NUCLEAR SECURITY SERIES NO. XX

NST045

DRAFT, December 2016

STEP 8: Submission to MS for comment

Interface document: NSGC, all SSCs

COMPUTER SECURITY FOR NUCLEAR SECURITY

DRAFT IMPLEMENTING GUIDE

FOREWORD

(Standard NSS Foreword to be added.)

CONTENTS

1. INTRODUCTION

BACKGROUND

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

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

1.3. The Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5) [2] state that:

> "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."
> (Ref. [2], paras 4.10)

1.4. The security of sensitive information is a component of Essential Element 3 for a national nuclear security regime: Ref. [1] states that: "the legislative and regulatory framework should 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 Materials [3] also identifies the protection of the confidentiality of information as its Fundamental Principle L.

1.5. The Nuclear Security Recommendations for other radioactive material and associated facilities [4] and for nuclear and other radioactive material out of regulatory control [5] also stress the need to protect sensitive information from compromise or malicious access.

1.6. When computer-based systems are used to process, transmit and store such a information, adequate protection of its confidentiality, integrity and availability cannot be achieved without 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. Threats have identified cyber-attacks as a means to target computer-based systems, whether directly or in combination with more conventional means such as physical access and insiders, to carry out or facilitate malicious acts, which could have unacceptable radiological consequences.

1.8. A nuclear security regime cannot address the range of potential nuclear security threats without consideration of those who have or can acquire skills in using computer-based systems for cyber-attacks. Furthermore, nuclear security threats that 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 and other radioactive material, as well as in associated activities such as transport, is a significant challenge, due 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 require effective computer security.

OBJECTIVE

1.10. The objective of this publication is to provide guidance on developing, implementing and integrating computer security as a key component of nuclear security.

1.11. This Implementing Guide is intended for policy makers, competent authorities, operators (including, for example, facility management, staff with security responsibilities, technical staff, vendors and contractors), nuclear security professionals and nuclear safety professionals.

SCOPE

1.12. The guidance in this publication applies to the computer security aspects of nuclear security[1] and its interfaces with nuclear safety and with other elements of a State’s nuclear security regime, such as physical protection, detection of and response to nuclear security events and information security.

[1] In Ref. [2], the term “physical protection” has been used to describe what is now known as the nuclear security of nuclear material and nuclear facilities.

The scope of this publication includes those computer-based systems that, if compromised, could adversely affect nuclear security.

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 can be found in IAEA Nuclear Security Series technical guidance and other supporting documents.

1.14. This publication refers to guidance on information security in the Nuclear Security Fundamentals [1] and Recommendations [2, 4 and 5], but does not provide detailed guidance on this general topic. A separate Implementing Guide [6] provides guidance on information security and the identification and protection 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 other roles and responsibilities. Section 5 describes the activities of the State in developing a computer security strategy for nuclear security, and Section 6 describes activities for implementing the strategy. Section 7 describes the recommended elements and measures for the computer security plan. Section 8 describes activities to sustain the strategy.

1.16. Annex I provides an overview of the cyber threat. Annex II discusses the assignment of computer security responsibilities in the nuclear security regime. Annex III provides and enhanced discussion of the nuclear safety-security interface with respect to computer security. Finally, Annex IV provides an illustration of a framework for computer security competence development.

2. CONCEPTS AND CONTEXT

KEY TERMINOLOGY

2.1. A State creates, processes, handles and stores many types of information. It may deem some of this information sufficiently important to require specific protection. The State may establish national information security laws defining and classifying such information and define specific protection requirements, including those for data in electronic form and for associated computer-based systems.

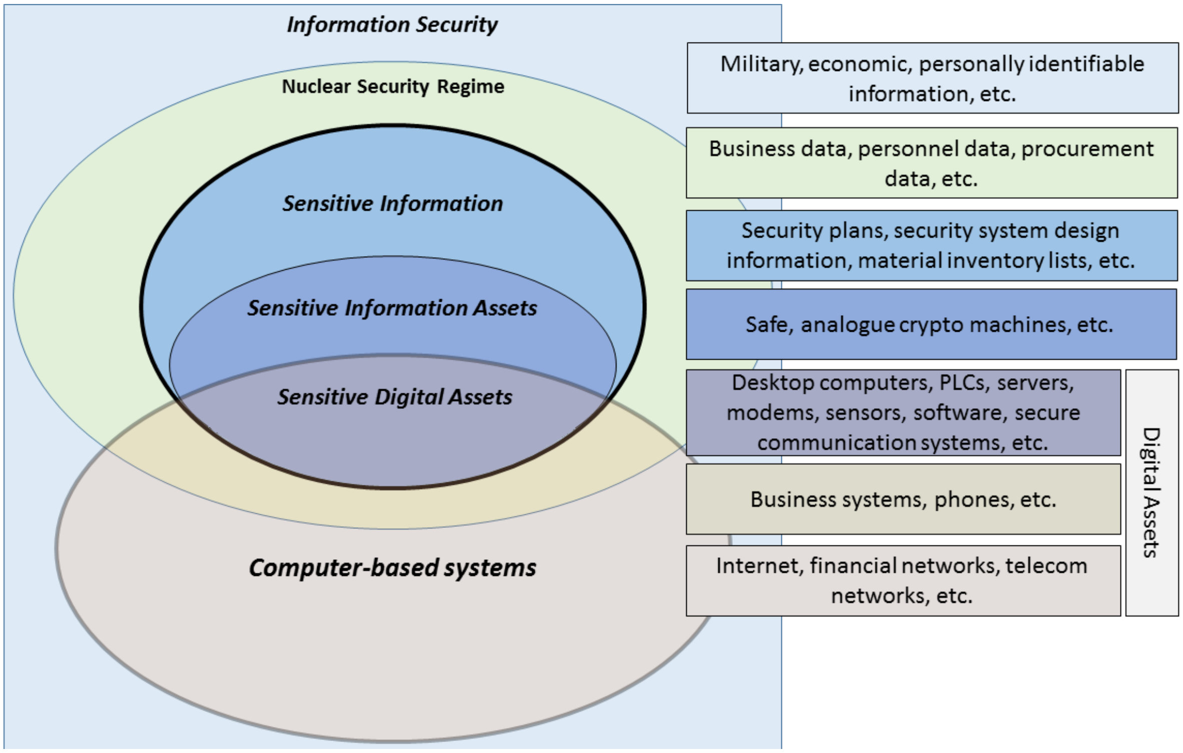

Information Security
Nuclear Security Regime
Sensitive Information
Sensitive Information Assets
Sensitive Digital Assets
Computer-based systems
Military, economic, personally identifiable information, etc.
Business data, personnel data, procurement data, etc.
Security plans, security system design information, material inventory lists, etc.
Safe, analogue crypto machines, etc.
Desktop computers, PLCs, servers, modems, sensors, software, secure communication systems, etc.
Business systems, phones, etc.
Internet, financial networks, telecom networks, etc.
Digital Assets

FIG. 1. Illustration of information and information assets.

2.2. Information within the State’s nuclear security regime may be subject to these same requirements, but additional protection may be required for certain types of information that, if compromised could assist an adversary in carrying out a malicious act against a facility or activity, i.e. sensitive information. [1] Figure 1 illustrates this concept and indicates what is meant in this publication by sensitive information assets, computer-based systems and sensitive digital assets, as described below.

2.3. Sensitive information assets are defined [1] as any equipment or components that are used to store, process, control or transmit sensitive information. This applies whether the information is in electronic or any other format.

2.4. Computer-based systems are technologies that create, provide access to, process, compute, communicate, store, or control services involving digital information. Such systems include, but are not limited to, desktops and laptop computers, tablets and other personal computers, smart phones, mainframe computers, servers, virtual computers, 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.

2.5. Sensitive information assets need protection to prevent the compromise of the sensitive information that they store, process, control and or transmit. Protection approaches will vary depending upon the types of asset and the form of the information. Ref. [6] primarily addresses protection of written information on paper and other information in 'hard copy' form. The term sensitive digital assets (SDAs) is used in this publication to identify those sensitive information assets that are computer-based and need computer security measures for their protection.

2.6. SDAs support systems that perform nuclear safety, nuclear security or nuclear material accountancy and control functions, or that store and process sensitive information related to such functions. SDAs 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 nuclear safety. . Compromise of SDAs could potentially contribute to or result in, for example:

— Unacceptable radiological consequences;

— Unauthorized removal of nuclear or other radioactive material;

— Degraded capabilities to prevent, detect and respond to nuclear security events; or

— Loss of sensitive information.

2.7. Depending on the situation, software may need to be treated as information or as an integral part of computer-based systems or both. For example, in its initial design phase, software may be a high-level expression of a processing algorithm and best treated as information. In its operational 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. The application of computer security is essential for SDAs. In view of the interconnectivity of computer networks and information flow, however, computer security measures are 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

2.9. Designers of facilities and systems should identify all SDAs and their potential impact on nuclear security by a systematic process that identifies and evaluates digital assets in terms of their potential impact on system function if compromised. Computer security maintains the attributes of confidentiality, integrity and availability of sensitive information within SDAs, and of the SDAs themselves. Depending on the sensitive information and system function performed by the SDAs, consideration should be given for the preservation of each of these attributes.

2.10. The process should first identify the overall allocation of computer-based systems that directly support nuclear security (i.e. physical protection systems, nuclear material accountancy and control systems, and sensitive information systems) and nuclear safety objectives and respective functions.

2.11. The process should then conduct an initial consequence analysis of the digital assets within such systems to determine which assets that if compromised in a cyber-attack, could impact the required system functions thereby adversely impacting nuclear security, i.e. the SDAs. This concept is illustrated in Figure 2. This initial analysis should be conducted without accounting for existing computer security measures to determine what the “worst case” impact would be if the SDA were to be compromised.

