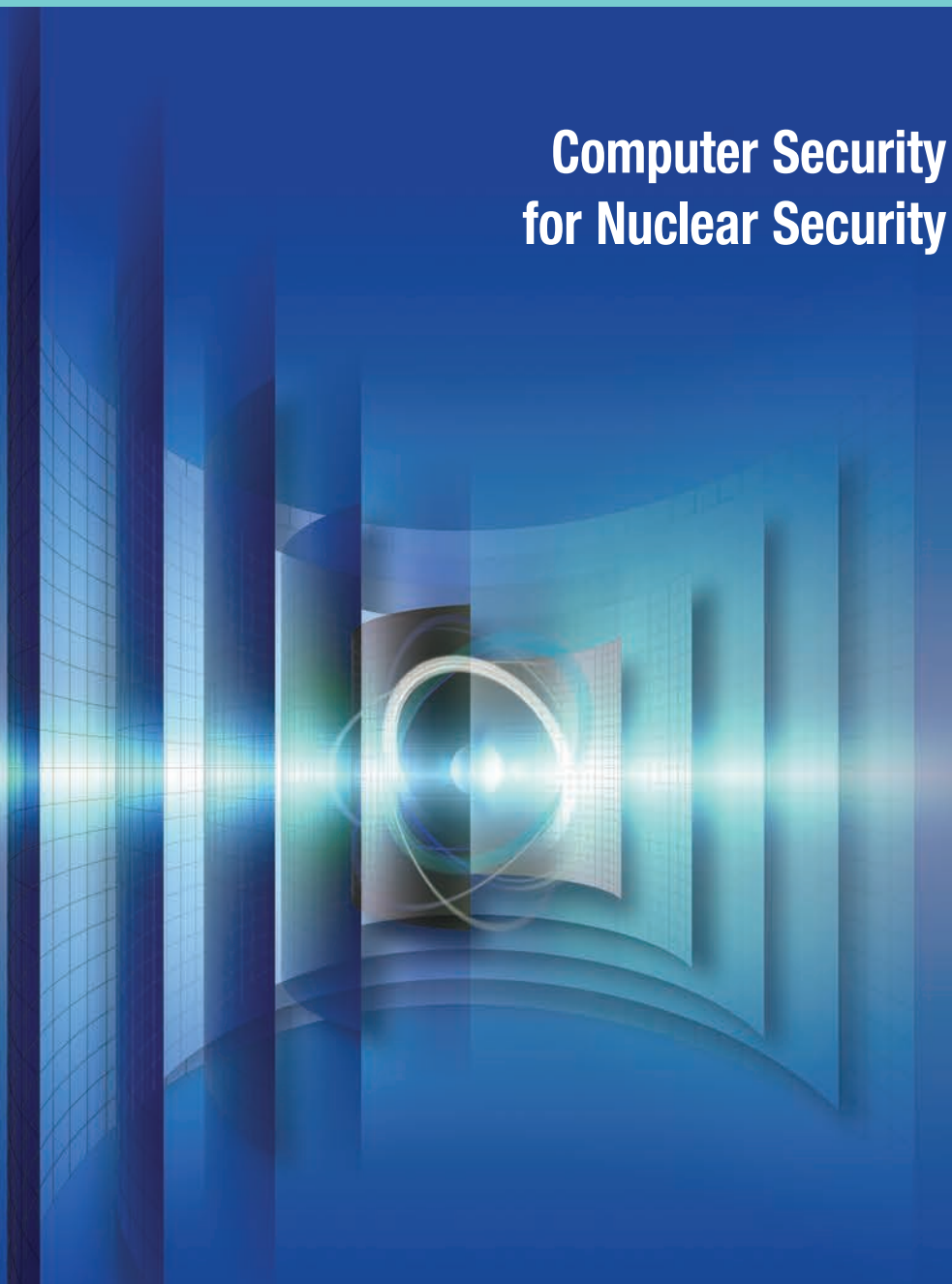
IAEA Nuclear Security Series No. 42-G

Implementing Guide

Computer Security for Nuclear Security



IAEA
International Atomic Energy Agency

IAEA NUCLEAR SECURITY SERIES

Nuclear security issues relating to the prevention and detection of, and response to, criminal or intentional unauthorized acts involving, or directed at, nuclear material, other radioactive material, associated facilities or associated activities are addressed in the **IAEA Nuclear Security Series**. These publications are consistent with, and complement, international nuclear security instruments, such as the Convention on the Physical Protection of Nuclear Material and its Amendment, the International Convention for the Suppression of Acts of Nuclear Terrorism, United Nations Security Council resolutions 1373 and 1540, and the Code of Conduct on the Safety and Security of Radioactive Sources.

CATEGORIES IN THE IAEA NUCLEAR SECURITY SERIES

Publications in the IAEA Nuclear Security Series are issued in the following categories:

- **Nuclear Security Fundamentals** specify the objective of a State's nuclear security regime and the essential elements of such a regime. They provide the basis for the Nuclear Security Recommendations.
- **Nuclear Security Recommendations** set out measures that States should take to achieve and maintain an effective national nuclear security regime consistent with the Nuclear Security Fundamentals.
- **Implementing Guides** provide guidance on the means by which States could implement the measures set out in the Nuclear Security Recommendations. As such, they focus on how to meet the recommendations relating to broad areas of nuclear security.
- **Technical Guidance** provides guidance on specific technical subjects to supplement the guidance set out in the Implementing Guides. They focus on details of how to implement the necessary measures.

DRAFTING AND REVIEW

The preparation and review of Nuclear Security Series publications involves the IAEA Secretariat, experts from Member States (who assist the Secretariat in drafting the publications) and the Nuclear Security Guidance Committee (NSGC), which reviews and approves draft publications. Where appropriate, open-ended technical meetings are also held during drafting to provide an opportunity for specialists from Member States and relevant international organizations to review and discuss the draft text. In addition, to ensure a high level of international review and consensus, the Secretariat submits the draft texts to all Member States for a period of 120 days for formal review.

For each publication, the Secretariat prepares the following, which the NSGC approves at successive stages in the preparation and review process:

- An outline and work plan describing the intended new or revised publication, its intended purpose, scope and content;
- A draft publication for submission to Member States for comment during the 120 day consultation period;
- A final draft publication taking account of Member States' comments.

The process for drafting and reviewing publications in the IAEA Nuclear Security Series takes account of confidentiality considerations and recognizes that nuclear security is inseparably linked with general and specific national security concerns.

An underlying consideration is that related IAEA safety standards and safeguards activities should be taken into account in the technical content of the publications. In particular, Nuclear Security Series publications addressing areas in which there are interfaces with safety — known as interface documents — are reviewed at each of the stages set out above by relevant Safety Standards Committees as well as by the NSGC.

COMPUTER SECURITY FOR NUCLEAR SECURITY

The following States are Members of the International Atomic Energy Agency:

AFGHANISTAN
ALBANIA
ALGERIA
ANGOLA
ANTIGUA AND BARBUDA
ARGENTINA
ARMENIA
AUSTRALIA
AUSTRIA
AZERBAIJAN
BAHAMAS
BAHRAIN
BANGLADESH
BARBADOS
BELARUS
BELGIUM
BELIZE
BENIN
BOLIVIA, PLURINATIONAL STATE OF
BOSNIA AND HERZEGOVINA
BOTSWANA
BRAZIL
BRUNEI DARUSSALAM
BULGARIA
BURKINA FASO
BURUNDI
CAMBODIA
CAMEROON
CANADA
CENTRAL AFRICAN REPUBLIC
CHAD
CHILE
CHINA
COLOMBIA
COMOROS
CONGO
COSTA RICA
CÔTE D'IVOIRE
CROATIA
CUBA
CYPRUS
CZECH REPUBLIC
DEMOCRATIC REPUBLIC OF THE CONGO
DENMARK
DJIBOUTI
DOMINICA
DOMINICAN REPUBLIC
ECUADOR
EGYPT
EL SALVADOR
ERITREA
ESTONIA
ESWATINI
ETHIOPIA
FIJI
FINLAND
FRANCE
GABON
GEORGIA
GERMANY
GHANA
GREECE
GRENADA
GUATEMALA
GUYANA
HAITI
HOLY SEE
HONDURAS
HUNGARY
ICELAND
INDIA
INDONESIA
IRAN, ISLAMIC REPUBLIC OF
IRAQ
IRELAND
ISRAEL
ITALY
JAMAICA
JAPAN
JORDAN
KAZAKHSTAN
KENYA
KOREA, REPUBLIC OF
KUWAIT
KYRGYZSTAN
LAO PEOPLE'S DEMOCRATIC REPUBLIC
LATVIA
LEBANON
LESOTHO
LIBERIA
LIBYA
LIECHTENSTEIN
LITHUANIA
LUXEMBOURG
MADAGASCAR
MALAWI
MALAYSIA
MALI
MALTA
MARSHALL ISLANDS
MAURITANIA
MAURITIUS
MEXICO
MONACO
MONGOLIA
MONTENEGRO
MOROCCO
MOZAMBIQUE
MYANMAR
NAMIBIA
NEPAL
NETHERLANDS
NEW ZEALAND
NICARAGUA
NIGER
NIGERIA
NORTH MACEDONIA
NORWAY
OMAN
PAKISTAN
PALAU
PANAMA
PAPUA NEW GUINEA
PARAGUAY
PERU
PHILIPPINES
POLAND
PORTUGAL
QATAR
REPUBLIC OF MOLDOVA
ROMANIA
RUSSIAN FEDERATION
RWANDA
SAINT LUCIA
SAINT VINCENT AND THE GRENADINES
SAMOA
SAN MARINO
SAUDI ARABIA
SENEGAL
SERBIA
SEYCHELLES
SIERRA LEONE
SINGAPORE
SLOVAKIA
SLOVENIA
SOUTH AFRICA
SPAIN
SRI LANKA
SUDAN
SWEDEN
SWITZERLAND
SYRIAN ARAB REPUBLIC
TAJIKISTAN
THAILAND
TOGO
TRINIDAD AND TOBAGO
TUNISIA
TURKEY
TURKMENISTAN
UGANDA
UKRAINE
UNITED ARAB EMIRATES
UNITED KINGDOM OF GREAT BRITAIN AND NORTHERN IRELAND
UNITED REPUBLIC OF TANZANIA
UNITED STATES OF AMERICA
URUGUAY
UZBEKISTAN
VANUATU
VENEZUELA, BOLIVARIAN REPUBLIC OF
VIET NAM
YEMEN
ZAMBIA
ZIMBABWE

The Agency's Statute was approved on 23 October 1956 by the Conference on the Statute of the IAEA held at United Nations Headquarters, New York; it entered into force on 29 July 1957. The Headquarters of the Agency are situated in Vienna. Its principal objective is "to accelerate and enlarge the contribution of atomic energy to peace, health and prosperity throughout the world".

IAEA NUCLEAR SECURITY SERIES No. 42-G

COMPUTER SECURITY FOR NUCLEAR SECURITY

IMPLEMENTING GUIDE

INTERNATIONAL ATOMIC ENERGY AGENCY
VIENNA, 2021

COPYRIGHT NOTICE

Marketing and Sales Unit, Publishing Section
International Atomic Energy Agency
Vienna International Centre
PO Box 100
1400 Vienna, Austria
fax: +43 1 26007 22529
tel.: +43 1 2600 22417
email: sales.publications@iaea.org
www.iaea.org/publications

Printed by the IAEA in Austria
July 2021
STI/PUB/1918

IAEA Library Cataloguing in Publication Data

Names: International Atomic Energy Agency.
Title: Computer security for nuclear security / International Atomic Energy Agency.
Description: Vienna : International Atomic Energy Agency, 2021. | Series: IAEA nuclear security series, ISSN 1816–9317 ; no. 42-G | Includes bibliographical references.
Identifiers: IAEAL 21-01371 | ISBN 978–92–0–121120–0 (paperback : alk. paper) | ISBN 978–92–0–121220–7 (pdf) | ISBN 978–92–0–121320–4 (epub) | ISBN 978–92–0–121420–1 (mobipocket)
Subjects: LCSH: Computer networks — Security measures. | Nuclear facilities — Security measures. | Computer security.
Classification: UDC 621.039:004.056 | STI/PUB/1918

FOREWORD

by Rafael Mariano Grossi
Director General

The IAEA Nuclear Security Series provides international consensus guidance on all aspects of nuclear security to support States as they work to fulfil their responsibility for nuclear security. The IAEA establishes and maintains this guidance as part of its central role in providing nuclear security related international support and coordination.

The IAEA Nuclear Security Series was launched in 2006 and is continuously updated by the IAEA in cooperation with experts from Member States. As Director General, I am committed to ensuring that the IAEA maintains and improves upon this integrated, comprehensive and consistent set of up to date, user friendly and fit for purpose security guidance publications of high quality. The proper application of this guidance in the use of nuclear science and technology should offer a high level of nuclear security and provide the confidence necessary to allow for the ongoing use of nuclear technology for the benefit of all.

Nuclear security is a national responsibility. The IAEA Nuclear Security Series complements international legal instruments on nuclear security and serves as a global reference to help parties meet their obligations. While the security guidance is not legally binding on Member States, it is widely applied. It has become an indispensable reference point and a common denominator for the vast majority of Member States that have adopted this guidance for use in national regulations to enhance nuclear security in nuclear power generation, research reactors and fuel cycle facilities as well as in nuclear applications in medicine, industry, agriculture and research.

The guidance provided in the IAEA Nuclear Security Series is based on the practical experience of its Member States and produced through international consensus. The involvement of the members of the Nuclear Security Guidance Committee and others is particularly important, and I am grateful to all those who contribute their knowledge and expertise to this endeavour.

The IAEA also uses the guidance in the IAEA Nuclear Security Series when it assists Member States through its review missions and advisory services. This helps Member States in the application of this guidance and enables valuable experience and insight to be shared. Feedback from these missions and services, and lessons identified from events and experience in the use and application of security guidance, are taken into account during their periodic revision.

I believe the guidance provided in the IAEA Nuclear Security Series and its application make an invaluable contribution to ensuring a high level of nuclear security in the use of nuclear technology. I encourage all Member States to promote and apply this guidance, and to work with the IAEA to uphold its quality now and in the future.

EDITORIAL NOTE

Guidance issued in the IAEA Nuclear Security Series is not binding on States, but States may use the guidance to assist them in meeting their obligations under international legal instruments and in discharging their responsibility for nuclear security within the State. Guidance expressed as 'should' statements is intended to present international good practices and to indicate an international consensus that it is necessary for States to take the measures recommended or equivalent alternative measures.

Security related terms are to be understood as defined in the publication in which they appear, or in the higher level guidance that the publication supports. Otherwise, words are used with their commonly understood meanings.

An appendix is considered to form an integral part of the publication. Material in an appendix has the same status as the body text. Annexes are used to provide practical examples or additional information or explanation. Annexes are not integral parts of the main text.

Although great care has been taken to maintain the accuracy of information contained in this publication, neither the IAEA nor its Member States assume any responsibility for consequences which may arise from its use.

The use of particular designations of countries or territories does not imply any judgement by the publisher, the IAEA, as to the legal status of such countries or territories, of their authorities and institutions or of the delimitation of their boundaries.

The mention of names of specific companies or products (whether or not indicated as registered) does not imply any intention to infringe proprietary rights, nor should it be construed as an endorsement or recommendation on the part of the IAEA.

CONTENTS

1. INTRODUCTION

BACKGROUND

1.1. Computer based systems play an essential role in all aspects of the safe and secure operation of facilities and activities using, storing and transporting nuclear material and other radioactive material, including maintaining physical protection, and in measures for detection of and response to material out of regulatory control. All such computer based systems therefore need to be secured against criminal or intentional unauthorized acts. As technology advances, the use of computer based systems in all aspects of operations, including nuclear security and safety, is expected to increase.

1.2. The Nuclear Security Fundamentals [1] stress the importance of information security, including computer security, within a nuclear security regime, and the need for assurance activities to identify and address issues and factors that might affect the capacity to provide adequate nuclear security, including computer security.

1.3. The security of sensitive information is a component of Essential Element 3 for a national nuclear security regime. Reference [1] states that: "The legislative and regulatory framework, and associated administrative measures … Provide for the establishment of regulations and requirements for protecting the confidentiality of *sensitive information* and for protecting *sensitive information assets*". The security of sensitive information and sensitive information assets implies protecting the confidentiality, integrity and availability of such information and assets. The Amendment to the Convention on the Physical Protection of Nuclear Material [2] also identifies the protection of the confidentiality of information as its Fundamental Principle L.

1.4. Paragraph 4.10 of the Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5) [3] states:

> "Computer based systems used for physical protection, nuclear safety, and nuclear material accountancy and control should be protected against compromise (e.g. cyber attack, manipulation or falsification) consistent with the *threat assessment* or *design basis threat*."

1.5. The Nuclear Security Recommendations on radioactive material and associated facilities [4] and on nuclear and other radioactive material out of

regulatory control [5] also stress the need to prevent unauthorized access to sensitive information and to protect it from compromise. Suggested Recommendations level guidance, intended to supplement the recommendations on computer security in Refs [3–5] pending future revision of these publications, is provided in Annex I.

1.6. When computer based systems are used to process, transmit and store sensitive information in digital form, its confidentiality, integrity and availability need to be sufficiently protected through the implementation of computer security measures throughout the life cycle of such digital assets. Computer security includes the measures necessary for the prevention and detection of, response to and recovery of computer based systems from cyber-attacks.

