SECURITY, Cybersecurity Best Practices for Users of Radioactive Sources (2018).
10. INTERNATIONAL ATOMIC ENERGY AGENCY, Objective and Essential Elements of a State’s Nuclear Security Regime, IAEA Nuclear Security Series No. 20, IAEA, Vienna (2014).
11. UNITED STATES NUCLEAR REGULATORY COMMISSION, Cyber Security for Radioactive Byproduct Materials Licensees, <https://www.nrc.gov/security/byproduct/cyber-security-radioactive-byproduct-materials-licensees.html> (accessed October 11, 2019).

PNNL-SA-149458

1. The IAEA uses the term computer security for what in some countries is referred to as cybersecurity or information technology (IT) security. The paper follows IAEA usage, recognizing these three terms are synonymous. [↑](#footnote-ref-2)