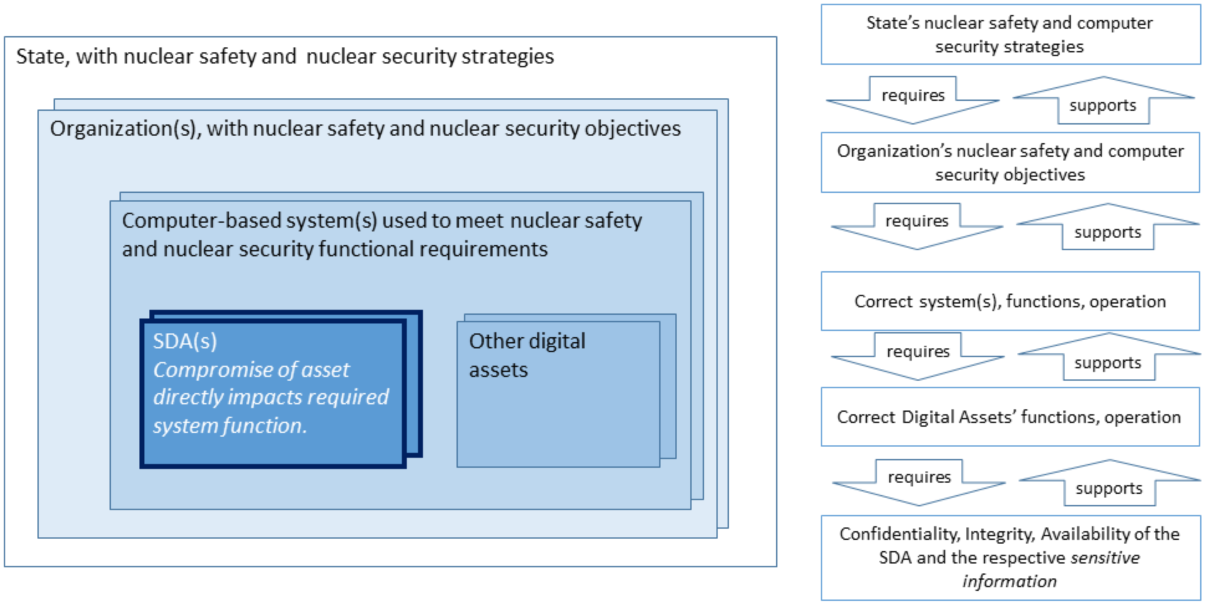

State, with nuclear safety and nuclear security strategies
Organization(s), with nuclear safety and nuclear security objectives
Computer-based system(s) used to meet nuclear safety and nuclear security functional requirements
SDA(s)
Compromise of asset directly impacts required system function.
Other digital assets
State’s nuclear safety and computer security strategies
requires
supports
Organization’s nuclear safety and computer security objectives
requires
supports
Correct system(s), functions, operation
requires
supports
Correct Digital Assets’ functions, operation
requires
supports
Confidentiality, Integrity, Availability of the SDA and the respective *sensitive information*

FIG. 2. Conceptual diagram of an SDA within a system within an organization.

2.12. The process should also evaluate support systems or equipment not directly associated with nuclear security and nuclear safety functions, for dependency relationships to determine whether cyber-attack on those systems or equipment could either directly or indirectly impact nuclear security and nuclear safety functions. Digital assets which have the potential capability to temporary connect to an SDA should also be evaluated for possible classification as an SDA. Examples of such systems may include maintenance computers and test equipment.

2.13. Organizations may choose different strategies to manage SDAs. This may include the grouping and collective management of SDAs within a particular system, of those that are similar in nature. For example, a computer-based system that performs an important function may be treated as one SDA or as a set of SDAs.

2.14. The requirements for confidentiality, integrity and availability of each SDA should be determined by the contribution of that SDA to nuclear safety and nuclear security and the potential consequences of improper operation of that SDA following a cyber-attack. This determination may call for domain expert judgement, guided by principles and assessment.

2.15. Until a computer-based system has been evaluated to determine whether or not it is an SDA should be treated as 'unassigned'. The computer security measures for unassigned computer-based system 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 such assets within the nuclear security regime. For example, personal telephones may be prohibited within nuclear facilities; and third party computers may be prohibited from connection to any system at a nuclear facility until fully assessed.

2.16. 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.

2.17. Particular care should be taken if using virtual and contracted services, such as cloud computing, as SDAs, as such services include elements that are not under the data owners' 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, There should be stringent (contractual) requirements, such as for access control, segregation of data, data destruction, etc., on the communication interface, software, hardware, and administrative processes in order to protect the application unauthorized access and manipulation.

2.18. SDAs may be industrial control systems, information technology (IT) systems, or a combination of the two. Computer security should use measures that are appropriate to the different types of system. However, these measures often cannot be treated completely separately, due to the existence of common interfaces, and therefore the set of computer security measures applied should be coherent with the approaches adopted for both types of system.

2.19. As in other specialized domains such as aerospace, the nuclear security community has applied processes, commonly referred to as 'life cycle models', 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, 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 assets including SDAs and should be considered in the context of the life cycle for a facility

CYBER-ATTACK

2.20. The term 'cyber-attack' is used in this publication to describe a criminal or intentional unauthorized act directed at or affecting computer-based systems with the intention of achieving or facilitating the theft, alteration, prevention of access to or destruction of sensitive information or sensitive information assets. Cyber-attacks jeopardize the confidentiality, integrity, availability[1] or a combination of these properties, of the sensitive information within an SDA, or of the SDA itself.

2.21. A cyber-attack may be carried out through direct physical access to the information or assets, or through electronic access, or a combination of the two, and may 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, are treated as computer security incidents.

[1] Other properties such as authentication and non-repudiation are considered to be included in protecting confidentiality, integrity and availability.

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

2.23. In this publication the term ‘computer security’ is used to cover the security against cyber-attack of computer-based systems as described above, and of all interconnected systems and networks of which such systems are elements. The terms IT security and cyber security are, for the purpose of this publication, considered synonymous with computer security and are not used. Computer security is a subset of information security, as discussed in Ref. [NSG23]. Information security and computer security often share objectives, methodology and terminology.

2.24. Computer security aims to maintain the 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 computer-based systems that support the nuclear security regime.

COMPUTER SECURITY ACROSS NUCLEAR SECURITY

2.25. The nuclear security regime addresses the three domains covered in Refs [2], [4] and [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 materials and nuclear facilities

2.26. The physical protection of nuclear material and nuclear facilities depends upon security measures to:

- Protect against unauthorized removal;
- Locate and recover missing nuclear material;
- Protect against sabotage; and
- Mitigate or minimize effects of sabotage.

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

Radioactive material and associated facilities

2.28. 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.

2.29. 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 incident response.

Nuclear and other material out of regulatory control

2.30. Material out of regulatory control (MORC) is nuclear or other radioactive material that should be under regulatory control, but is not under control, either because controls have failed 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.

2.31. 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 processes.

COMPUTER SECURITY COMPETENCES AND CAPABILITIES

2.32. 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 specific computer security competences and capabilities.

THREAT, VULNERABILITY AND COMPUTER SECURITY MEASURES

Threat

2.33. A nuclear security threat is a person or group of persons with motivation, intention and capability to commit criminal or intentional unauthorized acts involving or directed at nuclear material, other radioactive material, associated facilities or associated activities or other acts determined by the State to have an adverse impact on nuclear security.[1] A person or group of persons actually attempting such an act is an adversary.

2.34. An understanding of the cyber threats 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 may have in planning and conducting a cyber-attack. Annex 1 provides some examples of general characterizations of the threats of cyber-attack.

Vulnerabilities

2.35. Vulnerabilities are weaknesses in security. Such weakness may be administrative, physical or technical in nature. Through exploitation of vulnerabilities, an adversary may 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 upon its potential to adversely affect the operation of the SDA and the respective system function.

2.36. The complexity of both hardware and software in computer-based systems is continuously increasing, as is the number of computer-based systems and their interconnectivity. This complexity often leads to a lack of understanding of system, and thus of the expertise necessary for security management. The number of vulnerabilities in a system can be related to its complexity.

2.37. The exploitation of newly discovered vulnerabilities forms the basis for many successful cyber-attacks. Zero-day attacks are situations in which the adversary exploits a vulnerability before the defender is aware of its existence. Furthermore, the rapid evolution of new computer technologies provides opportunities for the nature of vulnerabilities to change, with entire new classes of vulnerabilities only emerging after these new technologies have become operational and been adopted.

[1] The term “nuclear security threat” is equivalent to “threat actor”, which is often used in computer security standards and guidance.

2.38. Due to the complexity of, and the possibility of hidden vulnerabilities in some computer-based systems, it may not be possible to make them sufficiently secure to achieve the desired level of risk for use in specific nuclear security and nuclear safety applications.

A graded approach to computer security measures

2.39. Computer security measures may be technical, physical or administrative, or a combination of these. A combination of 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.

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

2.41. Organizations may adopt 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 each 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 those SDAs for which the potential consequences of being compromised are similar are provided with similar levels of protection. Once identified and categorized according to their potential consequences if compromised, a graded approach, using defence in depth, can be applied.

2.42. One practical way to implement a graded approach is to group computer-based systems and the associated SDAs into zones, where graded protective measures are applied for each zone based on the level of security considered necessary for the zone. If the security levels approach is used, the security level applied to a zone is the level of the SDA(s) within the zone considered to need the highest level of protection.

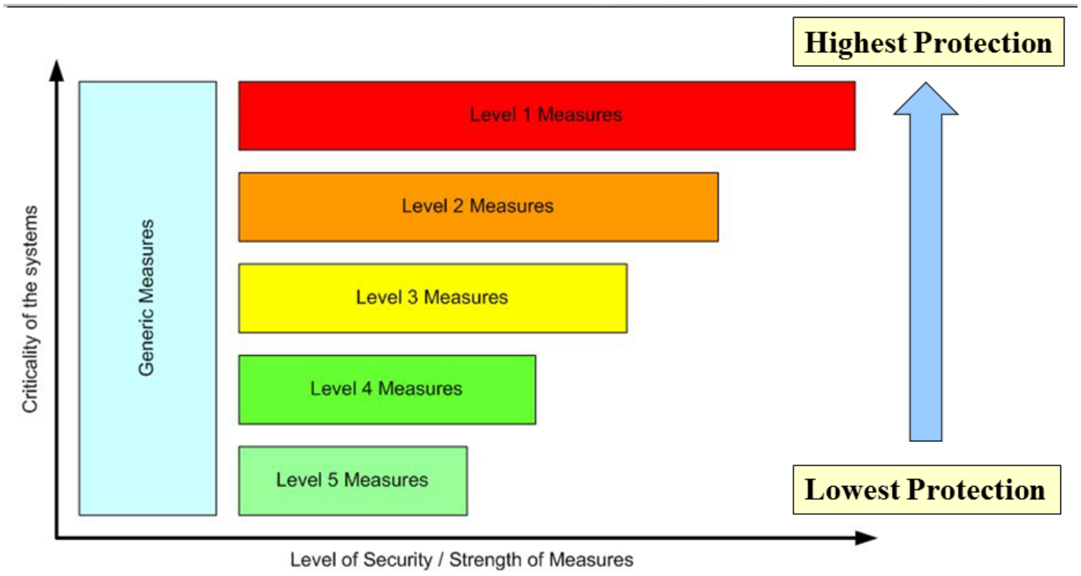


FIG. 3 Illustration of the graded approach using the security level concept.