1.7. Nuclear security threats have identified cyber-attacks as a means to target computer based systems to carry out or facilitate malicious acts, whether directly or in combination with more conventional means such as physical access and insiders. Such acts could result in unauthorized removal of nuclear or other radioactive material or sabotage potentially leading to unacceptable radiological consequences. Cyber-attacks could also be used to facilitate other criminal or intentional unauthorized acts, such as trafficking of nuclear or other radioactive material out of regulatory control.

1.8. To address the full range of potential nuclear security threats, therefore, a nuclear security regime needs to include the means to address threats who have or can acquire skills for targeting computer based systems with cyber-attacks. Furthermore, nuclear security threats who do not themselves have such skills can induce individuals who do have them (for example, by payment or by duress) to assist.

1.9. Maintaining effective computer security at facilities handling nuclear material or other radioactive material, and in associated activities such as transport, is a significant challenge, owing to the substantial and rapidly evolving threat. Many of the essential elements of a State's nuclear security regime depend upon, or are supported by, computer based systems and therefore depend upon effective computer security.

OBJECTIVE

1.10. The objective of this publication is to provide guidance on developing and implementing computer security as an integral component of nuclear security.

1.11. This Implementing Guide is intended for policy makers, competent authorities, operators, shippers, carriers and others with responsibilities for nuclear security and safety.

SCOPE

1.12. The guidance in this publication applies to the computer security aspects of nuclear security and its interfaces with nuclear safety and with other elements of a State's nuclear security regime, such as physical protection of nuclear material and nuclear facilities, security of radioactive material and associated facilities and activities, and detection of and response to nuclear security events. The scope of this publication includes computer based systems, the compromise of which could adversely affect nuclear security or nuclear safety.

1.13. This publication addresses general aspects of computer security applicable to all areas of nuclear security, including the security of nuclear material and nuclear facilities, of radioactive material and associated facilities, and of nuclear and other radioactive material out of regulatory control. More detailed guidance on computer security specific to the security of nuclear facilities, including focused examples of technical implementation of computer security measures and computer security risk management can be found in IAEA Nuclear Security Series Nos 33-T, Computer Security of Instrumentation and Control Systems at Nuclear Facilities [6] and 17-T (Rev. 1), Computer Security Techniques for Nuclear Facilities [7].

1.14. This publication refers to guidance on information security in the Nuclear Security Fundamentals [1] and Recommendations [3–5], but does not provide detailed guidance on this general topic. IAEA Nuclear Security Series No. 23-G, Security of Nuclear Information [8] provides guidance on the security of nuclear information and the identification and securing of sensitive information and sensitive information assets.

STRUCTURE

1.15. Following this introduction, Section 2 introduces key terminology and concepts. Section 3 sets out the State's roles and responsibilities in relation to computer security in the nuclear security regime, and Section 4 sets out roles and responsibilities of relevant entities. Section 5 describes the activities of the State in establishing a computer security strategy for nuclear security, and Section 6

describes activities for implementing the strategy. Section 7 describes elements and measures for a computer security programme (CSP[1]). Section 8 describes activities to sustain computer security. The Appendix provides important technical considerations concerning interfaces with nuclear safety.

1.16. Annex I provides suggested Recommendations level guidance on computer security for a national nuclear security regime, with which the implementing guidance in this publication is consistent. Supporting the guidance provided in this publication, examples of possible implementation measures are provided in Annexes II–IV. Annex II provides an overview of the cyberthreat profiles. Annex III provides examples of the assignment of computer security responsibilities in the nuclear security regime, and Annex IV provides an illustration of a framework for computer security competences.

2. CONCEPTS AND CONTEXT

KEY TERMINOLOGY

2.1. Organizations within a State create, process, handle and store many types of information. Some of this information, such as military secrets or personal information of the citizens, may be deemed sufficiently sensitive as to require specific protection. The State may establish national information security laws defining and classifying information and define specific protection requirements, including those for data in digital form and for associated computer based systems. Information within the State's nuclear security regime will be subject to these requirements, and may require protection of other additional information, or additional protection for certain types of information that, if compromised could assist an adversary in carrying out a malicious act against a facility or activity or other criminal or intentional unauthorized act involving nuclear or other radioactive material. Sensitive information is defined as information, in whatever form, including software, the unauthorized disclosure, modification, alteration, destruction or denial of use of which could compromise nuclear security [1]. Figure 1 illustrates the concepts of and relationships between sensitive information

[1] Some organizations may refer to the computer security programme as a computer security plan.

assets, computer based systems and sensitive digital assets (SDAs). These concepts are described further below.

2.2. Sensitive information assets are defined [1] as any equipment or components that are used to store, process, control or transmit sensitive information. Sensitive information can be in digital or any other format.

2.3. Computer based systems are technologies that create, provide access to, process, compute, communicate or store digital information, or perform, provide or control services involving such information. Such systems may include desktops, laptops, tablets and other personal computers, smart phones, mainframe computers, servers, digital instrumentation and control devices, programmable logic controllers, printers, network devices, and embedded components and devices. Such systems may also include virtual services, such as cloud computing or virtual machines. These systems may exist as a single component or as a collection of digital assets.

2.4. Computer based systems perform many functions across a State. There may be computer based systems within the nuclear security regime that provide valuable business and communications functions, but that are not sensitive in

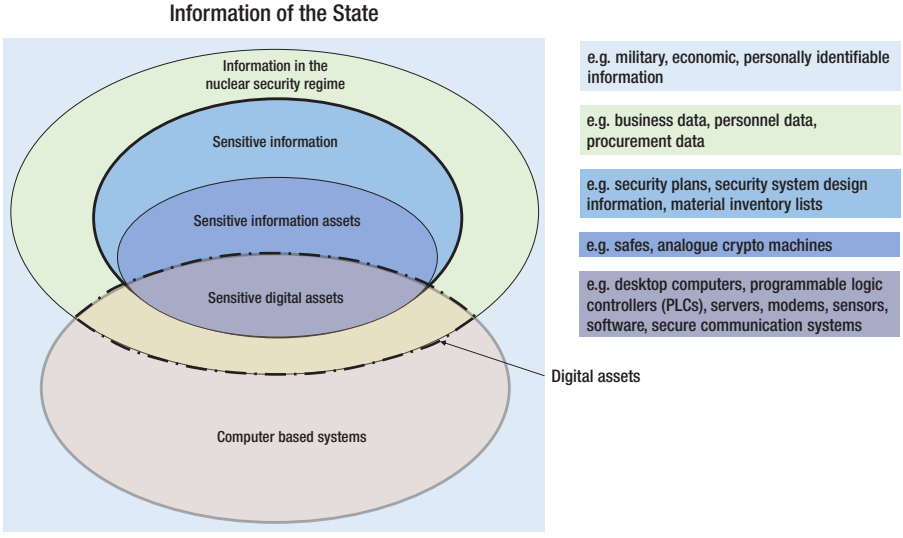


FIG. 1. Information and computer based systems in the State and in the nuclear security regime.

relation to nuclear security and are therefore outside the scope of the guidance in this publication.

2.5. Sensitive information assets need to be protected to prevent the compromise of the sensitive information that they store, process, control or transmit. Protection approaches will vary depending upon the type of asset in question and the form of the information. Reference [8] primarily addresses protection of written information on paper and other information in 'hard copy' form. Digital assets are computer based systems (or parts thereof) that are associated with or within a State's nuclear security regime. The term 'sensitive digital asset' (SDA) is used to identify those sensitive information assets that are (or are parts of) computer based systems. SDAs need computer security measures for their protection.

2.6. SDAs support systems that perform nuclear safety, nuclear security and nuclear material accounting and control functions, or that store and process sensitive information related to such functions. SDAs, and hence the essential functions they perform, might be vulnerable to cyber-attack and might be specifically targeted by adversaries. Such an attack and the compromise of the SDA could lead to adverse impacts on nuclear security and safety. Compromise of SDAs could potentially contribute to or result in, for example:

(a) Sabotage leading to unacceptable radiological consequences or high radiological consequences if vital areas were to be affected;
(b) Unauthorized removal of nuclear or other radioactive material;
(c) Degraded capabilities to prevent, detect and respond to nuclear security events;
(d) Loss or alteration of, or denial of access to sensitive information.

2.7. Depending on the situation, software may need to be treated as information or as an integral part of a computer based system, or both. For example, in its initial design phase, software might be a high level expression of a processing algorithm and best treated as information. In its operational (i.e. executable) form, software will form an intrinsic part of its associated computer based system without which the system does not function, and most cyber-attacks will aim to exploit vulnerabilities in that software.

2.8. Computer security is a particular aspect of information security that is concerned with the protection of computer based systems against compromise. This includes all interconnected systems and networks of which such systems are elements. The terms 'IT security' and 'cybersecurity' are, for the purposes of this publication, considered synonymous with computer security and are not

used. Computer security is a subset of information security, as stated in Ref. [8]. Information security and computer security often share objectives, methodology and terminology.

2.9. In view of the interconnectivity of computer networks and information flow, computer security measures are also needed to protect SDAs against threats exploiting other digital assets and other computer based systems. A layered approach of graded security measures across all digital assets provides defence in depth against cyber-attacks.

IDENTIFICATION OF SENSITIVE DIGITAL ASSETS

2.10. Owners and/or designers of computer based systems should use a systematic process to identify the functions performed by their digital assets that are required for nuclear security and safety, any associated SDAs, and the potential effect on nuclear security and safety if any SDAs are compromised. In doing so, they should recognize that a computer based system that does not itself contain SDAs could nevertheless, if compromised or infected with malware[2], potentially affect SDAs in other systems.

2.11. Computer security aims to maintain the attributes of confidentiality, integrity and availability of sensitive information within SDAs, and of the SDAs themselves. The SDAs and their sensitive information support the correct operation of the functions that support the nuclear security regime. Depending on the sensitive information within, and the system function performed by each SDA, consideration should be given to the needs for protection of each of these attributes.

2.12. The first step in a systematic process should be to identify the functions that directly support one or more aspects of nuclear security (e.g. physical protection, nuclear material accounting and control and sensitive information management) and nuclear safety. The computer based systems and component digital assets that support those functions should then be identified.

---

[2] Malware or malicious software is any form of computer code that is intentionally designed to perform a malicious act. This might include facilitating the theft of sensitive information, compromising the design of a computer based system, or compromising a function performed by a computer based system.

2.13. An initial consequence analysis should then be conducted on the effects of compromise of the digital assets within such systems to determine those assets that, if compromised in a cyber-attack, could affect the required system functions and thereby adversely affect nuclear security. Those digital assets whose compromise could cause adverse effects are the SDAs. This concept is illustrated in Fig. 2. This initial analysis should be conducted without taking account of existing computer security measures, to determine what the 'worst case' effect would be if the digital assets were to be compromised.

2.14. The process should also include evaluation of support systems, or equipment not directly associated with nuclear security and safety functions, to determine whether cyber-attack on those systems or equipment could directly or indirectly affect nuclear security and safety functions. Any digital asset that could temporarily connect to an SDA should also be evaluated for possible classification as an SDA. Examples of such systems may include maintenance computers and digital test equipment.

2.15. Organizations may choose from a number of different strategies to manage SDAs. They may group SDAs — for example, those that belong to the same system, or those that are similar in nature — and manage all of the SDAs in a group collectively. A computer based system that performs an important function may therefore be treated as one SDA, or as a set of SDA components. Such grouping should help to ensure that similar levels of protection are provided for those SDAs for which the potential consequences of being compromised

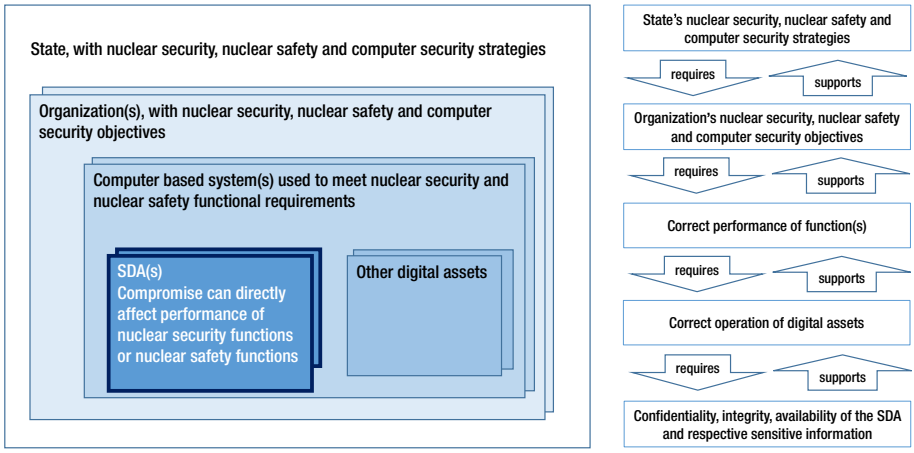


FIG. 2. Conceptual diagram of a sensitive digital asset (SDA) within a computer based system within an organization.

are similar. Once SDAs have been identified and categorized according to the potential consequences if they are compromised, a graded approach, using defence in depth, can be applied.

2.16. The requirements for confidentiality, integrity and availability of each SDA should be determined by assessing the contribution of that SDA to nuclear security and safety and the potential consequences of mal-operation of that SDA following a cyber-attack. This determination may call for judgement by a subject matter expert, guided by principles and analytical processes.

2.17. Until a computer based system has been evaluated to determine whether or not it is an SDA (or contains SDAs), it should be treated as 'unassigned'. The computer security measures for unassigned assets should usually be very stringent, as a cautious approach, because the potential effects of cyber-attack are unknown. Consideration should be given to whether to prohibit or restrict the use of such assets within the nuclear security regime. For example, use of personal devices belonging to staff, such as mobile telephones and tablet computers, may be prohibited within nuclear facilities; and connection of third party computers to any system at a nuclear facility may be prohibited until they are fully assessed. The appropriate definition of what constitutes an SDA, of its extent, boundaries and interfaces, and of acceptable degrees of dependence upon other digital assets, are key aspects of creating a secure design, calling for expert judgement guided by computer security and systems engineering principles. For example, by amending the overall system design to transfer functionality between SDAs and other digital assets, it may be possible to simplify the definition of SDAs and simplify associated computer security measures.

2.18. Particular care should be taken if using SDAs from virtual and contract services, such as cloud computing, as such services include elements that are not under the data owner's direct control. For example, an SDA that is a cloud based application or service will rely upon software and associated hardware that are under the control of the cloud operator (e.g. cloud based storage). In such cases, there should be stringent contractual requirements on matters such as access control, availability, segregation of data, data destruction, the communication interface, software, hardware and administrative processes, in order to ensure that the application is adequately protected against unauthorized access and manipulation. Contracting the provision of SDAs to another organization (i.e. outsourcing) does not remove the responsibility from the process owner or operator for the protection of that SDA.

2.19. SDAs may include components of information technology systems and operational technology systems. The appropriate computer security measures for such components will depend on the type of system and its function. However, interfaces often exist between information technology and operational technology systems, and the set of computer security measures applied to the individual systems should take account of any such interfaces.

2.20. Processes, commonly referred to as 'life cycle models', have been applied to provide assurance that SDAs fulfil their specialized requirements. Life cycle models describe the activities for the development, operation, maintenance and removal of SDAs, and the relationships between these activities. Computer security needs to be considered at all phases in the SDA's life cycle. Facilities, functions, systems, components, SDAs and other digital assets may each have their own life cycles, with interactions between them. The notional system development life cycle, set out for instrumentation and control systems, can be used as the basis for the life cycle for computer based systems, including SDAs, and should be considered in the context of the lifetime of a facility.

CYBER-ATTACK

2.21. The term 'cyber-attack' is used to describe a malicious act with the intention of stealing, altering, preventing access to or destroying a specified target through unauthorized access to (or actions within) a susceptible computer based system. Cyber-attacks jeopardize the confidentiality, integrity or availability[3] (or a combination of these properties) of the sensitive information within an SDA, or of the SDA itself, and might be used to carry out or facilitate a malicious act against a facility or activity or other criminal or intentional unauthorized act involving nuclear or other radioactive material. A closely related concept is the non-targeted attack, in which, for example, non-directed malicious codes might be inadvertently introduced into computer based systems and networks. Such an attack could also adversely affect nuclear security.

2.22. A cyber-attack can be carried out through direct physical access to the information or information assets or through electronic access, or a combination of the two, and can be carried out directly by an adversary or by (or with the assistance of) an insider knowingly or unknowingly influenced by an adversary. Cyber-attacks, once detected, should be treated as computer security incidents.

---

[3] Protection of other properties, such as authentication and non-repudiation, is assumed to be included in protecting confidentiality, integrity and availability.

2.23. Computer security incidents resulting from cyber-attacks might lead to further computer security incidents and ultimately to nuclear security events, either directly or as part of a sequence of malicious activities, which might include other cyber-attacks, or unauthorized physical access or exploitation of insiders, or a combination in a blended attack.

COMPUTER SECURITY ACROSS NUCLEAR SECURITY

2.24. The nuclear security regime addresses the three domains covered in Refs [3–5], and computer security supports the nuclear security objectives in each of these domains. The role of computer security in each of these domains is briefly described in the following sections.

Nuclear material and nuclear facilities

2.25. The physical protection of nuclear material and nuclear facilities depends on security measures to do the following [3]:

(a) Protect against unauthorized removal;
(b) Locate and recover missing nuclear material;
(c) Protect against sabotage;
(d) Mitigate or minimize effects of sabotage.

2.26. Computer based systems in nuclear facilities support process control, nuclear safety, nuclear security and nuclear material accounting and control functions. The performance of each of these functions uses SDAs that could be targeted to support a stand-alone attack or used in combination with a physical attack (e.g. a blended attack). Computer security is needed to protect these computer based systems from cyber-attacks.