2.43. The use of levels and zones is a graded approach to identify computer security measures that are proportionate to the potential consequences of the failure of those measures. In the illustration in Figure 3:

— Level 1 measures would be applied for those SDAs that, if compromised, operation could lead to the most severe consequences, including the most significant nuclear security events.

— Lower level measures, for example levels 4 and 5, might be applied for computer-based systems that have nuclear security related functions but that are not considered SDAs.

— Generic measures would be applied to all computer-based systems with nuclear security related functions, and may include measures that are common to computer-based systems in other areas.

2.44. 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 security measures across all computer systems provides defence in depth against cyber-attacks. In the above example, computer-based systems in zones with Level 5 measures might not be categorized as SDAs, but some protective measures are applied to provide layers of defence against intrusion and compromise of zones of higher levels.

2.45. 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 affect an SDA. The appropriate combination of complementary and overlapping computer security measures provides defence in depth. Further, defence in depth is achieved not only by implementing multiple security boundaries, but also by implementing computer security measures that assess, prevent, detect, protect, respond, mitigate and recover from an attack on an SDA. For example, if a failure in prevention were to occur (e.g., a violation of mobile media usage policy) or if protection mechanisms were to be bypassed (e.g., by a new virus that is not yet identified as a cyber-attack), mechanisms would still be in place to detect and respond to an unauthorized alteration in an affected SDA.

2.46. Effective defence in depth also requires that, by design, no single failure 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 demands diversity of devices, configurations or other measures.

2.47. Defence in depth may depend on a system design comprising zones of different computer security strengths, often visualized as concentric rings. A general principle is that direct connections should only exist between adjacent computer security zones.

2.48. A contribution to defence in depth may also be achieved by ensuring organizations have complementary roles and responsibilities in computer security.

2.49. Identifying threats, vulnerabilities and evaluating risk provides the risk-informed basis for determining proportionate security measures. Risk is the potential that a given threat will exploit vulnerabilities and that such threat activities could lead to adverse impacts on SDAs and nuclear safety and nuclear security. Risk is a function of the likelihood of an event 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 Figure 4:

- Computer-based system owners in nuclear security regimes (i.e. Asset owners) seek to avoid nuclear security events and thus seek to minimize risks of computer security incidents that could contribute to nuclear security events.

- Threats may wish to cause nuclear security events. Threats may target SDAs for compromise and/or sabotage.

- Consequently, threats initiate threat activity that exploits vulnerabilities that lead to computer security risks to SDAs; those risks of computer security incidents can lead to nuclear security events.

- Asset owners impose computer security measures to reduce computer security risks to SDAs.

- A risk-informed approach may consider the likelihood of particular computer security incidents when determining proportionate computer security measures. Risks may be reduced by eliminating the threat, imposing computer security measures that decrease the likelihood the exploit resulting in a computer security incident or by limiting or mitigating the severity of the impact of the computer security incident.

- Risk identification and the associated risk management should be continual processes responsive to changes in risk factors.

2.50. In most cases, a certain level of residual risk will remain. The acceptance of such residual risks should be an informed decision.

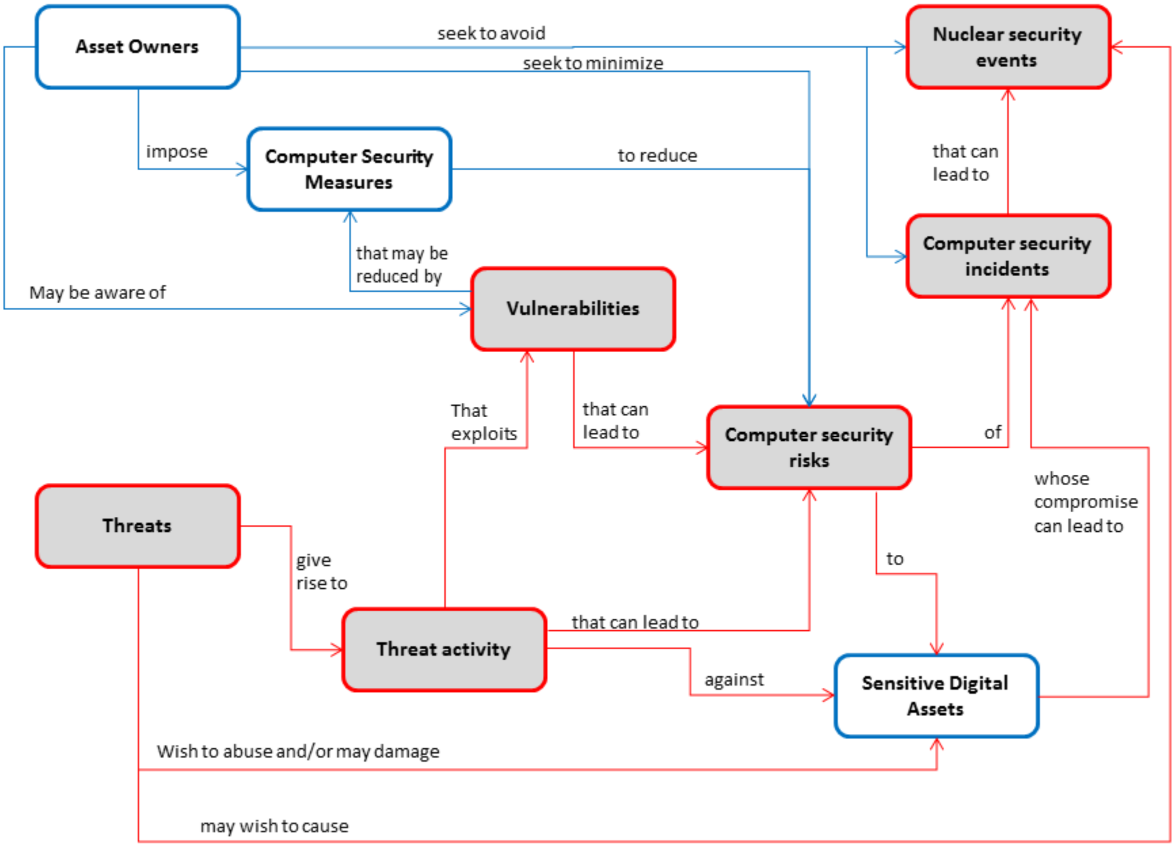


FIG. 4: Risk-informed approach to computer security measures (adapted from ISO 13335–1 2004)[9]

Computer security responsibilities within a nuclear security regime

2.51. Many organizations within a nuclear security regime use computer-based systems for functions that include, but are not limited to, information processing, nuclear security, nuclear safety and nuclear material accountancy and control functions.

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

2.53. Figure 5 provides a visualization of the organizations in a nuclear security regime that may have computer security responsibilities. The entities include competent authorities and operators[1], which have responsibilities for computer security in the nuclear security regime that are assigned through national law and regulation. Contractors, vendors and suppliers include organizations which provide goods and services to competent authorities and operators, but whose computer security responsibilities (e.g. to protect sensitive information and associated SDAs) may not be derived from national legal and regulatory requirements, but may arise from conditions specified in their contracts with competent authorities and operators.

2.54. The expectation for computer security of the State, competent authorities[2], operators, contractors, vendors and suppliers is further discussed.

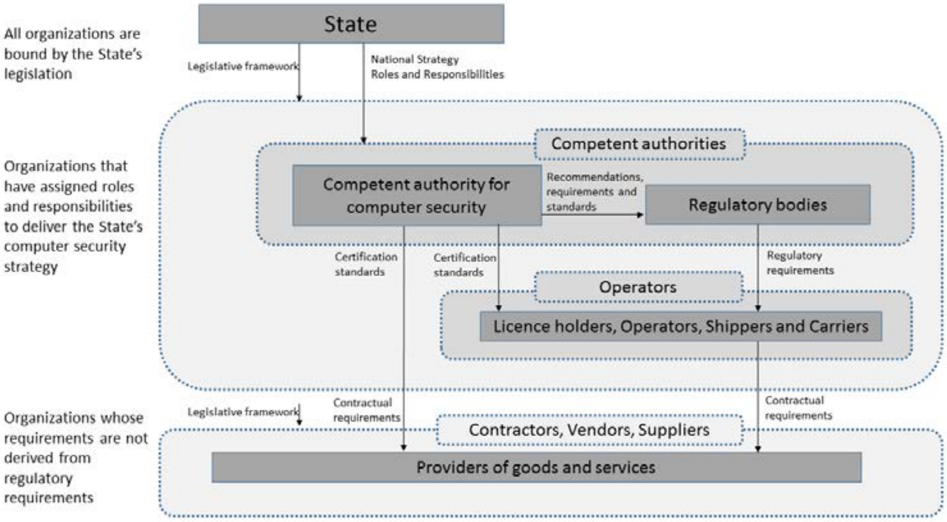

State
All organizations are bound by the State's legislation
Legislative framework
National Strategy
Roles and Responsibilities
Organizations that have assigned roles and responsibilities to deliver the State's computer security strategy
Competent authorities
Competent authority for computer security
Recommendations, requirements and standards
Regulatory bodies
Certification standards
Certification standards
Regulatory requirements
Operators
Licence holders, Operators, Shippers and Carriers
Organizations whose requirements are not derived from regulatory requirements
Legislative framework
Contractual requirements
Contractual requirements
Contractors, Vendors, Suppliers
Providers of goods and services

FIG. 5 Organizations with computer security responsibilities in a nuclear security regime.

[1] Operators in this publication refer to the range or licensed entities in a nuclear security regime including operators, shippers, and carriers.

[2] Competent authorities also include police, rescue, border guard, defence forces which have a role in securing facilities and activities and in detection and response to MORC.

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 document as “the strategy”). The State should designate a competent authority as having lead responsibility in the development of the strategy.

COMPETENT AUTHORITY FOR COMPUTER SECURITY IN THE NUCLEAR SECURITY REGIME

3.2. The State should designate a competent authority as having lead responsibility in the development and implementation of the legislative and regulatory framework for computer security based upon this strategy.

3.3. The State should designate a competent authority with responsibility for computer security in the nuclear security regime from among its competent authorities. The State may establish multiple competent authorities for computer security in its nuclear security regime to represent the multitude and diversity of activities. As an example, the competent authority for computer security for nuclear power facilities will likely be different from the competent authority for computer security for border monitoring operations.

3.4. When there is more than one competent authority for computer security in the nuclear security domain, or it is different from the competent authority responsible for nuclear security, the State should ensure the close cooperation between the respective organizations. This coordinating body or mechanism should be chosen to ensure clarity over responsibility and accountability for every aspect of computer security across all competent authorities.

RELEVANT ENTITIES IN THE NUCLEAR SECURITY REGIME

3.5. The State should identify all the competent authorities and operators with roles and responsibilities relating to computer security in the nuclear security regime and ensure each entity falls under the appropriate competent authority for computer security in the nuclear security domain

3.6. The State should consider including all levels of competent authorities[1] and operators. Annex II offers a typical list of nuclear security responsibilities from which computer security assignments may be inferred, according to the nature of the State’s nuclear regimes and their SDAs.

[1] Consideration should be given to any coordinating body or mechanism, law enforcement, customs and border control, intelligence and security agencies, health and environment agencies.

3.7. The State should require the identified competent authorities and operators to develop and implement computer security plans (CSP) in accordance with the strategy.

3.8. The State should define and assign computer security responsibilities to all such entities.

3.9. Some supporting organizations may not be within the authority of the State's regulatory bodies, but have a critical role in supporting and 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 contractors, vendors and suppliers.

LEGISLATIVE AND REGULATORY CONSIDERATIONS

3.10. The State should ensure that computer security is appropriate 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 measures that will ensure the proper implementation of computer security within nuclear security.

3.11. The State should ensure that its current legislation criminalizes cyber-attacks on nuclear security regimes. Computer security may need special legislative provisions to take into account the unique crimes and modes of operation associated with cyber-attacks.

3.12. The State should ensure that sanctions for intentional unauthorized acts against SDAs are part of its legislative or regulatory framework.

3.13. The State should consider other laws, international legal instruments and conventions to inform/define computer security and its implementation. These may include:

- Laws concerning computer offenses;
- Laws on terrorism;
- Laws on the protection of critical national infrastructure;
- Laws mandating disclosure of information;
- Laws on privacy and handling of personal information;
- International instruments such as conventions on cybercrime.

3.14. The State should continuously review and update its legislation and regulatory framework to include provisions for new and emerging cyber threats and vulnerabilities.

3.15. The State should designate the lead competent authority[1] for computer security 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"). Such laws and regulations may extend beyond the nuclear security regime.

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

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

INTERFACES WITH OTHER DOMAINS

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

3.19. The State should ensure that the strategy defines the interfaces between computer security and all other relevant domains in order that respective competent authorities and operators understand their roles and responsibilities for those interfaces.

3.20. For each respective competent authorities and operators, some of the following interfaces will be internal – within the relevant entity's organization – and some will be external. This distinction is a key determinant in defining the nature of the interface.

Nuclear safety

3.21. Nuclear security and nuclear safety have in common the aim of protecting persons, 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

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

that security measures do not compromise safety and safety measures do not compromise security [1].

3.22. Computer security represents one of the greatest interfaces across nuclear security and nuclear safety especially when considering the shift to computer-based systems within all operational aspects of nuclear facilities.

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

3.24. Any nuclear safety function that uses a computer-based system will in general rely for its proper operation upon the principles of availability, integrity, and to a lesser degree confidentiality. Maintaining these principles are at the core of computer security measures. 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 safety requirements are considered together.

3.25. There should be a causal relationship between safety levels and computer security levels for digital assets, to ensure that a digital asset assigned to a particular safety level has the appropriate computer security protection. There is not necessarily a simple equivalence between safety levels and computer security levels. The determination of appropriate computer security levels will depend on the particular digital asset within the context of the system and the organization. This determination will require the appropriate competences and capabilities, using judgement informed by principles.

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

3.27. Maintenance, operations and engineering staffs should be aware of both the safety and security significance of instrumentation and control features.

3.28. Appendix I describes further considerations for the State when designing the interface with the safety domain.

Physical protection[1]

3.29. Physical protection systems, for example those systems performing physical access control, security monitoring and detection, alarm and response functions often rely on computer-based systems. Malicious compromise of the computers associated with these systems (i.e. compromise of the confidentiality, integrity and/or availability) could result in reduction of the physical protections system function and could support physical actions aimed at material theft or system sabotage. Computer security should be implemented as an integral part of the life cycle processes of computer-based systems used for physical protection measures.

3.30. Physical protection measures such as physical access control are a valuable component of computer security implementation and should be considered for protection of computer-based systems.

3.31. Some States may treat computer security as part of physical protection, as defined in Ref. [2]. This publication treats computer security as a separate topic, distinct from physical security, to clarify and emphasize the differences. The nature of the interface to the physical protection domain will depend upon the circumstances in each State.

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

3.33. Maintenance, operations and engineering staffs for physical protection systems should be aware of both the cyber-threat and potential impact on physical protection system functions.

Information technology and operational technology functions

3.34. The responsibility for the management and security of IT systems and operational technologies (including industrial control and instrumentation and control systems) are often different departments within an organization. An effective interface and collaboration between these groups is essential for comprehensive security of the associated SDAs used within each system. Past cyber-attacks have shown the use of IT systems as both a resource for reconnaissance and a vector for attack against operational technologies.

3.35. There may be differences of procedures, vocabulary and risk assessment between those responsible for IT systems and those responsible for operational technologies. Misunderstandings

[1] Physical protection for the purposes of this publication refers to personnel, procedures, and equipment that prevent physical access, theft, and damage to nuclear materials and associated systems.

and inconsistent application of computer security measures between them represent a significant source of risk to the nuclear security regime.

3.36. This interface is very likely to be a mixture of internal and external (e.g. contractor, vendor, and supplier) relationships.

Intelligence organizations

3.37. The State should ensure that intelligence organizations provide appropriate support to contribute to or maintain an accurate and up-to-date national threat assessment including the threat of cyber-attack against the nuclear security regime. Protocols and processes should be in place to support the transfer of cyber threat information to relevant parties within the nuclear security regime as appropriate to ensure adequate computer security against changing threat situations.

3.38. The State should ensure that intelligence organizations have knowledge of the nuclear security regime including the types of SDA that may exist.

Response organizations

3.39. 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 notify the relevant competent authorities so that appropriate response action can be initiated.

3.40. Contingency plans should include provisions for responding to cyber-attacks and/or blended attacks.

International assistance and cooperation (including information exchange)

3.41. States are encouraged to cooperate between each other or with identified international organizations, when appropriate, to secure SDAs and associated sensitive information and in order to identify threats of cyber-attack. Confidence-building and improved computer security can be achieved through sharing information, and its analysis, regarding vulnerabilities, threats, and computer security incidents in a timely manner. This information should be appropriately protected.

3.42. The State is encouraged to engage periodic advisory or assessment services to evaluate its strategy, consequent computer security plans, and their implementation in the State’s nuclear security regime.

3.43. 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 threats that are transnational.

4. ROLES AND RESPONSIBILITIES OF RELEVANT ENTITIES

4.1. Computer security is a cross cutting issue for the competent authorities and operators in a nuclear security regime. All such entities have a level of responsibility in the protection of SDAs. This section discusses their associated responsibilities.

4.2. Competent authorities and operators are both generators and consumers of sensitive information, which is often processed by, resides on or is integral to SDAs. Competent authorities and operators should implement computer security measures to protect SDAs and the associated sensitive information.

4.3. Competent authorities and operators should identify their SDAs and characterize them based on their potential impact on nuclear safety and nuclear security and define within their CSP the level of computer security measures required for 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 be:

— designed to deny unauthorized access of persons, processes and/or equipment to SDAs (in accordance with a graded approach).

— in place to ensure that malicious code or data are not introduced into SDAs.

— integrated into competent authority's supply chain management arrangements.

4.5. Competent authorities and operators should use a formal process to ensure personnel deemed trustworthy, competent, and authorized perform all 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 interface between safety and security activities [4] in a manner to ensure that they do not adversely affect each other and that, to the degree possible, they are mutually supportive.

4.8. Each competent authority and operator should maintain a computer security plan that describes how it will provide adequate computer security for its SDAs, as required by the State and its competent authorities. Note that in certain cases, relevant entities may share or depend on each other's SDAs and competent authorities and operators should reflect all shared responsibilities or dependencies in their CSPs.

4.9. Competent authorities and operators should periodically evaluate that their computer security measures comply with regulatory requirements. The period between evaluation and assessment should be of a frequency to take into account changes in risk. These assurance activities may include audits, reviews, performance testing, exercises, etc. Competent authorities and operators should also conduct self-evaluations when computer-based systems are modified because modifications may induce new vulnerabilities and create new SDAs.

WORKING WITH CONTRACTORS, VENDORS AND SUPPLIERS

4.10. Competent authorities and operators should place contractual requirements on contractors, vendors and suppliers to implement computer security measures that are commensurate with their support or contractual interface. The contractual requirements should specify computer security measures to ensure that neither party is a cyber-attack vector for the other and that respective sensitive information is protected.

4.11. Competent authorities and operators and respective contractors, vendors and suppliers should maintain protocols and procedures for the timely communication of computer security incidents that have the potential to affect each other.

COMPETENT AUTHORITY FOR COMPUTER SECURITY

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

4.13. The competent authority for computer security should ensure such requirements reflect both the strategy and the unique operational and security requirements of each competent authority or operator and its demonstrated capabilities and competences in computer security.

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 lifecycle of SDAs for which they have responsibilities, e.g. design, implementation, maintenance, and final disposition, are appropriately controlled and monitored/recorded.

4.16. Each competent authority should verify continued compliance with its computer security regulations through regular evaluations and, when necessary, ensuring corrective action.

4.17. The competent authority for computer security may prescribe specific computer security measures (i.e. a prescriptive approach) for the competent authority or operator to implement. Alternatively the competent authority for computer security may define performance-based requirements for computer security requirements, allowing the competent authority or operator to use a risk-informed approach to determine proportionate computer security measures. The competent authority for computer security may employ the two approaches in combination.

4.18. The criteria for the selection of a performance-based approach or a prescriptive approach will depend on the State’s legislative framework and organizational structure and several other factors such as:

— The competence of the operator to interpret performance requirements and to design, implement, and evaluate an effective physical protection system;

— The number of facilities and operators that will be governed by the regulation, and the extent to which prescriptive requirements limit the flexibility of the operator to develop appropriate protective measures;

— The severity of the potential consequences of the malicious acts that are to be prevented. [7]

Performance-based method

4.19. In the performance-based method, the competent authority for computer security defines computer security objectives and requires the competent authority or operator to design and implement computer security measures that meets those objectives, achieving a specified level of effectiveness in protecting against cyber-attacks and providing contingency responses.

4.20. The performance-based method allows flexibility for the competent authority or operator to propose an organization-specific combination of 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 method is that it recognizes that many different combinations of security measures can achieve an effective computer security, and that each organization and its operational circumstances may be different.

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

Prescriptive method

4.22. In the prescriptive method, the competent authority for computer security establishes specific computer security measures that it considers are necessary to meet its defined computer security objectives for that SDA in the circumstances of that organization.