Radioactive material and associated facilities

2.27. Radioactive material is used worldwide for a wide variety of purposes, including many in which nuclear material is not involved. Computer based systems are increasingly used in these industries for safety, security and operations. Security measures, including computer security measures, are needed to prevent the unauthorized access to or acquisition of such material for a malicious act, or sabotage of this material and the associated facilities.

2.28. The legislative and regulatory framework should reflect the fact that the national register of radioactive sources or radioactive material will usually contain sensitive information that needs to be secured. Computer security is needed within this domain to protect the confidentiality, integrity and availability of the sensitive information and sensitive information assets, including SDAs; for example, to support the confidentiality and integrity of registers of sources and the availability of data needed for response to incidents.

Nuclear and other radioactive material out of regulatory control

2.29. Material out of regulatory control is nuclear or other radioactive material that is present in sufficient quantity that it should be under regulatory control, but for which control is absent, either because controls have failed for some reason, or because they never existed. The security of nuclear and other radioactive material out of regulatory control is achieved by coordinated action of competent authorities to carry out their assigned functions of preventing, detecting and responding to nuclear security events. SDAs make up or support many of the systems used to perform these functions.

2.30. Computer security is needed within this domain, for example, to protect the confidentiality of sensitive information, the integrity of detection systems, the confidentiality, integrity and availability of data transmission systems, and the availability of measures supporting response, such as communications and nuclear forensics.

THREATS, VULNERABILITIES AND COMPUTER SECURITY MEASURES

Threats

2.31. A threat is a person or group of persons with motivation, intention and capability to commit a malicious act. Any individual performing or attempting to perform a malicious act is an adversary.

2.32. An understanding of the threats and risks associated with possible cyber-attacks is essential to developing effective computer security in the context of nuclear security. This includes understanding the motivation, intentions, capabilities and tactics that a nuclear security threat might have in planning and conducting a cyber-attack. Annex II provides some examples of general characterizations of nuclear security threats who might make use of cyber-attacks.

Vulnerabilities

2.33. Vulnerabilities in a computer based system or network are operational attributes that render the system open to exploitation or susceptible to a given threat. Such weaknesses might be administrative, physical or technical in nature. Through exploitation of vulnerabilities, an adversary might gain unauthorized access to or control of an SDA. The consequences associated with the exploitation of a vulnerability in an SDA can range from negligible to severe, depending on its potential to adversely affect the operation of the SDA and its function.

2.34. The complexity of both hardware and software in computer based systems is continuously increasing, as are the number of computer based systems and their interconnectivity. This complexity increases the challenge in maintaining full understanding of systems, and thus maintaining the expertise necessary for security management. The number of vulnerabilities in a system can be related to its complexity, and therefore systems should only be as complex as needed for their intended function.

2.35. The exploitation of newly discovered vulnerabilities forms the basis for many successful cyber-attacks. For example, 'zero-day attacks' are situations in which the adversary exploits a vulnerability that is previously unknown to the defender. Furthermore, the rapid evolution of new computer technologies provides opportunities for the nature of vulnerabilities to change, with entire new classes of vulnerabilities only becoming apparent after these new technologies have been adopted and become operational.

2.36. Owing to the complexity of some computer based systems and the possibility of hidden vulnerabilities in them, the available computer security measures might not be sufficient to reduce risk to an acceptable level for use in specific nuclear security and safety applications. Where measures are unable to reduce the risk to an acceptable level, alternative approaches (e.g. a different design or assignment of functions) should be considered.

A graded approach and defence in depth for computer security

2.37. Computer security measures may be technical, physical or administrative, or a combination of these. A combination of control measures should be chosen using a risk informed approach based on a graded approach and defence in depth to achieve adequate computer security. The specific computer security measures implemented may be a combination of some that are prescribed by higher level

guidance or State requirements and others determined by an operator through its own risk informed process.

2.38. Computer security levels are a way to indicate the extent and rigour of security considered necessary for different SDAs. Each level in a graded approach will need a different set of protective measures to satisfy the security requirements for that level. More stringent requirements are applied to the most critical SDAs. Figure 3 illustrates this concept.

2.39. One practical way to implement a graded approach is to group computer based systems and the associated SDAs into computer security zones, with graded computer security measures applied for each zone based on the protection requirements (i.e. level of security). Computer security levels are then assigned to specific zones based on the potential impact of cyber-attacks on functions, systems and SDAs within the zone.

2.40. The use of computer security levels, shown in Fig. 3, is a graded approach that involves identifying computer security requirements that are proportionate to the potential consequences of a successful cyber-attack. The following considerations could guide the application of this method:

(a) Higher level protection requirements would be enforced for those SDAs whose compromise could lead to the most severe consequences, including the most significant nuclear security events.

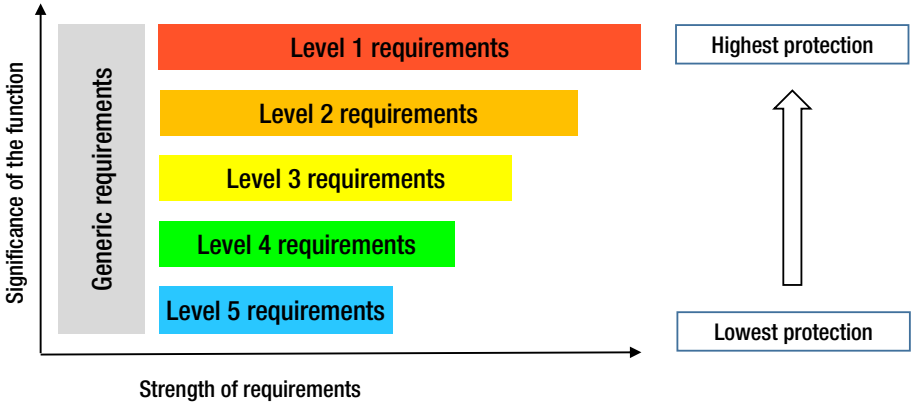


FIG. 3. Illustration of the graded approach using the computer security level concept.

(b) Lower level protection requirements would be enforced for computer based systems that have nuclear security related functions but that are not considered SDAs.
(c) Generic requirements would be enforced for all security levels and computer based systems with nuclear security related functions, and may be addressed through computer security measures that are common to computer based systems in other areas.

2.41. Computer security measures are also necessary for computer based systems that are not considered SDAs. Given the interconnectivity of computer networks and information flow, a layered approach of graded computer security requirements across all computer based systems is necessary to provide defence in depth against cyber-attacks. In the above example, computer based systems in zones with Level 4 and Level 5 requirements are likely not to be categorized as SDAs, but protective measures are applied to systems in these zones to provide layers of defence against intrusion and compromise of SDAs in zones with higher levels.

2.42. Defence in depth for computer security involves providing multiple defensive layers of computer security measures that would need to fail or be bypassed for a cyber-attack to progress and adversely affect an SDA. The appropriate combination of complementary and overlapping computer security measures provides defence in depth. Defence in depth is achieved not only by implementing multiple defensive layers, but also by implementing computer security measures that prevent, detect, protect against, respond to, mitigate the effects of and facilitate recovery from an attack on an SDA. For example, if a failure in prevention were to occur (e.g. violation of a policy prohibiting use of portable storage media) or if protection mechanisms were to be bypassed (e.g. by a new virus that is not recognized as a cyber-attack), mechanisms would still be in place to detect and respond to any unauthorized alteration in an affected SDA.

2.43. Effective defence in depth also means that, by design, no single failure of a layered computer security measure should render more than one layer invalid or ineffective. For example, exploitation of a critical vulnerability within a commonly deployed protection device could have the potential to bypass multiple layers of defence unless defence in depth provides diversity of devices, configurations or other measures. Diversity in computer security measures should be managed in such a way that there is balance between the defence in depth provided and the complexity of the system.

2.44. Defence in depth may depend on a system design comprising zones of different computer security levels, often visualized as concentric rings. A general

principle is that direct connections should only exist between adjacent computer security zones.

2.45. A contribution to effective defence in depth may also be achieved by ensuring that different parts of the operating organization have complementary roles and responsibilities in computer security, with effective separation of duties, such that any errors made by one person may be noticed by another and corrected.

2.46. Identifying threats and vulnerabilities and evaluating risk provides the risk informed basis for determining proportionate security measures. In this context, risk is the potential that adverse effects on SDAs, and consequently on nuclear security and safety, will result from nuclear security threats exploiting vulnerabilities, and thus is a function of the likelihood of an attack and the severity of its consequences. The relationship between these terms can be explained as follows in the context of computer security, as illustrated in Fig. 4:

(a) Owners of computer based systems in the nuclear security regime seek to avoid nuclear security events and thus seek to minimize risks of computer security incidents that could contribute to nuclear security events.
(b) Nuclear security threats might wish to cause nuclear security events, and might target SDAs for compromise and/or sabotage.
(c) Consequently, nuclear security threats might initiate activity that exploits vulnerabilities, thereby posing computer security risks to SDAs; those risks can lead to nuclear security events.
(d) Owners impose computer security measures to reduce computer security risks to SDAs.
(e) A risk informed approach may include considering the likelihood of particular computer security incidents when determining proportionate computer security measures. Risks can be reduced by eliminating the threat, imposing computer security measures that decrease the likelihood of an attack resulting in a computer security incident, or limiting or mitigating the severity of the effect of the computer security incident.
(f) Risk identification and the associated risk management should be continual processes responsive to changes in risk factors.

Computer security responsibilities within a nuclear security regime

2.47. Many organizations within a nuclear security regime use computer based systems for such functions as information processing, nuclear security, nuclear safety and nuclear material accounting and control.

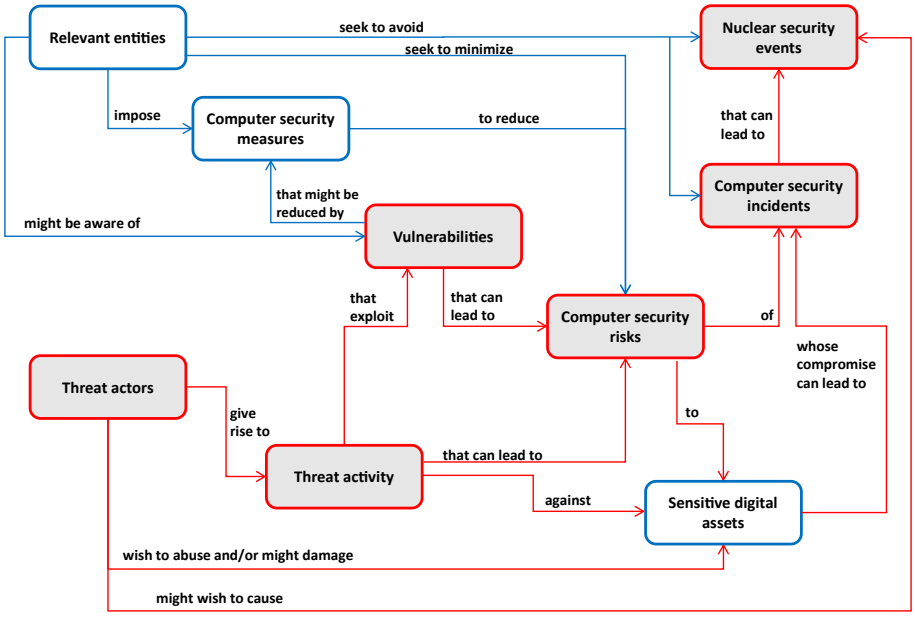


FIG. 4. Risk informed approach to computer security measures (adapted from ISO/IEC 27005:2018) [9].

2.48. Each of these organizations has the responsibility for the protection of sensitive information held within such systems and the associated SDAs.

2.49. Figure 5 provides a visualization of the organizations in a nuclear security regime that might have computer security responsibilities. These include competent authorities[4] and operators[5], which have responsibilities for computer security in the nuclear security regime that are assigned through national legal and regulatory requirements.

2.50. The State may have a designated competent authority (or authorities) for computer security, which may be different from the competent authorities with responsibilities for nuclear security. Further, competent authorities may have

[4] Competent authorities also include police, rescue, border guard and defence forces that have a role in securing facilities and activities and in detection and response to incidents involving nuclear and other radioactive material out of regulatory control.

[5] The term 'operators' in this publication refers to the range of licensed entities in a nuclear security regime, including operators of facilities and activities involving nuclear material or other radioactive material, shippers and carriers.

computer security requirements dictated by national legal requirements and standards outside of the nuclear security regime.

2.51. Vendors, contractors and suppliers include organizations that provide goods and services to competent authorities and operators, but whose computer security responsibilities (e.g. to protect sensitive information and associated SDAs) may be derived not from national legal and regulatory requirements, but from conditions specified in their contracts with competent authorities and operators.

2.52. The computer security related roles and responsibilities of the State, competent authorities and operators, and those of vendors, contractors and suppliers are further explained in Sections 3 and 4.

COMPUTER SECURITY COMPETENCES AND CAPABILITIES

2.53. Effective and robust computer security is implemented, maintained and sustained by competent and trustworthy staff with effective management and active, well informed leadership. Each organization within the nuclear security regime should, according to its particular roles and responsibilities, develop and sustain computer security competences and capabilities.

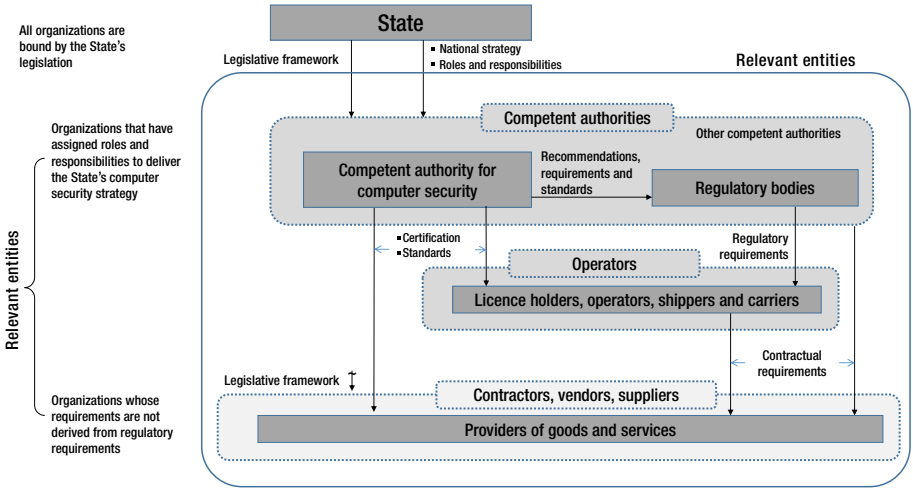


FIG. 5. Organizations having computer security responsibilities within a nuclear security regime.

3. ROLES AND RESPONSIBILITIES OF THE STATE

3.1. The State should develop and maintain a national computer security strategy as part of its nuclear security regime (referred to in the remainder of this publication as 'the strategy'). The State should designate a competent authority as having lead responsibility in the development of the strategy.

LEGISLATIVE AND REGULATORY CONSIDERATIONS

3.2. The State should ensure that computer security is appropriately addressed in a legislative and regulatory framework that is applicable to and consistent with the nuclear security regime. The State should incorporate within its national law appropriate requirements for computer security that will ensure the proper implementation of computer security within nuclear security.

3.3. The State should ensure that its legislation criminalizes cyber-attacks on computer based systems within the nuclear security regime. Computer security may need special legislative provisions to take into account the unique characteristics of some offences and modes of operation associated with cyber-attacks.

3.4. The State should ensure that sanctions for criminal or intentional unauthorized acts against SDAs that could jeopardize nuclear security are part of its legislative or regulatory framework.

3.5. The State should consider examples from other laws and international legal instruments (such as conventions) to assist it in defining computer security and its implementation as it relates to nuclear security. These may include the following:

(a) Laws concerning computer offences;
(b) Laws on terrorism;
(c) Laws on the protection of critical national infrastructure;
(d) Laws mandating disclosure of information;
(e) Laws on privacy and handling of personal information;
(f) International instruments, such as conventions, on cybercrime.

3.6. The State should continuously review and update its legislative and regulatory framework to include provisions for new and emerging cyberthreats and vulnerabilities.

3.7. The State should designate a lead competent authority for computer security[6], with responsibility for oversight and enforcement of computer security laws and regulations as applied to the nuclear security regime (hereafter referred to as the "competent authority for computer security").

3.8. The State may choose to implement a computer security legislative and regulatory framework that is not limited to the nuclear security regime, and some laws and regulations may have scopes that extend beyond the nuclear security regime. In such cases, the competent authority for computer security should ensure that the framework is sufficient for nuclear security and, if not, the State should supplement this framework with any necessary requirements in a manner coherent with the nuclear security regime.

3.9. The State should ensure that sufficient financial, human and technical resources are available to competent authorities for them to fulfil their responsibilities for correctly interpreting and implementing their legal obligations relating to computer security in the State's nuclear security regime.

COMPETENT AUTHORITY FOR COMPUTER SECURITY IN THE NUCLEAR SECURITY REGIME

3.10. Depending on the organization of the State, the competent authority for computer security in the nuclear security regime might or might not be the regulatory body for nuclear security. Similarly, the responsibilities regarding computer security within the State may be shared between several organizations, but the State should designate one specific competent authority to have responsibility for computer security in each specific area of the nuclear security regime. For example, the competent authority for computer security for nuclear power plants may be different from the competent authority for computer security in border monitoring operations.

3.11. When there is more than one competent authority for computer security in the nuclear security regime, or it is different from the competent authority responsible for nuclear security, the State should establish and maintain

[6] A State may assign this responsibility to different competent authorities in different contexts; for example, the competent authority responsible for computer security in nuclear facilities may be different from that responsible for computer security in medical practices or in border monitoring. In this publication, the term 'competent authority' is used to refer to whichever such authority has responsibility in a particular context.

an appropriate coordinating body or mechanism to ensure clarity in the responsibility and accountability for every aspect of computer security across all competent authorities.