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

4.24. The prescriptive method may lack flexibility to address specific circumstances. Furthermore, with this method the respective 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 respective competent authority or operator only has the responsibility for the effectiveness of the individual computer security measures for each SDA.

Combined approach

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

- To require application of a performance-based method for circumstances where the potential impact is for example high or very high, while allowing application of a prescriptive method where the potential impact is for example low or very low;
- The State may require that a set of prescriptive requirements be followed to address certain defined aspects of security (e.g. the protection of sensitive information), supplementing measures to address all other aspects derived using the performance-based method.
- The main advantage of the combined approach is the flexibility it allows. The limitations of a combined approach will be similar to those associated with the performance and prescriptive-based methods and will depend on the specific implementation. However, a well-executed combined approach may provide an appropriate balance and reduce the effects of the limitations associated with each of the other approaches.

REGULATORY BODY

4.26. The regulatory body[1] should establish regulatory requirements to implement computer security measures to protect SDAs and the associated sensitive information. The regulatory body should ensure through regulation that the regulated party performs its computer security as defined.

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

4.28. It is recommended that the regulatory body issue a guide to its regulation to assist regulated parties with its implementation. The guide should periodically be reviewed to ensure it adequately address the cyber threat and objectives of the regulation.

4.29. The regulatory body should ensure computer security is part of evaluation and licensing or other procedures to grant authorization to regulated parties.

4.30. The regulatory body should ensure that each regulated party addresses computer security in its CSP.

[1] There may be more than one regulatory body within a State, each having responsibility for nuclear security in different contexts; for example, a different regulatory body may be responsible for nuclear security in nuclear facilities from that responsible for nuclear security in industries using radioactive sources. In this publication, the singular term “regulatory body” is used to refer to whichever such body has responsibility in a particular context.

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

5. ESTABLISHING THE COMPUTER SECURITY STRATEGY

COMPUTER SECURITY STRATEGY FOR THE NUCLEAR SECURITY REGIME

5.1. The strategy[1] 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 elements:

- How threat assessment is performed including the identification of possible cyberattack scenarios
- How computer security objectives are determined
- How competences and levels of capability in computer security can be specified
- Assigning computer security roles and responsibilities for all competent authorities and, operators (and possibly contractors, vendors, or suppliers)
- Identifying and establishing new organizations or adaptation of computer security roles for existing organizations where capability gaps exist
- Implementing (integration and coordination) competent authorities' and operators', computer security activities
- Maintaining and sustaining computer security capabilities within the nuclear security regime

5.3. This and the following three sections (i.e. sections 5, 6, 7 and 8) provide further guidance on these elements, 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:

[1] 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.

- Performing threat assessment activities
- Quantifying the impact on nuclear security of a cyber-attack on SDAs
- Determining the use of performance-based vs. prescriptive approaches
- Specifying a framework for capabilities and competences in computer security
- Implementing (integration and coordination) competent authorities' and operators' computer security activities

ASSESSMENT OF CYBER THREAT 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 may additionally be used to develop a national threat statement or design basis threat (DBT).

5.6. The State's threat assessment and/or design basis threat should consider potential adversaries utilizing cyber capabilities, including the potential for insider activities and blended attacks.

5.7. Cyber-attacks allow for standoff attacks where the adversary initiates malicious acts outside the national jurisdiction that hosts the target site. The State should consider international threats in its assessment.

5.8. The State should ensure the threat assessment is updated regularly. The frequency of review of the threat relating to SDAs should reflect the rapidly evolving nature of technologies, advances in computer-based systems, newly discovered vulnerabilities, in changing nature of cyber-attacks (e.g. that can emerge and disappear within weeks) and in corresponding computer security approaches.

5.9. The State should ensure that changes to the cyber threat are communicated to relevant competent authorities' and operators' in a timely manner.

5.10. The State should take all reasonable steps to account for the changing nature of the cyber threat in order that computer security measures may anticipate changes and thereby remain effective.

5.11. In addition to national intelligence services, other competent authorities, operators, contractors, vendors and suppliers themselves may possess information that can inform the threat assessment process.

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

5.13. All 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 relevant entity. For competent authorities and operators implementing a DBT, this is often referred to as a 'beyond DBT event'. This distinction is illustrated in Figure 6.

5.14. In the case of physical threats, the criteria are often quantifiable. For threats of cyber-attack, defining the criteria above which State support is needed, becomes more challenging and will require skills and knowledge in computer security.

5.15. 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.

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

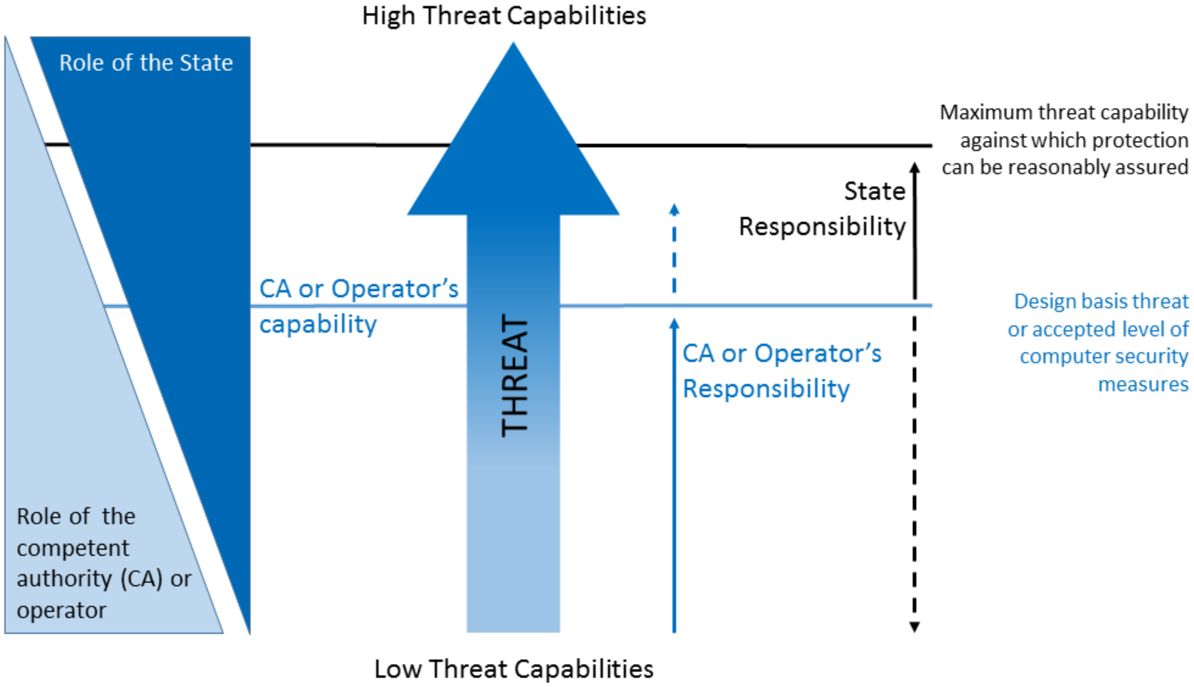

High Threat Capabilities
Role of the State
Maximum threat capability against which protection can be reasonably assured
State Responsibility
CA or Operator's capability
THREAT
Design basis threat or accepted level of computer security measures
CA or Operator's Responsibility
Role of the competent authority (CA) or operator
Low Threat Capabilities

FIG. 6 Roles and responsibilities for protecting against threats.

ASSIGNING A COMPETENT AUTHORITY FOR THREAT ASSESSMENT

5.17. The State should ensure that a competent assessment of the threat of cyber-attack is performed in a regular and timely manner. The State should assign to this role its most capable competent authority with respect to threat identification and assessment of cyber-attack. The competent authority for cyber threat assessment may be different from the competent authority for computer security.

5.18. The competent authority for cyber threat assessment should engage all competent authorities and operators identified by the State as having roles and responsibilities involved in analysis and assessment of threats of cyber-attack and having competences and capabilities in a formalized threat assessment process. Note that different, additional knowledge and skills will be required, compared with similar work on physical protection.

5.19. The competent authority for cyber threat assessment should lead the process of coordinating and combining these different assessments of threat of cyber-attack.

5.20. The competent authority for cyber threat assessment should be responsible for ensuring that the cyber threat assessment provides sufficient detail for the subsequent risk assessments that will lead to appropriate and effective implementation of computer security across the State’s nuclear security regime.

ASSESSMENT OF THE IMPACT ARISING FROM IMPROPER OPERATION OF SDAS

5.21. The competent authority for computer security should identify, for each of its constituent competent authorities and operators the maximum levels of consequences that should not be reached in case of a SDA's compromise..

5.22. Respective the competent authorities and operators should consider the severity of consequences independently from likelihood and should not consider the potential mechanism, e.g. type of cyber-attack that may lead to its occurrence. To clarify, assignment of the severity should be based upon the inherent characteristics and attributes of the SDAs.

5.23. Figure 7 provides a notional visualization of the varying impact levels for different types of nuclear security events across the domains of nuclear security as denoted by NSS13, NSS14 and NSS15. The competent authority for computer security should identify the severity of the consequence and determine the nature of computer security measures are sufficient to assure the mitigation of that undesirable outcome. This analysis will support the determination of the appropriateness of performance and/or prescriptive based measures for computer security for constituent entities.

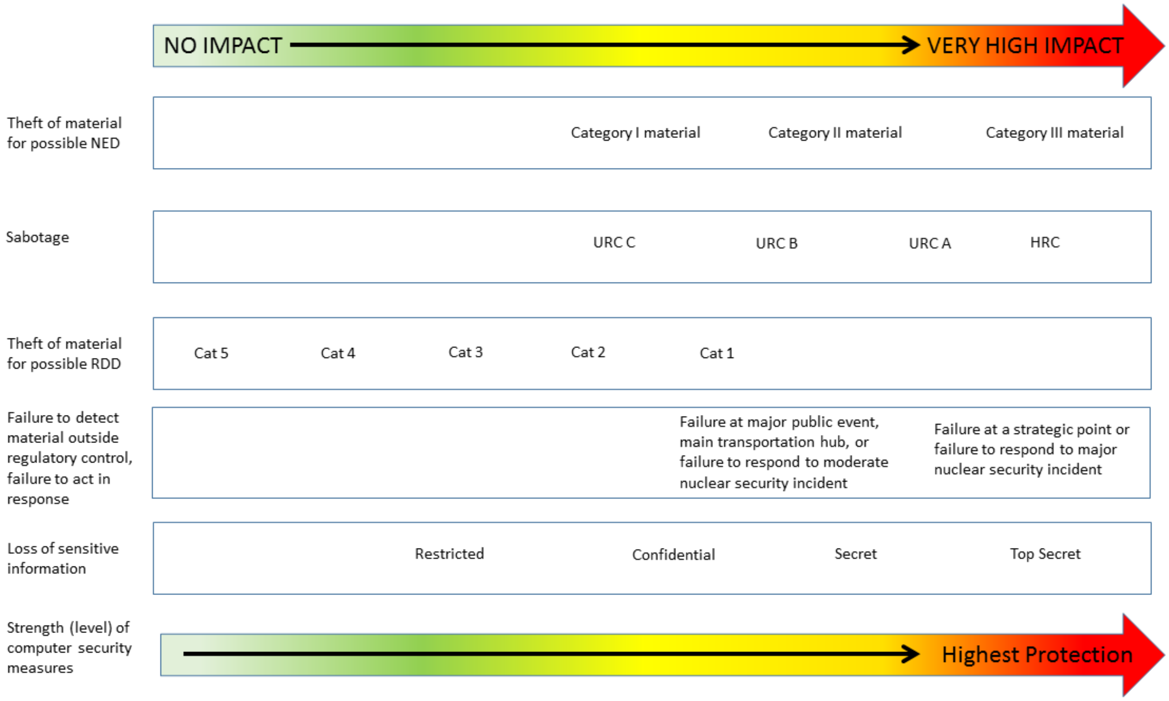

NO IMPACT
VERY HIGH IMPACT
Theft of material for possible NED
Category I material
Category II material
Category III material
Sabotage
URC C
URC B
URC A
HRC
Theft of material for possible RDD
Cat 5
Cat 4
Cat 3
Cat 2
Cat 1
Failure to detect material outside regulatory control, failure to act in response
Failure at major public event, main transportation hub, or failure to respond to moderate nuclear security incident
Failure at a strategic point or failure to respond to major nuclear security incident
Loss of sensitive information
Restricted
Confidential
Secret
Top Secret
Strength (level) of computer security measures
Highest Protection

FIG. 7. Illustration of varying impact levels for different types of nuclear security events.

5.24. The competent authority for computer security could identify (with prescriptive approach), in cooperation with other authorities, the levels of protection for levels of consequences. A framework of computer security competences and levels of capability

5.25. The implementation of computer security is complex, requiring a range of competences and levels of capability to suit the roles and responsibilities of each competent authorities, operators, contractors, vendors, and suppliers. Where judgement is required, the levels of capability will necessarily need to be higher. Effective computer security relies on being able to specify these competences and levels of capability for each competent authorities, operators, contractors, vendors, and suppliers and to gain assurance that they are being demonstrated and maintained.

5.26. 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 III.

5.27. The framework should ensure the computer security competences and levels of capability required for each competent authorities, operators, contractors, vendors, or suppliers is informed by the impact of any potential nuclear security event, and their responsibility for computer security measures that are designed to prevent or mitigate it.

5.28. Further guidance on defining roles, developing and maintaining competences within organizations, and on capacity building relating to organizations and individuals, is available in other Nuclear Security Series publications [11, 12].

RISK ASSESSMENT METHOD TO DETERMINE COMPUTER SECURITY REQUIREMENTS FOR EACH SDA

5.29. The application of computer security measures should be based upon a risk informed approach. The competent authority for computer security should define a method or sequence of methods that:

- Determines whether a computer-based system provides a relevant function for nuclear security regime ;
- Determines whether the digital asset is an SDA; and
- Performs a computer security risk analysis to produce a strength of measure for that SDA or other digital asset, illustrated in Figure 4.

5.30. The method should take into account the following

- Any relevant legislation or regulation;
- The importance of the SDA’s functions, including the confidentiality, integrity and availability of the SDA and of its sensitive information, for both safety (i.e. safety classification) and security;
- An assessment of the consequences of cyber-attack against that SDA;
- The operating environment for the SDA;
- Identification and assessment of threats to the competent authorities and operators, and respective contractors, vendors, and suppliers and to the SDA according to the national threat assessment or DBT or threat statement;
- The attractiveness of the SDA to potential threats; and
- The intrinsic vulnerabilities of the SDA.

5.31. The competent authority for computer security further modify the assessment results based on the potential impact if the asset is compromises, specifically if the resulting function results in:

- Function is indeterminate
- Function has unexpected behaviours or actions

- Function fails
- Function performs as expected (i.e. fault tolerant)

5.32. The risk assessment should consider all aspects of security collectively in order to address blended attacks, which can combine physical (including personnel, especially the ‘insider’) and cyber-attacks to be mutually supportive. Accordingly, those conducting the risk assessment should have access to individuals with competences from each of these areas.

6. IMPLEMENTING THE COMPUTER SECURITY STRATEGY

6.1. This section describes the responsibilities of the competent authority for computer security in its assignment of computer security responsibilities to each of the respective competent authorities or operators.

6.2. These responsibilities should be documented in the strategy or subsidiary documents.

6.3. The competent authority for computer security may place these requirements in its own recommendations, requirements, standard, in regulatory requirements via a regulatory body or in contractual requirements for contractors, vendors, or suppliers.

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 computer security responsibilities.

6.5. The competent authority for computer security should ensure that all competent authorities and operators, contractors involved in the life cycle of SDAs are assigned computer security responsibilities, including for the sustainability of the SDAs themselves.

6.6. The competent authority for computer security should ensure competent authorities and operators address computer security throughout the phases of computer security incident response: preparation; detection and analysis; containment eradication and recovery; and post-incident analysis [9].

6.7. The competent authority for computer security should identify the sharing of responsibilities between the State and the competent authorities and operators to ensure that the risks from the most capable adversarial threats are mitigated to an acceptable risk level.

COMPUTER SECURITY COMPETENCE AND CAPABILITY

6.8. 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 listing of the required competences for their organizations. Note that the competent authority for computer security may choose to conduct this analysis, particularly where the competent authority or operator has only prescribed computer security measures.

6.9. 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 perform the computer security requirements placed on them.

6.10. The competent authority for computer security should require competent authorities and operators to demonstrate that that all those charged with computer security responsibilities are deemed trustworthy, adequately trained, have sufficient skills and competence in their job function and have awareness of the threat from cyber-attack.

6.11. The competent authority for computer security should require competent authorities and operators to implement continuing maintenance programmes that develop the competences necessary to meet their computer security programme requirements.

6.12. The competent authority for computer security should encourage competent authorities and operators to develop metrics and assess their own levels of capability in the different competences to better develop and evolve their competences.

6.13. The competent authority for computer security should conduct assurance activities to evaluate computer security training and skills development of competent authorities and operators . The lead competent authority should place requirements on each competent authorities and operators to demonstrate continuing maintenance of its designated competences and levels of capabilities in computer security that are commensurate with its assigned computer security responsibilities

RELATIONSHIPS BETWEEN COMPETENT AUTHORITIES AND OPERATORS

6.14. The competent authority for computer security should make provision for the integration and coordination of computer security responsibilities between competent authorities and operators in the nuclear security regime and those outside it. For example, there may be additional national governance and other activities relating to computer security, outside the nuclear security regime, that will require coordination between governing bodies.

6.15. The competent authority for computer security should establish clear lines of responsibility and communication between the competent authorities and operators, and if applicable, coordinating bodies or mechanisms.

6.16. The competent authority for computer security should ensure a mechanism for computer security cooperation, coordination, information exchange and integration of computer security activities between competent authorities and operators.

6.17. When establishing competent authorities' and operators' computer security responsibilities, the competent authority for computer security should balance the competing demands of (i) the need for defence in depth and (ii) efficient and effective utilization of resources available to the State's nuclear security regime:

— Independence of thinking contributes to defence in depth because independent design choices and operational choices are less likely to suffer common failures. Independence includes both functional and financial independence from the entities they regulate and from any other bodies that deal with the promotion or 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 for independence in their computer security decision-making.

— The sharing of capabilities in this way improves the efficient and effective 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 required. In this example, the agreement between the relevant entities should specify the response time. The competent authority for computer security should ensure that arrangements are in place for competent authorities and operators whose capabilities need supporting by other competent authorities.

6.18. When considering the tension between independence and interdependence of competent authorities and operators, the competent authority for computer security should consider the resources required to protect against and respond to blended attacks, which may require the combination of computer security measures with other aspects of nuclear security (i.e. physical protection response forces). Implementation can rely on a multidisciplinary approach by several competent authorities.

6.19. Note that the combination of assigning responsibilities and assigning levels of competences and levels of capability may lead to the creation of new organizations, modification and/or reorganization of existing organizations.

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 plans for prevention, detection and response to computer security incidents.

6.21. The competent authority for computer security should provide guidance to competent authorities and operators as to what events might constitute a computer security incident. Such events may include the theft of sensitive information or the disruption of physical security and/or safety functions. Further, cyber-attacks may form part of blended attacks. Successful detection of subtle or attempted covert cyber-attacks may offer an advanced indicator of possible adversary intent.

6.22. The competent authority for computer security should ensure the existence of response capabilities of relevant response organizations, and competent authorities and operators to address computer security incidents, and define the criteria for which these capabilities would be activated within each of their CSPs.

6.23. The competent authority for computer security should define requirements for timely reporting of computer security incidents to the appropriate authority.

6.24. The competent authority for computer security should ensure that a competent authorities and operators with sufficiently advanced capabilities, e.g. one that is competent in computer security forensics, performs the technical characterization of any computer security incidents involving an SDA. Competent authorities and operators without advanced capabilities might not immediately recognize and understand the nature and significance of a computer security incident.

EXERCISES

6.25. The competent authority for computer security should ensure that nuclear security exercises 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 the CSP, including contingency plans. Where appropriate, these exercises should be integrated with other security exercises and on a periodic basis 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 the level of protection that is consistent with the threat assessment.

6.28. The competent authority for computer security should provide formal and regular assurance to the State that sufficient computer security capabilities and capacity exists across all competent authorities and operators, and development is in place for future needs, in light of the threat assessment.

Security qualification of parts and services

6.29. Security consideration in the procurement of equipment, parts, and services continues to be an area of high concern. Competent authorities, operators and their respective contractors, vendors, 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.

6.30. Competent authorities and operators should ensure that their respective contractors, vendors and suppliers that contribute to SDAs implement the required computer security measures (e.g. secure software development) with an aim to reduce the creation of vulnerabilities in SDAs and to prevent the use of the supply chain as a path for cyber-attack. This will include the use of reviews of methodologies, processes, and equipment.

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

6.32. The competent authority for computer security may designate a certifying authority that undertakes activities to assure that those contractors, vendors and suppliers designing, providing and supporting SDAs follow required computer security practices.