3.12. The State should identify all the competent authorities[7] and operators with roles and responsibilities relating to computer security in the nuclear security regime and ensure that each such organization falls under the oversight of the appropriate competent authority for computer security in the nuclear security regime.

3.13. The State should require the identified competent authorities and operators to develop and implement CSPs in accordance with the strategy.

3.14. The State should define and assign computer security responsibilities to all relevant entities in the nuclear security regime.

3.15. Annex III offers an example list of nuclear security responsibilities from which computer security assignments may be inferred, according to the nature of the State's nuclear security regime and its SDAs.

3.16. Some supporting organizations might not be within the authority of the State's regulatory bodies, but have a critical role in achieving nuclear security objectives with respect to computer security. The responsibilities and computer security requirements for such organizations may be defined via contractual agreements such as are used with vendors, contractors and suppliers. The State may assign computer security requirements (e.g. relating to design, performance and staff training) for specific computer based systems and to vendors, contractors and suppliers in the nuclear security regime, in accordance with the strategy.

INTERFACES WITH OTHER DOMAINS

3.17. The State should ensure that interfaces between computer security and other domains operate effectively. This may demand action by the State that is outside the scope of computer security (e.g. placing requirements on the other domains).

3.18. The State should ensure that the strategy defines the interfaces between computer security and all other relevant domains in order that respective

[7] Competent authorities to be considered include, as appropriate, any coordinating body or mechanism, law enforcement, customs and border control, intelligence and security agencies, and health and environment agencies.

competent authorities and operators understand their roles and responsibilities for those interfaces.

Nuclear safety

3.19. Nuclear security and nuclear safety have in common the aim of protecting people, property, society and the environment. Security measures and safety measures have to be designed and implemented in an integrated manner to develop synergy between these two areas and also in a way that security measures do not compromise safety and safety measures do not compromise security [1].

3.20. Computer security plays an important role in the interface between nuclear security and nuclear safety, especially in view of the increasing reliance on computer based systems within all operational aspects of nuclear facilities.

3.21. The State should consider the regulations for nuclear security and nuclear safety when preparing the regulations on computer security and ensure that these regulations are implemented in a coherent manner.

3.22. Any nuclear safety function that relies upon or is supported by a computer based system will depend on the integrity and availability of the associated information (including software) — and, where necessary, its confidentiality — for its proper operation. Therefore, computer security should be implemented as an integral part of the life cycle processes of computer based systems used for nuclear safety, to ensure that computer security and nuclear safety requirements are considered together.

3.23. There should be a consistent and rational relationship between the safety classes and computer security levels assigned to digital assets, to ensure that a digital asset assigned to a particular safety class has the appropriate computer security protection, but there is not necessarily a simple equivalence between safety classes and computer security levels. Furthermore, some digital assets without a formal safety classification might nevertheless be significant to safety from a security perspective, and thus be SDAs. The determination of the appropriate computer security level will depend on the system function and the particular digital asset within the context of the system and the organization. This determination will necessitate the appropriate competences and capabilities, using judgement based on agreed principles.

3.24. Implementation of computer security measures should not adversely affect the performance, effectiveness, reliability or operation of nuclear safety functions.

3.25. The Appendix describes further considerations for the State when addressing interfaces with nuclear safety.

Physical protection

3.26. Physical protection systems, such as those systems providing physical access control, security monitoring and detection, and alarm and response functions, often rely on computer based systems. Malicious compromise of these computer based systems (i.e. compromise of the confidentiality, integrity and/or availability of the information in them) could degrade the functioning of the physical protection system and could facilitate physical actions aimed at unauthorized removal of material or sabotage. Computer security should be implemented as an integral part of the life cycle processes of computer based systems used for physical protection functions or systems.

3.27. Physical protection systems, such as physical access control, might also be valuable contributors to computer security and should be considered for protection of computer based systems.

3.28. Some States may treat computer security as part of physical protection, as defined in Ref. [3]. This publication treats computer security as a separate topic, distinct from physical protection, to clarify and emphasize the differences. The nature of the interface with physical protection will depend on the circumstances in each State.

3.29. Implementation of computer security measures should not adversely affect the performance, effectiveness, reliability or operation of physical protection system functions.

Information technology and operational technology functions

3.30. The responsibilities for the management and security of information technology systems and of operational technologies (including industrial control and instrumentation and control systems) are often in different departments within an organization. Effective interface and collaboration between these groups is essential for comprehensive security. Past cyber-attacks have involved the use of information technology systems as both a resource for reconnaissance and a means for attack against operational technologies.

3.31. There might be differences of procedures, vocabulary and risk assessment between those responsible for information technology systems and those

responsible for operational technologies. Effective collaboration between them is essential to avoid misunderstandings and inconsistent application of computer security measures.

Intelligence organizations

3.32. The State should ensure that intelligence organizations provide appropriate support to contribute to or maintain an accurate and up to date national threat assessment that includes the threat of cyber-attacks against the nuclear security regime. Protocols and processes should be in place to support the transfer of information on cyberthreats to relevant entities within the nuclear security regime as appropriate to ensure adequate computer security against changing threats.

3.33. The State should ensure that intelligence organizations have knowledge of the role of computer security in the nuclear security regime, including knowledge of the types of SDAs that might exist and their significance.

Response organizations

3.34. The State should ensure that nuclear security systems and measures are in place at all competent authorities and operators in order to detect and assess computer security incidents that have actual or potential implications for nuclear security, and that relevant competent authorities are notified of such incidents so that appropriate response action can be initiated.

3.35. Contingency plans should include provisions for responding to cyber-attacks and blended attacks.

International assistance and cooperation (including information exchange)

3.36. States are encouraged to cooperate with each other and with international organizations, when appropriate, in order to secure SDAs and associated sensitive information and in order to identify threats of cyber-attack, especially credible threats of sabotage of nuclear material or a nuclear facility (e.g. pursuant to Article 5(3) of the Convention on the Physical Protection of Nuclear Material as amended [2]). Confidence building and improved computer security can be achieved through sharing and analysing information regarding vulnerabilities, threats and computer security incidents in a timely manner. The confidentiality of such information should be appropriately protected.

3.37. The State should establish secure and controlled information sharing mechanisms to coordinate response to cyber-attacks on the State's nuclear security regime. International cooperation and assistance is encouraged to support the investigation of cyber-attacks and the prosecution of offenders.

3.38. The State is encouraged periodically to engage advisory or assessment services to evaluate its strategy and CSPs and their implementation in the State's nuclear security regime.

4. ROLES AND RESPONSIBILITIES OF COMPETENT AUTHORITIES AND OPERATORS

4.1. Computer security is a cross-cutting issue for the competent authorities and operators in a nuclear security regime. All such organizations have some level of responsibility in the protection of SDAs.

4.2. Competent authorities and operators are both generators and users of sensitive information, which is often processed by, stored on or integral to SDAs under their control. Competent authorities and operators should implement computer security measures to protect such SDAs and associated sensitive information.

4.3. Competent authorities and operators should identify their SDAs, characterize these SDAs based on the potential effect of their compromise on nuclear security and nuclear safety, and define within their CSPs the level of computer security measures required for each of those SDAs.

4.4. Competent authorities and operators should implement computer security measures to protect the confidentiality, integrity and availability of SDAs and the sensitive information they contain. For example, computer security measures should have the following characteristics:

(a) They should be designed to deny unauthorized access, by persons, processes or equipment, to SDAs (in accordance with a graded approach).
(b) They should ensure that malicious code or data are not introduced into SDAs.
(c) They should be integrated into supply chain management arrangements.

4.5. Competent authorities and operators should use a formal process to ensure that only personnel determined to be competent and trustworthy are authorized to perform activities related to computer security.

4.6. Competent authorities and operators should permit personnel whose trustworthiness has not been determined to perform these activities only in exceptional cases and only where robust compensating security measures are in place to prevent or detect unauthorized acts.

4.7. Competent authorities and operators should assess and manage the computer security related interfaces between nuclear security and safety [4] in a manner to ensure that security measures and safety measures do not adversely affect each other and, to the degree possible, are mutually supportive.

4.8. Each competent authority and operator should maintain a CSP that describes how it will provide adequate computer security, as required by the State and its competent authority for computer security. If different organizations share or depend on each other's SDAs, all shared responsibilities or dependencies should be reflected in their respective CSPs.

4.9. Competent authorities and operators should periodically evaluate their computer security measures to ensure that they comply with regulatory requirements. The period between such evaluations should be set to promptly take into account any changes in the threat, or other factors affecting the risk. These evaluation activities may include audits, reviews, performance testing and exercises, as appropriate. Competent authorities and operators should also conduct self-evaluations when computer based systems are modified, to consider whether the modifications might introduce new vulnerabilities and/or create new SDAs.

WORKING WITH VENDORS, CONTRACTORS AND SUPPLIERS

4.10. Competent authorities and operators should place contractual requirements on vendors, contractors and suppliers to implement computer security measures that are commensurate with their role. The contractual requirements should specify computer security measures to ensure that activities of neither party provide a pathway for cyber-attack on the other and that both parties' sensitive information is appropriately protected.

4.11. Competent authorities and operators, and their vendors, contractors and suppliers, should maintain protocols and procedures for the timely communication of information about computer security incidents.

COMPETENT AUTHORITY FOR COMPUTER SECURITY

4.12. The competent authority for computer security should define computer security requirements, standards and recommendations suited to each competent authority or operator based on a risk informed, graded approach.

4.13. The competent authority for computer security should ensure that these requirements reflect the strategy, and the particular operational and security requirements and demonstrated capabilities and competences of the relevant competent authority or operator.

4.14. The competent authority for computer security should use a risk informed approach [1], based on a graded approach and defence in depth, in achieving adequate computer security.

4.15. Each competent authority should ensure that all operations throughout the life cycle of SDAs for which they have responsibilities (e.g. design, implementation, maintenance and final disposition) are appropriately controlled, monitored and documented.

4.16. Each competent authority should verify continued compliance with its computer security regulations through regular evaluations and, when necessary, ensure that corrective actions are taken.

4.17. The competent authority for computer security may prescribe specific computer security measures for the competent authorities or operators to implement based upon its assessment of risk (i.e. a prescriptive approach). Alternatively, the competent authority for computer security may define performance based requirements for computer security, allowing the competent authorities or operators to use a risk informed approach to determine proportionate computer security measures. The competent authority for computer security may also employ a combination of the two approaches.

4.18. The criteria for the selection of a prescriptive approach or a performance based approach (or an appropriate combination of the two) will depend on the

State's legislative framework and organizational structure and several other factors such as the following:

(a) The competence of the operator to interpret performance requirements and to design, implement and evaluate an effective nuclear security system;
(b) The number and variety of different facilities and operators that will be governed by the regulation, and the extent to which prescriptive requirements might limit the flexibility of the operator to develop appropriate measures;
(c) The severity of the potential consequences of the malicious acts that are to be prevented or protected against [10].

Prescriptive approach

4.19. In the prescriptive approach, the competent authority for computer security establishes specific computer security measures that it considers necessary to meet its defined computer security objectives.

4.20. Advantages of the prescriptive approach include simplicity in implementation for both the competent authority for computer security and the relevant competent authority or operator, elimination of the need to share sensitive information, and ease of inspection and evaluation. The use of the prescriptive approach might be particularly appropriate in cases where both the threat level and potential consequences are low. The prescriptive approach might also be more appropriate in cases where conducting a detailed threat assessment or establishing a design basis threat (DBT) is not practicable.

4.21. The prescriptive approach might lack flexibility to address specific circumstances. Furthermore, with this approach the relevant competent authority does not have the responsibility to ensure that the computer security measures implemented are sufficient; the prime responsibility for addressing risks belongs to the competent authority for computer security, as it prescribes exactly what computer security measures are needed to address the cyber-attack threat. The relevant competent authority or operator only has the responsibility for implementing the prescribed computer security measures.

Performance based approach

4.22. In the performance based approach, the competent authority for computer security defines computer security objectives and requires the competent authorities or operators to design and implement computer security measures that

meet those objectives, achieving a specified level of effectiveness in protecting against cyber-attacks and providing contingency responses.

4.23. The performance based approach allows flexibility for the competent authorities or operators to propose an organization specific combination of computer security measures. The adequacy of these measures is tested against the threat assessment or DBT, to ensure that the set of performance based measures meets the objectives. An advantage of the performance based approach is that it recognizes that many different combinations of computer security measures can achieve effective computer security, and that each organization and its operational circumstances might be different.

4.24. The performance based approach depends on both the competent authority for computer security and the competent authorities or operators having sufficient competences and capabilities in computer security to establish requirements and implement computer security measures. The performance based approach may involve the State providing sensitive information from the threat assessment or DBT to the respective competent authorities and operators.

Combined approach

4.25. The combined approach includes elements from both the prescriptive and performance based approaches. There are many ways of applying the combined approach, of which two are the following:

(a) The State may require application of a performance based approach for circumstances where the potential impact is high or very high, while allowing application of a prescriptive approach where the potential impact is low or very low;
(b) The State may impose a set of prescriptive requirements that are to be followed to address certain defined aspects of computer security (e.g. the protection of sensitive information), while supplementing computer security measures to address all other aspects derived using the performance based approach.

4.26. The main advantage of the combined approach is the flexibility it allows. The limitations of a combined approach are similar to those associated with the performance based and prescriptive approaches and depend on the specific implementation. However, a well executed combined approach might provide an appropriate balance and reduce the effects of the limitations associated with each approach.

REGULATORY BODY

4.27. The regulatory body[8] for nuclear security should establish regulatory requirements for computer security measures to protect SDAs and the associated sensitive information. The regulatory body should ensure through regulations that the relevant entities perform their computer security responsibilities in accordance with regulatory requirements.

4.28. The regulatory body should ensure that its regulations are sufficiently flexible to be adaptable to the changing nature and circumstances of computer based systems, cyber-attacks and computer security measures.

4.29. It is suggested that the regulatory body issue a guide to its regulations in the area of computer security to assist relevant entities with implementation. The guide should periodically be reviewed to ensure that it adequately addresses the cyberthreat and objectives of the regulations.

4.30. The regulatory body should ensure that computer security is part of evaluation and licensing or other procedures to grant authorization to licensees.

4.31. The regulatory body should ensure that each operator has a CSP that describes its computer security measures.

4.32. The regulatory body should verify continued compliance with regulatory requirements and licence conditions relating to computer security through regular inspections and, when necessary, the use of enforcement measures for ensuring that timely corrective action is taken.

---

[8] There may be more than one regulatory body within a State, each having responsibility for nuclear security in different contexts; for example, the regulatory body responsible for nuclear security in nuclear facilities may be different from that responsible for nuclear security in industries using radioactive sources. In this publication, the term ‘regulatory body’ is used to refer to whichever such body has responsibility in a particular context. The regulatory body for nuclear security may also be the competent authority for computer security, in which case the guidance in the previous subsection also applies to it.

5. ESTABLISHING THE COMPUTER SECURITY STRATEGY

COMPUTER SECURITY STRATEGY FOR THE NUCLEAR SECURITY REGIME

5.1. The strategy[9] sets the high level computer security goals of the State's nuclear security regime, to be reflected in lower level documents that will be used in implementing the strategy. The strategy needs to be enforceable, achievable and auditable.

5.2. The strategy should include the following items:

(a) How threat assessment is performed, including the identification of possible cyber-attack scenarios;
(b) How computer security objectives are determined;
(c) How competences and levels of capability in computer security can be specified;
(d) Assignment of computer security roles and responsibilities for all competent authorities and operators (and possibly for vendors, contractors and suppliers);
(e) Identification and establishment of new organizations or adaptation of computer security roles for existing organizations where capability gaps exist;
(f) Approaches for implementation, integration and coordination of competent authorities' and operators' computer security activities;
(g) Measures to sustain computer security capabilities within the nuclear security regime.

5.3. Sections 5–8 provide further guidance on these items, which the strategy should document.

5.4. This section describes the preparatory activities that the State and its competent authority for computer security should undertake to establish the strategy, including the following:

(a) Performing a threat assessment;

---

[9] The State may choose to put some sensitive information into appendices to the strategy, so that the distribution of that information can more conveniently be limited.

(b) Assessing the impact on nuclear security of a cyber-attack on SDAs;
(c) Determining whether to use the prescriptive or the performance based approach to regulate computer security, or a combination of the two;
(d) Specifying a framework for capabilities and competences in computer security;
(e) Implementing (integration and coordination) competent authorities' and operators' computer security activities.

ASSESSMENT OF CYBERTHREAT TO THE NUCLEAR SECURITY REGIME

5.5. The State should maintain an up to date assessment of threats to its nuclear security regime [1, 5]. This information can be used to develop a national threat statement or DBT.

5.6. The State's threat assessment and/or DBT should include potential adversaries using cyber-attacks, including the possible use of insiders in such attacks, and blended attacks.

5.7. Cyber-attacks allow the adversary to initiate a malicious act from outside the target site or even from outside the national jurisdiction of the target site. The State should therefore consider international threats in its assessment.

5.8. The State should ensure that the threat assessment relating to cyber-attack (cyberthreat assessment) is updated regularly. The frequency of review of the threat assessment should reflect the rapidly evolving nature of technologies, advances in computer based systems, newly discovered vulnerabilities, and the changing nature of potential cyber-attacks and corresponding computer security approaches.

5.9. The State should ensure that changes to the threat assessment relating to cyber-attack are communicated to relevant competent authorities and operators in a timely and secure manner.

5.10. The State should take all reasonable steps to take account of the changing nature of the cyberthreat, and to encourage computer security measures that anticipate or readily adapt to such changes and thereby remain effective.

5.11. In addition to national intelligence agencies, other competent authorities, operators, vendors, contractors and suppliers might possess information that can provide input to the threat assessment.

5.12. The State may define protocols for the secure sharing of threat information, including direct communications between organizations.

5.13. Competent authorities and operators cannot be expected to protect against all levels of threat. Above a certain threat level, the State is expected to respond in support of the competent authority or operator (Fig. 6). For competent authorities and operators using a DBT, this is often referred to as a 'beyond DBT event'.

5.14. The State should ensure that the threat assessment and/or DBT for computer security provides sufficient detail for the subsequent risk assessments, which in turn will lead to appropriate and effective implementation of computer security across the State's nuclear security regime.

5.15. The State, via the competent authority for computer security, should identify criteria, processes and resources for responding to cyber-attacks against competent authorities and operators and their vendors, contractors and suppliers. These processes should include secure communication protocols with the response organization.

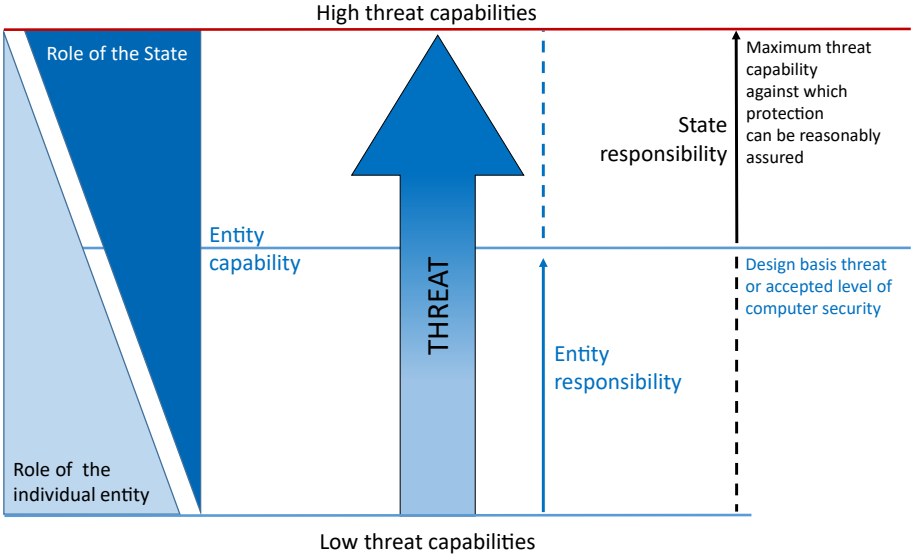


FIG. 6. Roles and responsibilities for protecting against threats.

ASSIGNING A COMPETENT AUTHORITY FOR CYBERTHREAT ASSESSMENT

5.16. The State should ensure that an assessment of the threat of cyber-attacks is performed in a regular and timely manner. The State should assign to this role a competent authority with expertise relevant to cyberthreat identification and assessment. The competent authority for cyberthreat assessment may be different from the competent authority for computer security.

5.17. In carrying out its functions, the competent authority for cyberthreat assessment should consult and cooperate with all competent authorities and operators identified by the State as having roles and responsibilities in cyberthreat assessments and having competences and capabilities in a formalized cyberthreat assessment process. The competent authority should lead the process of coordinating and combining these different inputs to the assessment of threats of cyber-attack.

5.18. The competent authority for cyberthreat assessment should be responsible for ensuring that the cyberthreat assessment provides sufficient detail for the subsequent risk assessments that will be used in designing appropriate and effective implementation of computer security measures across the State's nuclear security regime.

ASSESSMENT OF THE IMPACT ARISING FROM MAL-OPERATION OF SDAs

5.19. The competent authority for computer security should identify, for each relevant competent authority and operator, the severity of potential consequences of cyber-attacks they are required to prevent through effective computer security measures.

5.20. Assessment of the severity of consequences should be based upon the inherent characteristics and attributes of the SDAs. The competent authorities and operators should consider the severity of consequences independently of their likelihood and of the type of cyber-attack that might lead to their occurrence.

5.21. Figure 7 provides a visualization of the different impact levels for different types of nuclear security event across the domains of nuclear security covered by Refs [3–5]. The competent authority for computer security should identify

the severity of the consequences and assess the adequacy of computer security measures for assuring prevention or mitigation of those consequences.

5.22. The competent authority for computer security could identify, in cooperation with other relevant competent authorities, the level of protection to be required for each level in the severity of consequences.

5.23. The implementation of effective computer security needs a range of competences and levels of capability to suit the roles and responsibilities of each competent authority, operator, vendor, contractor and supplier. Where decisions and actions based on judgement are needed, the levels of capability will necessarily need to be higher. Effective computer security includes specifying these competences and levels of capability for each competent authority, operator, vendor, contractor and supplier and gaining assurance that they are being maintained and applied.

5.24. The competent authority for computer security should establish a framework of computer security competences and levels of capability. An example framework is provided in Annex IV.

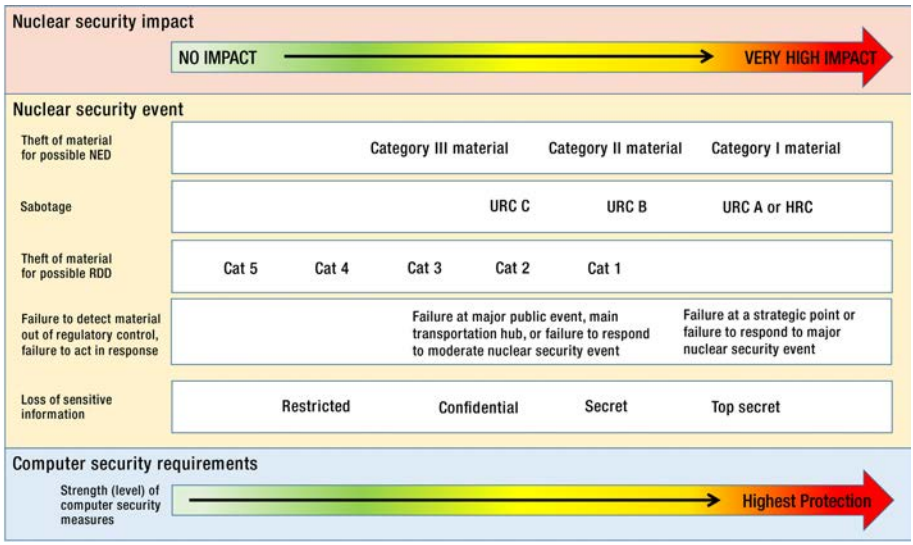


FIG. 7. Illustration of varying severity of consequence for different types of nuclear security event (the scales of impact are independent and the severity of each impact should be evaluated separately). HRC — high radiological consequences, NED — nuclear explosive device, RDD — radiological dispersal device, URC — unacceptable radiological consequences.

5.25. The framework should ensure that the computer security competences and levels of capability required for each competent authority, operator, vendor, contractor and supplier are appropriate to meet their respective responsibilities for computer security. Further guidance on defining roles, developing and maintaining competences within organizations, and capacity building relating to organizations and individuals is available in other IAEA Nuclear Security Series publications [3, 11].

RISK ASSESSMENT METHOD TO DETERMINE COMPUTER SECURITY MEASURES

5.26. The application of computer security measures should be based upon a risk informed approach. The competent authority for computer security should define a risk assessment method or sequence of methods by which responsible organizations do the following:

(a) Determine whether each computer based system provides a relevant function for the nuclear security regime;
(b) Determine whether each digital asset is an SDA;
(c) Perform a computer security risk analysis to determine the required strength of computer security measures for that SDA or other digital asset, as illustrated in Fig. 3.

5.27. The method should take into account the following:

(a) Any relevant legislation or regulation;
(b) The importance of the SDA's functions, including the importance of protecting the confidentiality, integrity and availability of the SDA and of its sensitive information, for both nuclear security and safety (i.e. its safety classification);
(c) An assessment of the consequences of cyber-attacks against that SDA;
(d) The operating environment for the SDA;
(e) Identification and assessment of the threats relevant to the competent authorities and operators, and their vendors, contractors and suppliers, and to the SDA according to the national threat assessment or DBT or threat statement;
(f) The attractiveness of the SDA to nuclear security threats;
(g) The intrinsic vulnerabilities of the SDA.

5.28. The competent authority for computer security may modify the results of the risk assessment based on the potential impact if the SDA is compromised, specifically whether this results in any of the following:

(a) The SDA's function becoming indeterminate;
(b) The SDA developing unexpected behaviours or actions;
(c) Failure of the SDA;
(d) The SDA performing as expected (i.e. being fault tolerant).

5.29. The risk assessment should consider all aspects of security collectively in order to address blended attacks, which can combine physical protection (including personnel, especially insiders) and computer security cyber-attacks. Accordingly, those conducting the risk assessment should have access to individuals with all relevant competences, such as those related to physical protection, computer security for nuclear security and safety.

6. IMPLEMENTING THE COMPUTER SECURITY STRATEGY

6.1. This section describes the responsibilities of the competent authority for computer security in assigning computer security roles and responsibilities to competent authorities or operators.

6.2. These roles and responsibilities should be documented in the strategy or supporting documents.

6.3. The competent authority for computer security may establish requirements in the form of standards, regulatory requirements via a regulatory body, or contractual requirements for vendors, contractors or suppliers, and may provide guidance documents to indicate how these requirements should be met.

ASSIGNMENT OF COMPUTER SECURITY RESPONSIBILITIES

6.4. The competent authority for computer security should ensure that all competent authorities and operators that operate SDAs are assigned the prime responsibility for the computer security of those SDAs and of any of their other

digital assets the compromise of which could adversely affect nuclear security or nuclear safety.

6.5. The competent authority for computer security should ensure that all relevant competent authorities, operators, vendors, contractors and suppliers involved in the life cycle of SDAs are assigned appropriate responsibilities for the computer security of those SDAs.

6.6. The competent authority for computer security should ensure that there is appropriate sharing of responsibilities between the State and the competent authorities and operators to ensure that the risks from the nuclear security threats with the highest capabilities are kept to an acceptable level.

6.7. The competent authority for computer security should ensure that relevant competent authorities and operators plan for and address computer security throughout the detection of and response to any computer security incident.

RELATIONSHIPS BETWEEN COMPETENT AUTHORITIES AND OPERATORS

6.8. The competent authority for computer security should make provision for the coordination of computer security responsibilities between competent authorities and operators in the nuclear security regime and those outside it. For example, there may be national authorities responsible for computer security outside the nuclear security regime, which will necessitate coordination with authorities within the nuclear security regime.

6.9. The competent authority for computer security should establish clear lines of communication between the competent authorities and operators, and, if applicable, the coordinating body or mechanism referred to in para. 3.11.

6.10. The competent authority for computer security should ensure that a mechanism exists for cooperation, coordination, information exchange and, where appropriate, integration of computer security activities between competent authorities and operators.

6.11. When assigning responsibilities for computer security to competent authorities and operators, the competent authority for computer security should balance the competing demands of the need for defence in depth and the efficient

and effective use of resources available to the State's nuclear security regime, taking account of the following considerations:

(a) Independence contributes to defence in depth because independent design and operational choices are less likely to allow for common cause or common mode failures. Independence includes both functional and financial independence from the organizations regulated and from any other bodies that deal with the utilization of nuclear material or other radioactive material. The competent authority for computer security should ensure that competent authorities and operators have sufficient competences and levels of capability to support independence in their decision making on computer security.
(b) The sharing of capabilities can improve efficiency and effectiveness in the utilization of resources. For example, a competent authority or operator may rely on another competent authority in specialized areas of computer security forensics because that competence is infrequently needed. In such a case, an agreement between the relevant entities should specify an agreed response time to provide support when requested. The competent authority for computer security should ensure that appropriate arrangements are in place to ensure the effectiveness and timeliness of support in cases where competent authorities and operators need support from other competent authorities.

6.12. When considering the balance between independence and interdependence of competent authorities and operators, the competent authority for computer security should consider the resources needed to protect against and respond to blended attacks, which may involve the combination of computer security measures with other nuclear security measures (e.g. physical protection response forces), that might be provided by other competent authorities.

6.13. The assigning of responsibilities and competences and levels of capability may identify a need for the creation of new organizations or the modification of existing organizations.

COMPUTER SECURITY COMPETENCES AND CAPABILITIES

6.14. The competent authority for computer security should require competent authorities and operators to perform an analysis of their computer security objectives to derive a comprehensive list of the required competences for their organizations. The competent authority for computer security may choose to

conduct this analysis itself, particularly where the competent authority or operator mostly applies computer security measures prescribed by the competent authority for computer security.

6.15. The competent authority for computer security should require competent authorities and operators to demonstrate that they have the necessary competences at the appropriate levels of capability to fulfil the computer security responsibilities placed on them. Annex III illustrates typical assignment of responsibilities to competent authorities, and Annex IV provides an example framework of competences and levels of capability.

6.16. The competent authority for computer security should require competent authorities and operators to demonstrate that all individuals with computer security responsibilities are trustworthy, are appropriately trained, and have sufficient skills and competence in their job functions and appropriate awareness of the threat from cyber-attacks.

6.17. The competent authority for computer security should require competent authorities and operators to implement continuing training programmes that develop and sustain the competences necessary to meet their computer security responsibilities.

6.18. The competent authority for computer security should encourage competent authorities and operators to assess their own levels of capability in the competences relevant to their responsibilities to support development and evolution of their competences.

6.19. The competent authority for computer security should conduct assurance activities to evaluate competent authorities' and operators' training and skills in computer security. The competent authority for computer security should place requirements on each competent authority and operator to demonstrate continuing maintenance of its designated competences and levels of capability in computer security commensurate with its assigned responsibilities for computer security.

RESPONDING TO COMPUTER SECURITY INCIDENTS

6.20. The competent authority for computer security should require competent authorities and operators to develop, implement and exercise computer security procedures for the prevention and detection of and response to computer security incidents.

6.21. The competent authority for computer security should provide guidance to competent authorities and operators on identification of incidents that might constitute computer security incidents. Computer security incidents might also be nuclear security events, for example the theft of sensitive information or the disruption of nuclear security or nuclear safety functions. Furthermore, cyber-attacks might form part of blended attacks. Successful detection of subtle or covert cyber-attacks might provide advance indicators of possible adversary intentions.

6.22. The competent authority for computer security should ensure that competent authorities and operators and relevant response organizations have appropriate response capabilities to address computer security incidents, and that these organizations define the circumstances under which these capabilities would be activated within their CSPs.

6.23. The competent authority for computer security should define requirements for timely reporting of computer security incidents to the regulatory body for nuclear security and/or other relevant competent authorities.

6.24. The competent authority for computer security should ensure that a competent authority or operator with sufficiently advanced capabilities (e.g. one that is competent in computer security forensics) performs the technical characterization of any computer security incident involving an SDA.

EXERCISES

6.25. The competent authority for computer security should ensure that nuclear security exercises are held with a computer security component to evaluate the State's ability to respond to computer security incidents, including blended attacks.

6.26. The competent authority for computer security should ensure that competent authorities and operators conduct regular computer security exercises to train participants and validate their CSPs, including contingency plans. Where appropriate, these exercises should be integrated with other nuclear security exercises, and should periodically be conducted jointly with emergency exercises.

ASSURANCE ACTIVITIES

6.27. The competent authority for computer security should conduct assurance activities to ensure the effective implementation of computer security across the

State's nuclear security regime and verify that the implemented computer security measures provide a level of protection that is consistent with the threat assessment and the State's determination of acceptable risk.

6.28. The competent authority for computer security should provide formal and regular assurance to the State that sufficient computer security competence and levels of capability exist in all competent authorities and operators.

Security qualification of parts and services

6.29. Competent authorities, operators and their respective vendors, contractors and suppliers need to have assurance that equipment, parts and services procured have computer security measures in place to prevent the introduction of vulnerabilities, including the direct introduction of malicious software or pathways for cyber-attack.

6.30. Competent authorities and operators should ensure that their vendors, contractors and suppliers that contribute to SDAs for which they are responsible implement the relevant computer security requirements (e.g. secure software development) with the aim of minimizing vulnerabilities in SDAs and preventing the use of the supply chain as a pathway for cyber-attack. This includes reviewing the methodologies, processes and equipment of the vendors, contractors and suppliers.

6.31. The competent authority for computer security may designate national or international standards for use by competent authorities, operators, vendors, contractors and suppliers in procurement specifications for SDAs and associated services. Such standards should refer to all phases of the life cycle of an SDA.

6.32. The competent authority for computer security may designate a certifying authority to undertake activities to provide assurance that those vendors, contractors and suppliers who design, provide and support SDAs follow required computer security practices.

6.33. Competent authorities and operators are encouraged as appropriate to undertake further assurance checks, such as factory acceptance testing and computer security inspections and/or audits (based on contractual requirements), on the vendors, contractors and suppliers.

6.34. The competent authority for computer security should ensure that the necessary relationships exist with counterpart authorities in other States and with international bodies to allow effective use of international cooperation and assistance, where appropriate, to support computer security relating to nuclear security regimes. The competent authority for computer security should consider those relationships in the light of the responsibilities, capabilities and competences of all relevant organizations.

7. DEVELOPING A COMPUTER SECURITY PROGRAMME

7.1. This section describes recommended components and measures of the CSP for each organization. Figure 8 illustrates an example framework for the CSP including supporting and subsidiary documents.

7.2. The CSP for each competent authority and operator defines that organization's role in implementing the strategy, in the form of organizational roles, responsibilities and procedures. The CSP also specifies the means by which the competent authority or operator aims to achieve the computer security objectives and/or implement computer security measures specified by legislation, regulation, standards and guidance from its regulatory body and competent authority for computer security.