6.33. Competent authorities and operators are encouraged as appropriate to undertake further activities such as factory acceptance testing and contractual based computer security inspections at the supplier as additionally assurance checks.

INTERNATIONAL COOPERATION AND ASSISTANCE

6.34. The competent authority for computer security should ensure that the necessary relationships exist with other counterpart authorities in other States and with international bodies. The lead competent authority should consider those relationships in the light of the responsibilities, capabilities and competences of all the constituent entities.

7. DEVELOPING A COMPUTER SECURITY PLAN

7.1. This section describes recommended elements and measures for the computer security plan (CSP) for each relevant entity. These strategy or subsidiary documents should document these requirements.

7.2. The CSP is each competent authority's and operator's implementation of the strategy in the form of organizational roles, responsibilities, and procedures. The CSP also specifies the means for the competent authority and operator achieving the computer security objectives and/or computer security measures specified by legislation, regulation, standards and guidance by its regulatory body and competent authority for computer security.

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

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

COMPUTER SECURITY PLAN

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

7.6. The minimum table of contents of a CSP is suggested below.

(a) Organization and responsibilities:

(1) Organizational charts;

(2) Responsible persons and reporting responsibilities;

(3) Periodic review and approval process.

(b) Asset management:

(1) List of all computer systems;

(2) List of all computer systems applications;

(3) Network diagram, including all connections to external computer systems;

(4) Classification of digital assets and identification of SDAs.

(c) Risk, vulnerability, and compliance assessment:

(1) Security plan review and reassessment periodicity;

(2) Self-assessment (including penetration testing procedures);

(3) Periodic and as needed risk assessment;

(4) Audit procedures and deficiency tracking and correction;

(5) Regulatory and legislative compliance review.

(d) System security design and configuration management:

(1) Fundamental architecture and design principles;

(2) Requirements related to the different security levels;

(3) Formalization of computer security requirements for suppliers and vendors;

(4) Full life cycle security.

(e) Operational security procedures:

(1) Access control;

(2) Data security;

(3) Communication security;

(4) Platform and application security (e.g. hardening);

(5) System monitoring;

(6) Computer security maintenance;

(7) Incident handling;

(8) Business continuity;

(9) System backup.

(f) Personnel management:

(1) Vetting;

(2) Training;

(3) Qualification;

(4) Termination/transfer.

7.7. The CSP should be addressed in an integrated and coordinated manner within the entities' management system.

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

- new technologies being used in computer-based systems;
- new threats of cyber-attack including tools, techniques and practices;
- new types of computer security events.

7.9. Competent authorities and operators should conduct regular exercises to assess and validate their CSP, including contingency plans, and as a tool to train the various participants. Where appropriate, these exercises should be integrated with other security exercises and on a periodic basis conducted jointly with emergency exercises.

ORGANIZATION LEVEL RISK ASSESSMENT

7.10. Depending of the maturity of the competent authority or operator and the potential adverse impact from cyber-attack, the CSP may include a methodology for conducting a local risk assessment for all computer-based systems that takes into account the local environment.

7.11. The purpose of this assessment is

- to identify and understand risk as well as contributors to that risk;
- to serve as the basis for discovering which computer-based systems are digital assets and SDAs;
- to set a baseline to support analyses of changes to digital assets and SDAs, the threat and potential impact on computer security and the resulting impact on nuclear security; and
- to assist in validating higher-level requirements.

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

7.13. Such risk assessments should use the national threat statement (and/or DBT) and consider other available sources to inform the assessment process.

7.14. The risk assessment process should consider the adverse level of consequence on nuclear security or nuclear safety for the compromise and/or improper 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 operator should resolve this issue in a timely manner. Such deviations may result from but are not limited to changes in the local threat environment or equipment changes including newly identified vulnerabilities.

7.16. The risk assessment should consider all aspects of security collectively in order to address blended attacks, which can combine physical, personnel (including the insider) and cyber-attacks to be mutually supportive. Accordingly, the risk assessment should be conducted using experts from each of these areas.

COMPUTER SECURITY MEASURES

7.17. Computer security measures include procedures, practices, methods and provisions that provide prevention, detection, delay, response, and mitigation against compromise as well as ensuring that non-malicious acts do not lead to degraded computer security resulting in increased exposure to or susceptibility to malicious acts, i.e. cyber-attacks.

7.18. Specific computer security measures can be assigned to three categories:

- Technical: hardware and/or software solutions for the protection, detection and mitigation of and recovery from intrusion or other malicious acts to SDAs. The attributes of technical measures to provide continuous and automatic protective actions should be considered when evaluating effectiveness of other types of measures (physical or administrative).
- Physical: physical barriers for the protection of SDAs from physical damage and unauthorized physical access. The physical measures include barriers such as locks, physical encasements, tamper seals, isolation rooms, gates and guards, etc.
- Administrative: policies, procedures and practices designed to protect SDAs by controlling personnel actions and behaviours (such as security culture). The administrative measures are directive in nature, specifying what employees and third party personnel should and should not do. In the nuclear environment, administrative measures are understood to include operational and management measures.

A GRADED APPROACH FOR DETERMINING COMPUTER SECURITY MEASURES

7.19. Computer security measures should be based on a graded approach, where security measures are applied in proportion to the potential impact of a cyber-attack. One practical implementation of the graded approach is to categorize computer-based systems in the nuclear security regime into zones, where graded protective principles are applied for each zone, based on the strength of computer security measure assigned to the zone.

7.20. The CSP should document a method, such as described in section 2, for determining the appropriate computer security level for each digital asset and SDA, where required to do so by the competent authority for computer security. For example, some competent authorities and/or, operators may be required only to implement prescriptive computer security measures, without having to determine which computer-based systems are digital assets and SDAs themselves.

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

DESIGN OF COMPUTER SECURITY MEASURES

7.22. The CSP should promote to the highest degree possible, that computer security measures are incorporated into the design of computer-based systems. Computer security is in general much cheaper and much more effective when incorporated as part of the design rather than added later.

7.23. Both nuclear safety requirements and nuclear security requirements should be considered at the point of design of computer-based systems.

DEFENCE IN DEPTH FOR COMPUTER SECURITY MEASURES

7.24. The principle of defence in depth is a fundamental to nuclear security. The nature of computer-based systems and computer security means that the implementation of defence in depth for computer security, however, is different from defence in depth measures used for physical security. This is for the following reasons:

7.25. In general, once a threat has defeated a particular computer security measure, all measures of that kind are less effective and in many cases forever defeated. This contrasts with a physical barrier where breaching one barrier does not in general reduce the cost of breaching other similar barriers and in general does not reduce the cost of breaching that barrier again in the future.

7.26. Most cyber-attacks rely on deception and guile. During cyber-attacks, the presence and activities of the attackers may not be recognized. Reports consistently reveal that threats may be present inside networks for many months before they are detected. Consequently, the three physical protection functions (detect, delay, response) are difficult to create in computer security measures because if detection is unreliable, it is difficult to benefit from any delay.

7.27. The CSP should, to the degree possible, require defence in depth for computer security measures. This may be achieved in different ways, including:

— Using diverse and independent computer security measures, requiring independence in their design, operation and maintenance activities. This will for example ensure that a single computer security vulnerability does not provide the adversary with the ability to systematically bypass several layers of defence in depth.

— Through the separation of duties for personnel or teams that have privileged access to SDAs in order to achieve defence in depth. This should include consideration to separate the design, implementation, and administration from the operations of computer security measures.

CONTRACTOR, VENDOR AND SUPPLIER MANAGEMENT

7.28. Sometimes a competent authorities or operator needs a contractor, vendor, or supplier to provide services or goods that involve sensitive information and SDAs. Such arrangements should be made through legal agreements such as a licence or contract and should include appropriate computer security requirements.

7.29. Competent authorities and operators should consider when developing its contracts that contractors, vendors and suppliers will possess unique and proprietary information concerning their product or service, e.g. about vulnerabilities to cyber-attacks, which may emerge and evolve long after the original contract has been completed

7.30. Competent authorities and operators should express in its CSP specific computer security requirements for such contractors, vendors and suppliers. This may include requirements for both onsite and offsite work.

7.31. Competent authorities and operators should ensure contractors, vendors and suppliers implement computer security measures within the products and/or services that they deliver.

7.32. Competent authorities and operators may for example need to express specific responsibilities for computer security within the contracted arrangements. These contractual arrangements may include, but are not limited to:

- Non-disclosure of sensitive information and other information
- Protection requirements for sensitive information including retention and destruction requirements
- Allowable access and activities to be performed on computer-based systems
- Penalties for non-compliance with stated computer security requirements
- Remote access restrictions
- Testing requirements for services and products delivered under contract

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

7.34. Competent authorities and operators should also require that contractors, vendors 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.

7.35. Note that accountability for computer security cannot be transferred to contractors, vendors and suppliers.

8. SUSTAINING COMPUTER SECURITY

8.1. This section describes recommended elements and measures within the CSP for sustaining computer security. These strategy or subsidiary documents should document these requirements.

8.2. Every competent authority and operator should have human resource development programmes to ensure that they remain capable and competent to perform their assigned computer security responsibilities.

8.3. Every competent authority and operator should have in place processes for using best practices and lessons learned from experience [1], particularly learning from computer security incidents and wherever possible learning from other competent authorities and operators, other industries and equivalent organizations in other States.

8.4. Every competent authority and operator should include computer security in its sustainability programme supported by provision of adequate resources. The sustainability programme should cover relevant aspects of competences and levels of capability needed in the development, implementation, maintenance and decommissioning or retirement of digital assets and SDAs.

SECURITY CULTURE

8.5. Developing, fostering and maintaining a robust nuclear security culture is an essential element of a nuclear security regime. This is especially true with computer security in which people and processes are often the key factor in securing SDAs. Human error is one of the biggest contributors to computer security incidents.

8.6. Computer security should be promoted as an essential component of nuclear security culture through the explicit commitment of top management, performance of activities to raise awareness and training. The CSP should contain activities that re-enforce as an element of nuclear security culture.

8.7. As part of an effective nuclear security culture, all organizations, employees and contractors should have a full understanding of their computer security responsibilities and the importance of these responsibilities, in particular with regard to their impact on nuclear safety and security. It is essential that employees and contractors receive security education and training commensurate with their individual responsibilities and needs. This applies equally to computer security.

TRAINING

8.8. Competent authorities and operators, as part of their CSP, should establish a training programme for computer security that is informed by the strategy with the objective of developing and sustaining their designated competences and level of capability.