7.3. The competent authority for computer security should ensure that each competent authority or operator develops and maintains its CSP as set out in this section. The CSP should be established within the framework of the overall site security plan and within the management system of each organization.

7.4. The competent authority for computer security should ensure that computer security is promoted as an essential component of nuclear security culture and should encourage a commitment to continuous improvement through the explicit commitment of senior management of each competent authority or operator.

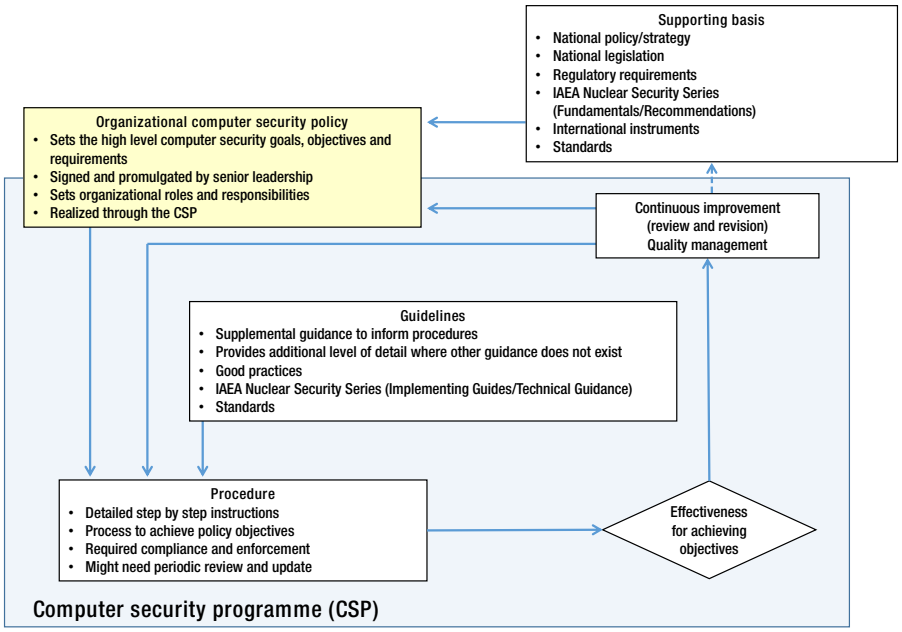


FIG. 8. Overview of a typical computer security programme.

CONTENTS OF A COMPUTER SECURITY PROGRAMME

7.5. The CSP should describe computer security in the organization, in terms of susceptibility to vulnerabilities, protective measures, consequence analysis and mitigation measures, to identify and maintain the acceptable level of risk arising from cyber-attacks and to facilitate recovery to a safe operational state.

7.6. The contents of a CSP should include the following at a minimum:

(a) Organization and responsibilities:
  (i) Organizational charts;
  (ii) Responsible persons and reporting responsibilities;
  (iii) Penalties and corrective actions;
  (iv) Periodic review and approval process;
  (v) Interfaces with other programmes.
(b) Digital asset management:
  (i) List of all computer based systems;
  (ii) List of all computer based system applications;

(iii) Data flow and network diagrams, including all connections to external computer based systems;
(iv) Configuration management (hardware, firmware, software applications, equipment status and associated configurations);
(v) Classification of digital assets and identification of SDAs, including significance classification (i.e. contribution to nuclear security, nuclear safety and nuclear material accounting and control functions).

(c) Risk, vulnerability and compliance assessment:
(i) Periodicity of CSP review and reassessment;
(ii) Self-assessment (including active and passive testing procedures);
(iii) Periodic and reactive risk reassessment and associated methodology;
(iv) Audit procedures and tracking and correction of deficiencies;
(v) Review of legislative and regulatory compliance.

(d) System security design:
(i) Fundamental architectural and design principles;
(ii) Fundamental security design approaches (e.g. security levels and zones);
(iii) Formalization of computer security requirements for vendors, contractors and suppliers;
(iv) Full life cycle security.

(e) Operational security procedures:
(i) Access control;
(ii) Data security;
(iii) Communication security;
(iv) Platform and application security (e.g. hardening, patch management, malware protection);
(v) System monitoring (including log management);
(vi) Computer security maintenance;
(vii) Incident handling;
(viii) Business continuity and disaster recovery;
(ix) System backup.

(f) Personnel management:
(i) Trustworthiness checks (personnel vetting);
(ii) Awareness raising and training;
(iii) Qualification of personnel;
(iv) Termination of employment or transfer of personnel.

7.7. The CSP should be an integrated and coordinated part of the organization's management system. The CSP may be divided into parts that have different levels of security classification, to facilitate the use of the plan efficiently and consistently with the 'need to know' rule and confidentiality requirements.

7.8. The CSP should be reviewed regularly and updated to reflect relevant new knowledge from within and from outside the nuclear security regime, including the following:

(a) New technologies that could be used in, or to protect against, cyber-attacks;
(b) New characteristics of cyberthreats, including identified changes in tactics, techniques and procedures;
(c) New types of computer security incident or nuclear security event.

7.9. The CSP should include provision for regular exercises to train participants and validate the CSP, including contingency plans. Where appropriate, these exercises should be integrated with other security exercises, and should periodically be conducted jointly with emergency exercises.

ORGANIZATIONAL LEVEL RISK ASSESSMENT

7.10. Depending on the capabilities of the competent authorities or operators and the potential adverse impact from cyber-attacks on the SDAs for which they are responsible, the CSP may include a methodology for organizations to conduct local risk assessments for their computer based systems that take into account the local threat environment.

7.11. The purpose of this assessment is to do the following:

(a) Identify and understand risk as well as contributors to that risk;
(b) Serve as the basis for identifying computer based systems and SDAs;
(c) Set a baseline to support analyses of changes to SDAs and other digital assets, the threat and potential impact on computer security and the resulting impact on nuclear security;
(d) Assist in validating higher level requirements.

7.12. The organization may perform risk assessments at both the organizational and system levels.

7.13. Such risk assessments should use as a basis the national threat statement and/or DBT and consider other available sources of information on cyberthreats to inform the assessment process.

7.14. The risk assessment process should include consideration of the adverse consequences on nuclear security or nuclear safety resulting from the

compromise and/or mal-operation of each computer based system, as the basis for identifying SDAs.

7.15. If the results of the risk assessment deviate significantly from what has been assumed by the competent authority for computer security, then the competent authorities or operators should resolve this issue in a timely manner. Such deviations might result from, for example, changes in the local threat environment or equipment changes introducing new vulnerabilities.

7.16. The risk assessment should address all aspects of nuclear security, including for example physical protection and protection against insider threats as well as computer security, collectively in order to assess the risk from blended attacks. Accordingly, the risk assessment should be conducted with input from experts in each of these areas.

COMPUTER SECURITY MEASURES

7.17. The CSP will specify computer security measures that provide prevention, detection, delay, response and mitigation functions as well as ensure that non-malicious acts do not lead to degraded computer security resulting in increased susceptibility to cyber-attacks.

7.18. Specific computer security measures can be assigned to the following three types:

(a) Technical control measures: Hardware and/or software solutions for the protection against, detection and mitigation of and recovery from intrusion or other malicious acts directed at SDAs. The advantages of technical control measures, notably the provision of continuous and automatic protective actions, should be considered when evaluating the effectiveness of different types of measure.
(b) Physical control measures: Physical barriers for the protection of SDAs from physical damage and unauthorized physical access. Physical control measures include guards, and barriers such as locks, fences, gates, physical encasements, tamper indicating devices and isolation rooms.
(c) Administrative control measures: Policies, procedures and practices designed to protect SDAs by controlling personnel actions and behaviours. Administrative control measures include operational and management measures, and are typically directive in nature, specifying what employees

and third party personnel should and should not do, but also include influencing measures, such as promoting a strong security culture.

A GRADED APPROACH FOR DETERMINING COMPUTER SECURITY MEASURES

7.19. Computer security measures within the CSP should be based on a graded approach, where security measures are applied proportionately to the potential impact of a cyber-attack. One practical implementation of the graded approach is to assign computer based systems in nuclear security into zones, with graded computer security measures applied for each zone. A common approach to applying the graded computer security measures is the designation of computer security levels (see paras 2.41–2.46).

7.20. The CSP should include a documented method, such as that described in Section 2, for determining the appropriate computer security level for each digital asset, including SDAs, if this is required by the competent authority for computer security. For example, some competent authorities or operators might be required to implement prescriptive computer security measures, rather than to determine for themselves the security level requirements for computer based systems, digital assets and SDAs.

7.21. The competent authority for computer security should approve the method used for determining computer security levels.

DESIGN OF COMPUTER SECURITY MEASURES

7.22. The CSP should promote the incorporation of computer security measures, to the highest degree possible, into the design of computer based systems. Computer security measures are generally much easier to implement and more effective when incorporated as part of the design rather than when added retrospectively.

7.23. Both nuclear security requirements and nuclear safety requirements should be considered when designing computer based systems.

DEFENCE IN DEPTH FOR COMPUTER SECURITY MEASURES

7.24. The concept of defence in depth is fundamental to nuclear security. The CSP should set out how defence in depth is applied to computer security measures. This may be achieved in different ways, including the following:

(a) Using diverse and independent computer security measures, and requiring independence in their design, operation and maintenance. This will, for example, ensure that a single computer security vulnerability does not provide an adversary with the opportunity to systematically bypass several layers of defence in depth.
(b) Separating duties for personnel or teams that have privileged access to SDAs. This should include considering separation of duties in the design, implementation and administration of computer security measures from the operations of the facility or activity.

MANAGEMENT OF VENDORS, CONTRACTORS AND SUPPLIERS

7.25. Competent authorities or operators may use vendors, contractors or suppliers to provide goods or services that necessarily involve vendors, contractors or suppliers accessing sensitive information and SDAs. In such cases, a legal agreement, such as a licence or the contract for provision of the goods or services, should include appropriate requirements relating to computer security.

7.26. When drafting such licences or contracts, competent authorities and operators should consider including provisions to account for the fact that vendors, contractors and suppliers might possess unique and proprietary information concerning their products or services (e.g. about vulnerabilities to cyber-attack that might become apparent after the original contract has been completed) and that they might be required to share this information with the competent authorities and operators.

7.27. Competent authorities and operators should define in their CSPs specific computer security requirements for vendors, contractors and suppliers. This may include requirements relating to both on-site and off-site work.

7.28. Competent authorities and operators should ensure that vendors, contractors and suppliers implement computer security measures in developing and delivering the products and services that they provide.

7.29. Competent authorities and operators may define specific requirements for computer security within contractual arrangements. These requirements may include the following:

(a) Non-disclosure of sensitive information and other specified information;
(b) Protection requirements for sensitive information, including requirements for the retention or destruction of such information;
(c) Limitations on allowable access to and activities to be performed on computer based systems;
(d) Prohibited activities;
(e) Penalties for non-compliance with stated computer security requirements;
(f) Restrictions on remote access;
(g) Testing requirements for services and products delivered under the contract.

7.30. Competent authorities and operators may consider requiring vendors, contractors and suppliers to demonstrate compliance with contractual computer security requirements.

7.31. Competent authorities and operators should require that vendors, contractors and suppliers report computer security incidents in a timely manner, including the identification of potential threats and vulnerabilities that could affect nuclear security. The obligations and protocols for reporting should be part of the contract.

7.32. The use of vendors, contractors and suppliers might result in the transfer or sharing of risk. Such transfer or sharing of risk might also require the approval of the regulatory body for nuclear security or the competent authority for computer security. However, the responsibility for nuclear security, including computer security, cannot be transferred to vendors, contractors and suppliers.

8. SUSTAINING COMPUTER SECURITY

8.1. This section describes recommended elements and measures for sustaining computer security as part of a nuclear security regime. These should be documented in the CSP.

8.2. Competent authorities and operators should have appropriate human resource development programmes to ensure that they maintain the competences

and level of capability needed to perform their assigned responsibilities for computer security.

8.3. Competent authorities and operators should have in place processes for using best practices and lessons from experience [1], particularly from computer security incidents and, where possible, from other competent authorities and operators, other relevant industries and equivalent organizations in other States.

8.4. Competent authorities and operators should include computer security in their sustainability programmes and support it by provision of adequate resources. Sustainability programmes should cover relevant aspects of the competences and levels of capability needed in the development, implementation, maintenance and decommissioning or removal of SDAs and other digital assets.

SECURITY CULTURE

8.5. Developing, fostering and maintaining a robust nuclear security culture is an essential element of a nuclear security regime [1]. In computer security, people and processes are often the key factor in securing computer based systems, and human error is one of the biggest contributors to computer security incidents. The nuclear security culture should support employees in recognizing and reporting unusual behaviour of computer based systems, or of people using them, as well as reporting human errors that could adversely affect computer security.

8.6. Computer security should be promoted as an essential component of nuclear security culture through the explicit commitment of senior management and through awareness raising and training. The CSP should include activities that reinforce nuclear security culture.

8.7. As part of an effective nuclear security culture, all organizations should ensure that their employees and contractors have a full understanding of their computer security responsibilities and the importance of these responsibilities, in particular with regard to nuclear security and safety. Employees and contractors should receive education and training in computer security commensurate with their roles and responsibilities.

TRAINING

8.8. Competent authorities and operators should establish training programmes for all employees and contractors on computer security that reflect the strategy and that aim to develop and sustain their designated competences and levels of capability.

8.9. Training programmes should include activities to enhance awareness and to develop competences and skills.

8.10. Recommended topics for raising computer security awareness and training include the following:

(a) Awareness of the types of cyberthreat and associated attack techniques;
(b) Awareness of and guidance to resist social engineering;
(c) Recognition of and response to a cyber-attack;
(d) Individuals' responsibilities for computer security and penalties for non-compliance;
(e) The potential impact on nuclear security and safety of cyber-attacks;
(f) Good practices for computer security;
(g) Use of portable devices and removable media;
(h) Use of social media;
(i) Changes to the level or nature of the cyber-threat or risk.

8.11. Maintenance, operations and engineering staff responsible for nuclear systems should be aware of the risks for both nuclear security and safety associated with potential cyber-attacks affecting instrumentation and control features.

8.12. Maintenance, operations and engineering staff responsible for physical protection systems should be aware of the potential effects of cyber-attacks on physical protection system functions.

8.13. Changes in security rules and procedures should be communicated to all relevant employees and contractors as soon as practicable.

8.14. Specialized skills training, appropriate to their specific job functions, should be provided for employees and contractors with administrative and technical responsibilities relating to computer security (e.g. information technology support staff, instrumentation and control staff, security system administrators, maintenance personnel for technical equipment).

8.15. Training programmes should specify training requirements for vendors, contractors and suppliers, for both on-site and off-site work.

8.16. Senior management should receive periodic training and awareness briefings on the cyberthreat and risk management.

8.17. Competent authorities and operators should frequently review and update their training programmes to take account of the dynamic nature of computer security, including changes in the cyberthreat and in techniques for cyber-attack.

8.18. Competent authorities and operators should assign responsibility for and allocate adequate resources to support and sustain training programmes.

8.19. Records of the formal training completed by all employees and contractors should be maintained.

8.20. Training and awareness raising activities on information security and computer security are often combined. Annex III to Ref. [8] provides a sample awareness programme for information security, which can be adapted to include computer security.

CONTINGENCY PLANS AND RESPONSE

8.21. The CSP should document computer security measures for the detection of, response to and mitigation of the consequences of computer security incidents.

8.22. The CSP should specify the appropriate analysis and response actions to characterize the cause, immediate effects and potential impact of the computer security incident. These elements might not be readily apparent, but need to be identified as soon as possible.

8.23. The analysis of the computer security incident should include consideration of the possibility that this incident could be a precursor or reconnaissance activity for a future attack.

8.24. The CSP should include contingency plans to respond to cyber-attacks. These plans should take account of the possibility of insider and blended attacks. The contingency plan should identify specific types of computer security incident and the required response to these incidents.

8.25. When a computer security incident is also a nuclear security event, the relevant contingency plan should be activated. The CSP and related contingency plans should specify immediate actions to be taken whenever nuclear safety is jeopardized (in such cases, emergency plans may also be activated, but these are outside the scope of this publication).

8.26. The CSP should include the criteria for involvement of additional resources and their role in response to computer security incidents.

8.27. Analysis of computer security incidents may involve a cross-cutting team to analyse the impact on both nuclear security and safety.

COMPUTER SECURITY ASSURANCE ACTIVITIES

8.28. Competent authorities and operators should ensure that their management systems include effective means to provide assurance that computer security requirements are met, including within the supply chain.

8.29. Competent authorities and operators (except those that implement only computer security measures prescribed by the regulatory body or the competent authority for computer security) should provide assurance to the competent authority for computer security that the resources assigned to computer security are appropriate and proportionate to the level of threat identified in the threat assessment.

8.30. Competent authorities and operators should ensure that the inspections or assessments to verify compliance with nuclear security requirements include the evaluation of computer security measures.

Appendix

NUCLEAR SAFETY INTERFACE CONSIDERATIONS FOR COMPUTER SECURITY AT FACILITIES

A.1. Sabotage of a facility could lead to compromise of its nuclear safety or of its availability in the case of cyber-attack on systems important to safety at the facility that use, rely upon or are supported by computer based systems. Such attacks might cause failures or mal-operation of such systems important to safety in ways that would not be possible if the systems were in their operational state or anticipated failure states.

A.2. Malicious acts might affect a single system (or item) or be a common cause of undesirable behaviour of multiple systems (or items). In the design of the facility it should be ensured that malicious acts cannot cause the failure of or bypass multiple levels of safety defence in depth.

A.3. Computer security is intended to reduce the possibility that adversaries can commit acts of sabotage via cyber-attacks that could compromise the security, safety or availability of the facility. Computer security contributes to all levels of defence in depth for safety, as described in Ref. [12], and therefore needs to be applied to functions, systems and equipment at all levels.

A.4. The safety–security interface in computer security comprises a number of elements that are important to nuclear security and nuclear safety. These elements include systems, procedures and personnel. Nuclear safety measures often also provide valuable functions for nuclear security (and vice versa), and opportunities to exploit such complementary functions should be considered when developing computer security measures.

A.5. One example of a safety measure that might also have security benefits is a feature providing the automated checking of the validity, authenticity and integrity of received data before use within a safety function. Maintenance or modification of the feature might degrade the safety or security functions if those performing such activities are not aware of the multiple functions (interdependencies). Consequently, both safety and security functions performed by such features should be described in system and component documentation.

A.6. Safety strategy might also adversely affect security (or vice versa). For example, design for safety often involves allocation of functions to different items

or systems in order to isolate the effects of failure, and the provision of redundant and diverse systems so that single failures will not compromise important functions. Such a strategy might result in an increase in the number of items in the system important to safety, which increases its complexity and might increase the number of possible targets for cyber-attack. Both security and safety measures should therefore always be considered to identify and resolve any conflicts.

A.7. The appropriateness of a given computer security measure will depend on both security and safety considerations, and therefore designing such measures needs expertise in both areas. Computer security measures will include technical, physical and administrative measures, and all of the measures need to work together. Such an approach might, for example, necessitate that certain security functions (e.g. collection of audit records, generation of security alarms) be implemented by systems that can monitor the instrumentation and control systems but cannot affect their performance, or that active security scans be performed only when instrumentation and control systems are offline. Exceptions to such an approach may be permitted, but they would need to be analysed and justified case by case.

A.8. The acceptable risk for a facility is likely to be the same whether the initiating cause is a safety or a security event. The common approaches to achieve this may be summarized as follows:

(a) Safety and security both apply the concept of defence in depth (i.e. the use of multiple layers of protection).
(b) Consideration is given to preventing an initiating event, early detection of any abnormal situations and prompt response to avoid escalation of the situation.
(c) Mitigation of consequences is planned for in design, in case the previous steps fail.
(d) Extensive emergency planning is in place to address situations where there is a failure of prevention, detection and mitigation.

A.9. The relationship between computer security and safety needs effective coordination, such as in the classification and management of assets taking into account security and safety considerations. This might be complicated by the increasing reliance on software and networks in computer based systems and their consequently rapidly evolving nature, which means that the design and operation of computer security measures also change rapidly. This presents a challenge when safety analyses rely upon accurate predictions of future deterministic behaviour. This analysis might be further complicated by uncertainty about the

effectiveness of computer security measures, which means that analysis might not provide accurate predictions of future system behaviour in response to initiating events (e.g. when targeted via cyber-attacks).

A.10. Application of computer security measures to existing systems is likely to necessitate review of the existing safety analysis. In general, integrated computer security measures have the potential to constrain or otherwise alter the behaviour of the system important to safety when compared to separate or standalone measures.

REFERENCES

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

[2] Convention on the Physical Protection of Nuclear Material, INFCIRC/274/Rev.1, IAEA, Vienna (1980); Amendment to the Convention on the Physical Protection of Nuclear Material, INFCIRC/274/Rev.1/Mod.1, IAEA, Vienna (2016).

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

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

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

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

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

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

[9] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, Information Technology — Security Techniques — Information Security Risk Management, ISO/IEC 27005:208, ISO, Geneva (2018).

[10] INTERNATIONAL ATOMIC ENERGY AGENCY, National Nuclear Security Threat Assessment, Design Basis Threats and Representative Threat Statements, IAEA Nuclear Security Series No. 10-G (Rev. 1), IAEA, Vienna (2021).

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

[12] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety of Nuclear Power Plants: Design, IAEA Safety Standards Series No. SSR-2/1 (Rev. 1), IAEA, Vienna (2016).

Annex I

SUGGESTED RECOMMENDATIONS LEVEL GUIDANCE ON COMPUTER SECURITY FOR A NATIONAL NUCLEAR SECURITY REGIME

I–1. "ELEMENTS OF A STATE'S NUCLEAR SECURITY REGIME FOR COMPUTER SECURITY" in this annex was developed by experts from more than 20 Member States to supplement the existing Recommendations publications in the IAEA Nuclear Security Series [I–1 to I–3] and provides suggested Recommendations level guidance on the design, implementation and sustaining of computer security in a State's nuclear security regime. States may choose to treat the text as Recommendations level guidance. The implementing guidance in the main text of this publication is consistent with the suggested Recommendations level guidance in this annex.

BACKGROUND

I–2. The purpose of the IAEA Nuclear Security Series Recommendations publications [I–1 to I–3] is to provide guidance to States and their competent authorities on how to develop or enhance, implement and maintain an effective national nuclear security regime to provide for the security of, respectively, nuclear material and nuclear facilities, radioactive material and associated facilities, and nuclear and other radioactive material out of regulatory control.

I–3. Recommendations publications present good practices that should be adopted by Member States in the application of the Nuclear Security Fundamentals [I–4]. These Fundamentals identify the responsibility for States to ensure that sensitive information and sensitive information assets are protected from nuclear security threats.

I–4. Nuclear security might target sensitive information or sensitive information assets to undermine the performance of nuclear security or nuclear safety system functions. The attack could be a solitary act of sabotage or it could be part of a blended attack against a facility, that might include elements of both a cyber-attack and physical attack, or against an organization to obtain unauthorized access to material. Therefore, computer security is intrinsic to the State's nuclear security regime and necessary to achieve its objectives.

I–5. Sensitive digital assets are those sensitive information assets that are computer based systems, the compromise of which could lead to adverse impacts on nuclear security. Therefore, sensitive digital assets demand the application of computer security measures.

I–6. Computer security measures aim to maintain the confidentiality, integrity and availability of sensitive information within sensitive digital assets and of the sensitive digital assets themselves.

I–7. The existing Recommendations level publications lack sufficient guidance on computer security measures for the protection of sensitive digital assets.

OBJECTIVE

I–8. This annex provides suggested computer security guidance for the implementation of essential elements of the Nuclear Security Fundamentals [I–4] where these are not sufficiently addressed within the Recommendations [I–1 to I–3]. This guidance is not intended to alter the existing Recommendations in any way.

I–9. This annex is intended for use by States, competent authorities, operators[1], suppliers, vendors, contractors, nuclear security professionals and nuclear safety professionals.

SCOPE

I–10. This guidance applies to the computer security aspects of nuclear security.

I–11. This guidance addresses general aspects of computer security applicable to all areas of nuclear security, including the security of nuclear material and nuclear facilities [I–1], of radioactive material and associated facilities [I–2], and of nuclear and other radioactive material out of regulatory control [I–3]. This guidance should be applied using a graded approach.

[1] In this context, ‘operators’ refers to licence holders, shippers and carriers.

ELEMENTS OF A STATE'S NUCLEAR SECURITY REGIME FOR COMPUTER SECURITY

State responsibility

I–12. The State should develop a computer security strategy[2] that supports its nuclear security regime.

Assignment of computer security responsibilities

I–13. The State should designate and empower competent authorities with responsibility in the development and implementation of the legislative and regulatory framework for computer security that supports the nuclear security regime. The competent authority for computer security may be different from the competent authority (or competent authorities) for other aspects of nuclear security.

I–14. The State should ensure that functions, roles, and other provisions for computer security are defined and closely coordinated between and within all competent authorities involved in nuclear security.

Legislative and regulatory framework

I–15. The State should ensure that the legislative and regulatory framework includes nuclear security requirements for prevention of, detection of and response to unauthorized acts against computer based systems that could adversely impact nuclear security. These requirements should be used in developing the State's threat assessment.

I–16. The State should establish an inspection and enforcement process to verify compliance with computer security requirements within its legislative and regulatory framework.

I–17. The State should ensure that sanctions for unauthorized acts against computer based systems that could adversely impact nuclear security are part of its legislative and regulatory framework.

---

[2] This strategy may be specific for nuclear security regimes or it may be more general, such as a strategy applicable to critical infrastructure protection. Some States may use the term 'policy' in this context.

Competent authorities

I–18. The competent authorities should ensure that operators develop and implement computer security policy and associated computer security programmes in accordance with national requirements for nuclear security.

I–19. The competent authorities should ensure that computer security is part of evaluation and licensing or other procedures to grant authorization.

I–20. The competent authorities should verify continued compliance of the operator with computer security requirements through regular inspections and, when necessary, make use of enforcement for ensuring that corrective action is taken.

Responsibility of operators

I–21. Operators should identify sensitive digital assets and characterize them based on potential consequences for nuclear security if compromised.

I–22. Operators should define appropriate computer security measures[3] and ensure such measures are implemented to protect sensitive digital assets from compromise throughout their life cycle (to the greatest extent possible) in accordance with the concepts of a graded approach and defence in depth.

I–23. Operators should apply computer security as a design principle for sensitive digital assets and their use, including protection against unauthorized access (of persons, processes or equipment) and against malware.

I–24. Operators should assess and manage computer security measures such that they do not adversely affect physical protection, nuclear safety, and nuclear material accounting and control activities.

I–25. Operators should conduct assurance activities to verify that their computer security measures comply with computer security requirements.

I–26. Operators should ensure that computer security measures are integrated into their nuclear supply chain management arrangements with the aim of minimizing

[3] Security measures may consist of physical, technical and administrative control measures.

vulnerabilities in computer based systems and preventing the use of the supply chain as a pathway for cyber-attacks.

I–27. State organizations, including competent authorities, should follow the recommendations in paras I–21 to I–26 when protecting sensitive digital assets for which these organizations are responsible.

International cooperation and assistance

I–28. International cooperation and assistance should include computer security considerations relevant to nuclear security.

Identification and assessment of threats

I–29. The State's threat assessment[4] (and design basis threat, if appropriate) should consider potential adversaries utilizing computer capabilities, including the potential for insider activities and blended attacks. The threat assessment should be reviewed and updated to reflect changes in the cyberthreat and should be appropriately communicated in a timely manner.

I–30. When the design basis threat or threat assessment for cyber-attack is separate from the design basis threat or threat assessment for physical attack, the State should ensure that the threat assessments (and design basis threat, if appropriate) are developed in a coordinated manner.

Safety and security interface

I–31. The interface between safety and security, including computer security, should be managed in a manner to ensure that they do not adversely affect each other and that, to the degree possible, they are mutually supportive.

Sustaining computer security

I–32. Computer security should be addressed in an integrated and coordinated manner within the management system of each competent authority and operator.

I–33. Computer security should be promoted as an essential component of nuclear security culture.

---

[4] This may be referred to as a 'national threat assessment'.

I–34. Computer security should be part of the competent authorities' and operators' sustainability programmes supported by provision of adequate resources.

Planning and preparedness for and response to computer security incidents

I–35. The State should ensure the existence of contingency plans and capabilities of competent authorities, operators and other relevant parties to adequately address computer security incidents that could adversely impact nuclear security.

I–36. The State should ensure that competent authorities, operators and other relevant parties conduct regular exercises to assess and validate computer security aspects of response plans.

I–37. The State's nuclear security regime should include requirements for timely reporting of computer security incidents to the competent authority (or authorities).

REFERENCES TO ANNEX I

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

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

[I–3] EUROPEAN POLICE OFFICE, INTERNATIONAL ATOMIC ENERGY AGENCY, INTERNATIONAL CIVIL AVIATION ORGANIZATION, INTERNATIONAL CRIMINAL POLICE ORGANIZATION–INTERPOL, UNITED NATIONS INTERREGIONAL CRIME AND JUSTICE RESEARCH INSTITUTE, UNITED NATIONS OFFICE ON DRUGS AND CRIME, WORLD CUSTOMS ORGANIZATION, Nuclear Security Recommendations on Nuclear and Other Radioactive Material out of Regulatory Control, IAEA Nuclear Security Series No. 15, IAEA, Vienna (2011).

[I–4] INTERNATIONAL ATOMIC ENERGY AGENCY, Objective and Essential Elements of a State's Nuclear Security Regime, IAEA Nuclear Security Series No. 20, IAEA, Vienna (2013).

Annex II

CYBERTHREAT PROFILES

II–1. Understanding the cyberthreat is important for developing and implementing protective measures. The cyberthreat is unlike the physical threat to nuclear and other radioactive material and its associated facilities and operations. The cyberthreat is not limited by proximity to the location, by numbers of attackers or by the boundary of the targeted facility. An understanding of the characteristics of the cyberthreat as well as the possible attack scenarios provides valuable insight into both prevention and response measures. Adversaries and their tools, tactics and targets are dynamic elements, and diligence needs to be maintained in assessing the current threat.

II–2. Prevailing trends include the following [II–1, II–2]:

(a) An increasing number of adversaries with capability to carry out cyber-attacks;
(b) An increasing number of individuals or groups offering 'cybercrime as a service', reducing the barriers for entry for adversaries who previously lacked the necessary skills;
(c) Increasing sophistication of the techniques used for cyber-attacks, making detection and response more difficult;
(d) Continuing use of social engineering in cyber-attacks, including 'spear phishing' and 'watering hole' techniques;
(e) Increasing focus by adversaries on finding and exploiting vulnerabilities in industrial control systems;
(f) Proliferation of ransomware;
(g) Continued difficulty in securing the supply chain against cyber-attacks.

II–3. At a minimum, the competent authority for cyberthreat assessment, competent authority for computer security, and operators participating in the threat assessment process have to consider the attributes and characteristics described in the following section for each identified internal and external threat. Characterization of the cyberthreat is difficult owing to the challenge of identifying attackers and the possibility of anonymous attack. It can be helpful, however, to develop threat profiles.

CYBERTHREAT ATTRIBUTES AND CHARACTERISTICS

II–4. The following cyberthreat attributes and characteristics may be useful in developing threat profiles:

(a) Motivation: Political, financial, ideological or personal.
(b) Intentions: Sabotage of radioactive material or of a radiological facility, theft of radioactive or nuclear material, causing public panic and social disruption, instigating political instability, causing mass injuries and casualties, theft of sensitive information.
(c) Relevant skills (capabilities): Skills in using computer and automated control systems in direct support of physical attacks, for intelligence gathering, for computer based attacks, for money gathering.
(d) Knowledge: Targets, site plans and procedures, security measures, safety measures and radiation protection procedures, operations, potential use of nuclear or other radioactive material.
(e) Funding: Source, amount and availability.
(f) Tactics: Use of stealth, deception or force.

BASIC DESCRIPTION OF THE CYBERTHREAT

II–5. Threats may be categorized in many ways. The following categories are presented as examples (some categories may overlap).

II–6. Insider threat: One of the most challenging attacks to defend against is the insider threat. An ‘insider’ is 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 [II–3]. The insider is someone who is trusted and has been trained on internal systems and who, for whatever reason, uses this access and knowledge in a compromising and potentially malicious manner. The specific rationale for insider activities varies greatly, and this category includes people ranging from disgruntled employees to covert agents. The unwitting insider is a special case. An unwitting insider is an insider without the intent and motivation to commit a malicious act who is exploited by an adversary without the unwitting insider’s awareness [II–3].

II–7. Extremist: Extremism refers to groups that go beyond the norm in political or social expression (i.e. activism which has exceeded accepted behaviours). Extremists might engage in a solitary act or might coordinate loosely with similarly minded individuals in a cyber-attack against a designated target. Such collectives might not be tightly controlled by a central figure and might not be operating under specific rules of engagement.

II–8. Recreational hacker: Recreational hackers include individuals or groups who are motivated by fame or notoriety rather than by the desire to inflict damage or by monetary gain. Compromise by recreational hackers might be non-targeted (i.e. the nuclear facility was not the specific target); instead, it might result from a hostile environment. An example of this would be a control system at a nuclear facility infected with a common virus owing to insecure management of portable devices and removable media.

II–9. Organized crime: Organized crime has developed very sophisticated and targeted cyber-attacks against multiple sectors of industry. The purpose is monetary gain, which might come directly from theft of money or indirectly from selling stolen data or selling information about a compromise to other threats.

II–10. Nation State: Nation States often represent a very capable and persistent threat. The motivations and objectives of such attacks are normally confined to information collection, and they are often bound by structured rules of engagement.

II–11. Terrorist: Past cyber-attacks attributed to terrorists have largely consisted of unsophisticated efforts such as ‘email bombing’ of ideological foes, denial of service attacks or defacing of websites, but terrorists might be gaining increasing technical competence to perform network based attacks. This technical competence might arise from internal expertise or from employing hackers [I–4]. Terrorists might target and attempt to sabotage critical infrastructure such as nuclear power plants, but their focus might also be the acquisition of nuclear and other radioactive material.

ATTACK CHARACTERISTICS

II–12. It is also important to understand attack characteristics in order to build deterrence, prevention, detection, mitigation and response measures. Several types of attack are described in the sections that follow (the categories are not mutually exclusive).

Non-targeted attack

II–13. Many of the threats described above are likely to undertake attacks directed against specific nuclear security targets. However, non-targeted attacks might also occur, for example, non-directed malicious codes can be inadvertently introduced into computer based systems and networks, adversely affecting nuclear security. An example of this would be a control system at a nuclear facility infected with a common virus owing to insecure management of mobile media.

Persistent attacks

II–14. A cyber-attack might aim for immediate impact or it might be part of a sustained campaign against a facility or organization. A persistent attack might start with compromise of a computer based system followed by a lengthy campaign of information collection. The result might be an impactful event, or the attack might simply aim to establish a presence for future activity.

Blended attacks

II–15. Blended attacks are coordinated acts which consist of a cyber-attack associated with a physical act. For example, a physical access control system could be compromised by cyber-attack to permit the physical entry of unauthorized individuals.

THREAT PROFILE TABLES

II–16. Tables II–1 and II–2 illustrate a possible set of attacker profiles. Table II–1 focuses on insider threats (see also Ref. [II–3]), while Table II–2 identifies possible external threats. The tables associate general types of attacker with their resources, the time span of the attack, the tools that are likely to be used and the attacker's motivations. Profiles have to be adapted to the individual situations.

TABLE II–1. INTERNAL THREATS

Threat	Resources (skills, knowledge, access, funding)	Time	Tactics	Motivation	Intentions
Covert agent	Facilitating 'social engineering' System access at some level System documentation and expertise available	Varied, but generally cannot devote long hours outside of normal work functions	Existing access, knowledge of programming and system architecture Possible knowledge of existing passwords Possibility to insert specifically crafted backdoors and/or Trojans Possible external expertise support Might be directed by an external handler	Political, financial, ideological	Theft of business information, technology secrets, personal information Sabotage

TABLE II–1. INTERNAL THREATS (cont.)

Threat	Resources (skills, knowledge, access, funding)	Time	Tactics	Motivation	Intentions
Coerced insider	System access at some level System documentation and expertise available	Varied, but generally cannot devote long hours outside of normal work functions	Existing access, knowledge of programming and system architecture Possible knowledge of existing passwords Possibility to insert specifically crafted backdoors and/or Trojans Possible external expertise support Directed by an external handler	Personal	Theft of business information, technology secrets, personal information Sabotage
Unwitting insider	System access associated with normal work functions		Unwittingly provides internal access to an adversary	No motivation necessary	

TABLE II–1. INTERNAL THREATS (cont.)

Threat	Resources (skills, knowledge, access, funding)	Time	Tactics	Motivation	Intentions
Disgruntled employee/system user (multiple types)					
Currently employed — non-technical computer users	Medium/strong resources System access at some level System documentation and expertise available on specific business and operations systems	Varied, but generally cannot devote long hours (might not be accurate for all)	Existing access, knowledge of programming and system architecture Possible knowledge of existing passwords Ability to insert 'kiddie' tools or scripts (potentially more elaborate if they have specific computer skills)	Personal financial	Revenge, havoc, chaos Theft of business information Embarrass employer/ another employee Degrade public image or confidence
Currently employed — technical computer users, administrators, developers, etc.	High level of computer access and authority Possible remote access	Lots of time		Personal financial	

TABLE II–1. INTERNAL THREATS (cont.)

Threat	Resources (skills, knowledge, access, funding)	Time	Tactics	Motivation	Intentions
Currently contracted — third parties	Local or remote access possibly associated with current support function	Varied	Infiltration of supply chain elements with compromised components Infiltration via mobile media or remote connection	Personal financial	
Disgruntled employee/user (no longer employed)	Limited resources if not working with a larger group of people Might still possess system documentation Might use unmanaged former access Possible ties to facility personnel	Varied and depending on the associated group of people	Possible knowledge of existing passwords Might use unmanaged former access Might have created system backdoors while still an employee 'Social engineering'	Personal	Revenge, havoc, chaos Theft of business information Embarrass employer/ another employee Degrade public image or confidence

TABLE II–2. EXTERNAL THREATS

Threat	Resources (skills, knowledge, access, funding)	Time	Tactics	Motivation	Intentions
Non-targeted attack	Varied skills	Varied	No specific targeting, generally rely on normal information technology processes and vulnerabilities, including social engineering	Personal — fun, status	Fame, attention of media Compromise of target of opportunity
Extremist	Varied skills, but generally limited Little knowledge of the system outside of public information	Potentially time sensitive in that activities might centre on current or recent events	Individual or small group hacking activities Distribution of tools to larger collective	Intent on political effect	Attention of media Public embarrassment
Recreational hacker	Varied skills, but generally limited Little knowledge of the system outside of public information	Lots of time, not very patient	Generally available scripts and tools Some tool development possible	Personal — fun, status	Compromise of target of opportunity Exploitation of 'low hanging fruit'

TABLE II–2. EXTERNAL THREATS (cont.)

Threat	Resources (skills, knowledge, access, funding)	Time	Tactics	Motivation	Intentions
Organized crime	Strong resources Employment of specialized expertise	Varied, but mostly short term	Scripts, home grown tools Might employ 'hacker for hire' Might employ former/current employee 'Social engineering'	Blackmail Extortion (financial gain) Play upon financial and perception fears of business Information for sale (technical, business or personal)	Material theft Sensitive information theft Sale of information or access
Nation State	Strong resources and expertise Intelligence gathering activities Possible training/ operating experience on the system Teams of trained experts	Varied, but able to support sustained attacks	Sophisticated tools Might employ former/current employee 'Social engineering'	Political Intelligence collection Building access points for later actions	Technology theft Reconnaissance for future attack Sabotage

TABLE II–2. EXTERNAL THREATS (cont.)

Threat	Resources (skills, knowledge, access, funding)	Time	Tactics	Motivation	Intentions
Terrorist	Varied skills Possible training/ operating experience on the system Possible infiltration with covert agent Potential to be well funded Growing skills	Lots of time, very patient	Scripts, home grown tools Might employ hacker for hire Might employ former/current employee 'Social engineering'	Intelligence collection Building access points for later actions Chaos Revenge Affect public opinion (fear)	Support for blended attack Reconnaissance for future attack Sabotage Material theft

REFERENCES TO ANNEX II

[II–1] AUSTRALIAN CYBER SECURITY CENTRE, ACSC 2015 Threat Report (2015), www.cyber.gov.au/sites/default/files/2020-04/ACSC_Threat_Report_2015.pdf

[II–2] GEORGIA INSTITUTE OF TECHNOLOGY, Emerging Cyber Threats Report 2016 (2015), https://iisp.gatech.edu/sites/default/files/documents/threats_report_2016.pdf

[II–3] INTERNATIONAL ATOMIC ENERGY AGENCY, Preventive and Protective Measures against Insider Threats, IAEA Nuclear Security Series No. 8-G (Rev. 1), IAEA, Vienna (2020).

[II–4] CONGRESSIONAL RESEARCH SERVICE, Terrorist Use of the Internet: Information Operations in Cyberspace (2011), www.hsdl.org/?view&did=8233

Annex III

ASSIGNMENT OF COMPUTER SECURITY RESPONSIBILITIES

III–1. Table III–1 illustrates typical assignment of responsibilities to competent authorities. It might be advantageous to develop a table of typical computer security responsibilities that correspond to these typical nuclear security responsibilities.

TABLE III–1. TYPICAL COMPUTER SECURITY RESPONSIBILITIES IN A NUCLEAR SECURITY REGIME

Type of entity	Nuclear security responsibilities
Regulatory body	Establish a system of regulatory control over radioactive material, associated facilities and associated activities that places the primary responsibility for nuclear security on authorized persons Establish a system of security based categorization Develop and maintain a national register of radioactive material Participate in national threat assessment Develop and apply design basis threat, alternative threat statement or other defined threat for purposes of regulation for security Implement authorization (licensing) process, including review and assessment of security systems and security management measures Establish regulatory requirements and provide guidelines for security, including requirements for information protection Manage the safety–security interface Conduct security inspections Take enforcement action for non-compliance Participate in regional and international databases and other cooperative activities Encourage and promote a robust nuclear security culture Participate in planning and preparedness for and response to nuclear security events, including participation in exercises Administer procedures for authorizing and controlling the import and export of radioactive material Notify operators concerning specific or increased threat Review and assess the design of the security system (in the authorization process)

TABLE III–1. TYPICAL COMPUTER SECURITY RESPONSIBILITIES IN A NUCLEAR SECURITY REGIME (cont.)

Type of entity	Nuclear security responsibilities
Law enforcement	Provide response to interrupt malicious acts (unauthorized access, unauthorized removal, sabotage) Participate in planning and preparedness for and response to nuclear security events, including participation in exercises Participate in national threat assessment Identify specific or increased threats Conduct background checks for purposes of trustworthiness verification Detect and investigate nuclear security events
Customs and border control	Participate in national threat assessment Identify specific or increased threats Control and detect non-compliance with respect to imports or exports Communicate with regulatory body with respect to national inventory of radioactive material
Intelligence and security agencies	Direct national threat assessment Identify specific or increased threats
National emergency response agency	Coordinate planning and preparedness for and response to nuclear security events
Civil defence, health and environment agencies	Participate in planning and preparedness for and response to nuclear security events
Ministry of justice and prosecuting authorities	Impose sanctions against perpetrators of malicious acts
Ministry of foreign affairs	Engage in regional and international cooperation

Annex IV

EXAMPLE FRAMEWORK OF COMPUTER SECURITY COMPETENCES AND LEVELS OF CAPABILITY

IV–1. The establishment of a framework of competences and levels of capability plays a key role in ensuring that organizations and individuals are competent and remain competent to perform their computer security roles and responsibilities.

IV–2. This annex provides an illustration of what is meant by a framework of competences and levels of capability. It is not intended to provide sufficient guidance to develop such a framework.

IV–3. For each organization or individual, the framework identifies the competence needed from the specific domains of computer security. An example list of such domains is as follows:

(a) Management (capacity, strategic, crisis management, governance, organization);
(b) Incident response (computer forensics, network defence);
(c) Legislative and regulatory framework (criminal law, regulations);
(d) Information security and management (cryptography, encryption, storage);
(e) Procurement (contracts, supply chain);
(f) Assurance activities (testing, certification, configuration management);
(g) Computer security architecture;
(h) International coordination and assistance.

Alternatively, the international standards ISO 27002 [IV–1] (for information security management systems) and IEC 63096 [IV–2] (ISO 27002 applied to nuclear power plants) offer lists of control areas that can be adapted for use as competence domains.

IV–4. The framework identifies the specific computer security skills and knowledge needed within each competence, informed by the threat assessment for cyber-attack, knowledge of the nature of computer based systems available to the nuclear security regime, and knowledge of the vulnerabilities of those computer based systems.

IV–5. Organizations and individuals exhibit different levels of maturity in computer security competences. The framework categorizes the level of

capability for each competence, using a scale of at least three different levels. This provides for the implementation of a graded approach. An example of such a categorization, from lowest maturity to highest, is the following:

(a) Fundamental (novice): Exhibits automatic, rule based behaviour that is strongly constrained and inflexible.
(b) Intermediate (practitioner): Acts consciously to meet long term goals and plans within established policy.
(c) Advanced (expert): Intuitively understands the situation, is able to focus immediately on the key aspects.

IV–6. Higher levels of capability are needed to ensure protection against highly capable threats or to prevent high radiological consequences. For example, competent authorities and operators that store, transport, or use Category I or II nuclear material, or operate facilities or perform activities that have the potential for high radiological consequences, are considered to be managing very high or high consequences.

IV–7. The framework ensures that organizations and individuals responsible for design of computer security measures demonstrate a high level of the relevant competences.

IV–8. Some organizations demand that those capabilities be continuously available on-site, while others rely on assistance from other organizations.

IV–9. The framework specifies in detail the typical profile of activities that it might permit a competent authority or operator or third party to perform. For example, a competent authority or operator with the necessary competences at an advanced level might perform a leading role in the national threat assessment activities relating to computer security. A competent authority or operator with competences at a fundamental level might perform only a supporting role in the national threat assessment. Table IV–1 illustrates this.

TABLE IV–1. CATEGORIZATION OF ACTIVITIES ACCORDING TO COMPETENCY LEVEL

Activity type	Fundamental stakeholders	Intermediate stakeholders (adds to fundamental)	Advanced stakeholders (adds to intermediate)
Activities regarding knowledge of the threat environment	Maintaining basic awareness of threat behaviours (e.g. 'phishing' attacks)	Understanding the consequences of computer security threats to own environment	Consistently and proactively monitoring rapidly evolving computer security threats
Activities regarding threat assessments and creating scenarios	Contributing role when requested (e.g. providing practical detail about what really happens in the workplace)	Participating role in national threat assessment Creating site-specific scenarios to elaborate on the threat assessment where potential impact is medium, low or very low	Leading role in the national threat assessment activities Creating site-specific scenarios where potential impact is very high or high Assessing scenarios from intermediates

REFERENCES TO ANNEX IV

[IV–1] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, Information Technology — Security Techniques — Code of Practice for Information Security Controls, ISO/IEC 27002:2013, ISO, Geneva (2013).

[IV–2] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Nuclear Power Plants — Instrumentation, Control and Electrical Power Systems — Security Controls, IEC 63096:2020, IEC, Geneva (2020).

GLOSSARY

blended attack. A malicious act involving the coordinated use of cyber-attack and physical attack.

computer based systems. Technologies that create, provide access to, process, compute, communicate or store digital information, or perform, provide or control services involving such information.

ⓘ These systems may be physical or virtual. They may include: desktops, laptops, tablets and other personal computers, smart phones, mainframe computers, servers, virtual computers, software applications, databases, removable media, digital instrumentation and control devices, programmable logic controllers, printers, network devices, and embedded components and devices.

computer security. A particular aspect of information security that is concerned with the protection of computer based systems against compromise.

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

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

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.

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

computer security zone. A group of systems having common physical and/or logical boundaries — and, if necessary, arranged using additional criteria — that is

assigned a common computer security level to simplify the administration, communication and application of computer security measures.

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

information security. The preservation of the confidentiality, integrity and availability of information.

sensitive digital assets (SDAs). Sensitive information assets that are (or are parts of) 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. For example, sensitive information assets include control systems, networks, information systems and any other electronic or physical media.

IAEA
International Atomic Energy Agency

No. 26

ORDERING LOCALLY

IAEA priced publications may be purchased from the sources listed below or from major local booksellers.

Orders for unpriced publications should be made directly to the IAEA. The contact details are given at the end of this list.

NORTH AMERICA

Bernan / Rowman & Littlefield
15250 NBN Way, Blue Ridge Summit, PA 17214, USA
Telephone: +1 800 462 6420 • Fax: +1 800 338 4550
Email: orders@rowman.com • Web site: www.rowman.com/bernan

REST OF WORLD

Please contact your preferred local supplier, or our lead distributor:

Eurospan Group
Gray's Inn House
127 Clerkenwell Road
London EC1R 5DB
United Kingdom

Trade orders and enquiries:
Telephone: +44 (0)176 760 4972 • Fax: +44 (0)176 760 1640
Email: eurospan@turpin-distribution.com

Individual orders:
www.eurospanbookstore.com/iaea

For further information:
Telephone: +44 (0)207 240 0856 • Fax: +44 (0)207 379 0609
Email: info@eurospangroup.com • Web site: www.eurospangroup.com

Orders for both priced and unpriced publications may be addressed directly to:

Marketing and Sales Unit
International Atomic Energy Agency
Vienna International Centre, PO Box 100, 1400 Vienna, Austria
Telephone: +43 1 2600 22529 or 22530 • Fax: +43 1 26007 22529
Email: sales.publications@iaea.org • Web site: www.iaea.org/publications

NUCLEAR SECURITY RECOMMENDATIONS ON PHYSICAL PROTECTION OF NUCLEAR MATERIAL AND NUCLEAR FACILITIES (INFCIRC/225/REVISION 5)
IAEA Nuclear Security Series No. 13
STI/PUB/1481 (57 pp.; 2011)
ISBN 978–92–0–111110–4 Price: €28.00

NUCLEAR SECURITY RECOMMENDATIONS ON RADIOACTIVE MATERIAL AND ASSOCIATED FACILITIES
IAEA Nuclear Security Series No. 14
STI/PUB/1487 (27 pp.; 2011)
ISBN 978–92–0–112110–3 Price: €22.00

NUCLEAR SECURITY RECOMMENDATIONS ON NUCLEAR AND OTHER RADIOACTIVE MATERIAL OUT OF REGULATORY CONTROL IAEA
IAEA Nuclear Security Series No. 15
STI/PUB/1488 (33 pp.; 2011)
ISBN 978–92–0–112210–0 Price: €23.00

COMPUTER SECURITY AT NUCLEAR FACILITIES
IAEA Nuclear Security Series No. 17
STI/PUB/1527 (69 pp.; 2011)
ISBN 978–92–0–120110–2 Price: €33.00

OBJECTIVE AND ESSENTIAL ELEMENTS OF A STATE'S NUCLEAR SECURITY REGIME
IAEA Nuclear Security Series No. 20
STI/PUB/1590 (15 pp.; 2013)
ISBN 978–92–0–137810–1 Price: €20.00

COMPUTER SECURITY OF INSTRUMENTATION AND CONTROL SYSTEMS AT NUCLEAR FACILITIES
IAEA Nuclear Security Series No. 33–T
STI/PUB/1787 (58 pp.; 2018)
ISBN 978–92–0–103117–4 Price: €42.00

This publication provides guidance on developing and implementing computer security as a key component of nuclear security. This publication applies to the computer security aspects of nuclear security and its interfaces with nuclear safety and with other elements of a State's nuclear security regime, including the security of nuclear material and nuclear facilities, of radioactive material and associated facilities, and of nuclear and other radioactive material out of regulatory control. The scope of this publication includes: computer based systems, the compromise of which could adversely affect nuclear security or nuclear safety; the roles and responsibilities of the State and of relevant entities in relation to computer security in the nuclear security regime; the activities of the State in establishing and implementing a computer security strategy for nuclear security; the elements of computer security programmes; and the activities to sustain computer security as part of the nuclear security regime.

INTERNATIONAL ATOMIC ENERGY AGENCY
VIENNA