8.9. The training programme should contain activities to enhance awareness and to develop competences (i.e. skills).

8.10. Recommended computer security awareness training topics include, but are not limited to:

- Computer security awareness training for all employees. Awareness of the types of computer threats and associated attack techniques
- Awareness and guidance to guard against social engineering
- Recognition and response to a cyber attack
- Their responsibilities within the computer security procedures and penalties for noncompliance
- The potential impact on nuclear security from a cyber attack
- Good practices for computer security behaviours
- Mobile media use
- Social media guidelines
- Changes to the current cyber threat or risk condition

8.11. Changes in security rules and procedures should be made known to all relevant employees and contractors as soon as practicable.

8.12. Specialized skills training for those with computer security administrative and technical responsibilities (i.e. IT staff, instrumentation and control staff, security system administrators, technical equipment maintenance personnel, etc.). The training programmes should specify training requirements for specific job functions.

8.13. The training programme should specify contracted party training requirements addressing both onsite and offsite work.

8.14. Senior leadership should receive periodic training and awareness briefings on the cyber threat and risk management.

8.15. Competent authority and operator should frequently review and update to their training curriculum to reflect the dynamic nature of computer security including the current threat and cyber-attack tactics.

8.16. The competent authority or operator should assign responsibility and adequate resources to support training implementation and sustainability.

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

8.18. Information and computer security training and awareness activities are often combined within individual organizations. Annex III of Ref. [6] provides a sample security awareness programme which can be adapted to include computer security.

CONTINGENCY PLANS AND RESPONSE TO EVENTS

8.19. The CSP should detail computer security measures for detection of computer security incidents.

8.20. The CSP should specify the appropriate response and analysis activities to characterize the cause, impact and severity of the computer security incident. Note that these elements may not be readily apparent.

8.21. The analysis of the incident should account for the fact that the incident could be a precursor or reconnaissance activity for a future attack.

8.22. The CSP or site security plan should contain contingency plans to respond to malicious acts against SDAs. These plans should also account for the possibility of insider and blended attacks.

8.23. The contingency plan should identify specific computer security incidents and the required response to these incidents.

8.24. When the computer security incident is also a nuclear security incident, the contingency plans should be enacted.

8.25. In all cases, the CSP and related contingency plans should take immediate action whenever nuclear safety is jeopardized.

8.26. Analysis of computer security incident may require a cross-cutting team to analyse the impact on physical security and nuclear safety.

8.27. The CSP should include the criteria for involvement of the additional resources and their role in response to the incident.

COMPUTER SECURITY ASSURANCE ACTIVITIES

8.28. Competent authorities and operators should ensure that their quality assurance policy and programmes test that computer security requirements are satisfied.

8.29. Competent authorities and operators that are responsible for a risk-managed approach should provide assurance to the lead competent authority for computer security that the resources assigned to computer security measures are appropriate and proportionately balanced in light of the threat assessment.

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

8.31. Competent authorities and operators should ensure that quality assurance policy and programmes monitor that computer security principles also apply throughout all stages of the supply chain.

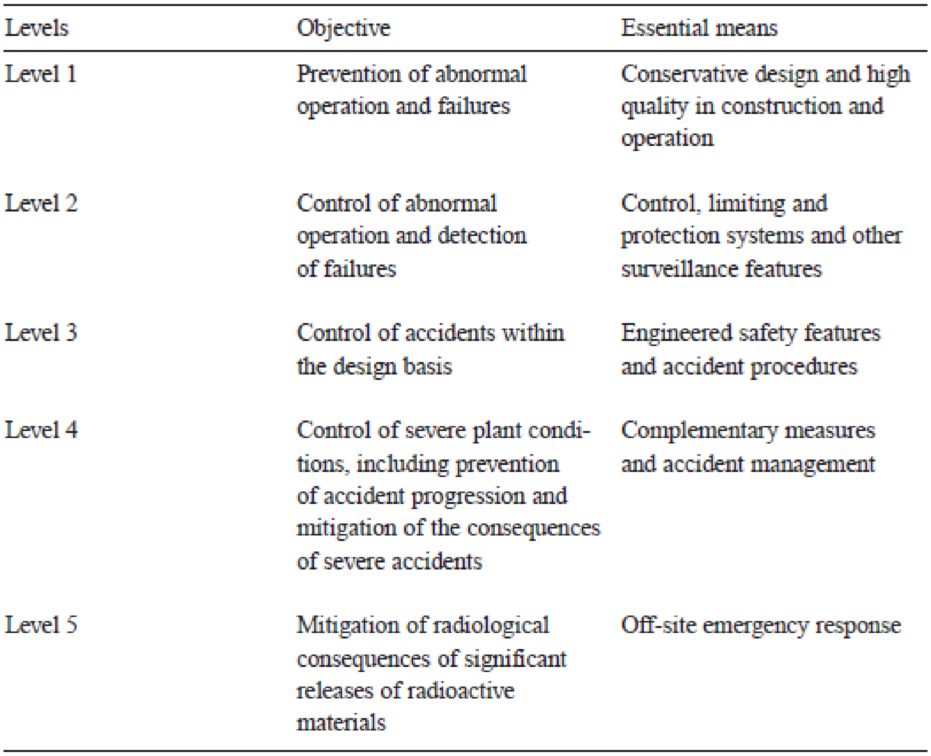
APPENDIX I: SAFETY INTERFACE CONSIDERATIONS FOR COMPUTER SECURITY AT NUCLEAR AND OTHER RADIOACTIVE MATERIAL FACILITIES

A-1. Adversaries can sabotage the safety and availability of a facility by cyber-attack of the facility's instrumentation and control (I&C) systems. Such attacks might cause failures of I&C systems or might cause I&C systems to operate in ways that would not be possible in the systems their designed operational state or envisioned failure states.

A-2. Malicious actions may also affect single items or be a common of undesirable behaviour of multiple I&C systems. In the design of the facility it should be ensured that malicious acts/a single malicious act may not bypass multiple levels of safety defence in depth or that they could cause simultaneous failure of multiple levels.

A-3. Implementation of computer security for facility I&C systems is intended to reduce the possibility that adversaries can sabotage security or availability via cyber-attack on digital I&C systems. Implementation of computer security is not goal in itself. Computer security resides at Level 1 of the Safety Defence in Depth framework, but it needs to be applied to functions, systems and equipment at all levels of the defence in depth. Within the safety paradigm, defence in depth is well defined to consist of five levels, as shown in Table A-1 [8].

TABLE A-1. SAFETY DEFENCE IN DEPTH LEVELS



Levels	Objective	Essential means
Level 1	Prevention of abnormal operation and failures	Conservative design and high quality in construction and operation
Level 2	Control of abnormal operation and detection of failures	Control, limiting and protection systems and other surveillance features
Level 3	Control of accidents within the design basis	Engineered safety features and accident procedures
Level 4	Control of severe plant conditions, including prevention of accident progression and mitigation of the consequences of severe accidents	Complementary measures and accident management
Level 5	Mitigation of radiological consequences of significant releases of radioactive materials	Off-site emergency response

A-4. The safety security interface within computer security has multiple interface elements in which security and safety responsibilities may be shared. These elements include systems, procedures, and personnel. Safety requirements also often provide security value and may should be considered when developing computer security measures.

A-5. Many features that are designed into I&C systems for safety reasons may also have security benefits. One example is thorough checking of received data for validity, authenticity, and integrity before it is used in an I&C function. Maintenance or modification of such features may degrade security or security functions if those performing such activities are not aware that multiple purposes are being accomplished. Consequently, both safety and security reasons for I&C features should be described in system and component documentation.

A-6. Safety strategy may also affect security. For example, design for security often involves allocation of functions to different processors 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. These strategies result in an increase in the number of processors in the I&C systems which in turn increases the number of targets for cyber attack. Safety should always take priority, but design should consider the security effects.

A-7. Adding security functions to an I&C system increases that system's complexity and might introduce into the system potential failure modes that would challenge its ability to reliably perform its safety function or increase the potential for spurious operation. Neither the function nor failure of security features should compromise the safety functions of I&C systems.

A-8. The appropriateness of a given control will depend on both safety and security considerations, thus assigning controls requires expertise and effort from both domains. Security controls cannot exist in isolation from safety concerns, and safety controls cannot exist in isolation from security concerns. Such an approach may, for example, necessitate that certain security functions (e.g., collection of audit records, generation of security alarms) be implemented in separate systems that can monitor the I&C system but not affect their performance or performance of active security scans only when I&C systems are off line. Exceptions to this concept may exist, but they should be analysed and justified. Computer security controls will include both technical and administrative controls. The administrative controls may involve physical security features, and personal security features. The full set of controls needs to work together..

A-9. The acceptable risk is presumptively the same whether the initiating cause is a safety or a security event. The philosophies to achieve this fundamental objective are similar:

— Safety and security typically follow the principle of defence in depth — that is, the employment of layers of protection;

— Equal consideration is given to prevention; early detection of abnormal situations, and prompt response to avoid consequent damage;

— Mitigation is the third part of an effective approach;

— extensive emergency planning should be in place in the case of the failure of prevention, detection and mitigation systems.

A-10. Despite much common ground, the relationship between computer security and safety cases requires coordination, such as in the classification and management of assets taking into account safety and security considerations.. It is made difficult with the software-intensive, networked and consequently evolving nature of many computer-based systems, which means the design and operation of computer security cannot be static.

A-11. This presents a challenge when safety depends upon adequate and effective computer security measures. Safety analysis or cases rely upon accurate predictions of future deterministic behaviour, which is complicated by the evolving nature of software-based systems, may be further complicated by ineffective computer security measures; and made more difficult by analysis that does not provide those accurate predictions of future behaviour, e.g. when targeted via cyber-attacks.

A-12. Further, application of computer security measures to an existing system is likely to require the review of the existing safety analysis. This is because, in general, computer security measures will constrain or otherwise alter the behaviour of the computer-based system itself rather than being separate from the computer-based system.

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] 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).

[3] 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, GOV/INF/2005/10–GC(49)INF/6, IAEA, Vienna (2005).

[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, Security of Nuclear Information, IAEA Nuclear Security Series No. 23-G, IAEA, Vienna (2015).

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

[8] INTERNATIONAL ATOMIC ENERGY AGENCY, Defence in Depth in Nuclear Safety, Report by the International Nuclear Safety Advisory Group, IAEA, Vienna (1996).

[9] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Information Technology — Security Techniques — Management of Information and Communications Technology Security — Part 1: Concepts and Models for Information and Communications Technology Security Management, ISO/IEC 13335-1:2004, ISO, Geneva (2004).

ANNEX I: CYBER THREAT PROFILES

I-1. Understanding the cyber threat is an important aspect for developing and implementing protective measures. The cyber threat is unlike the traditional physical threat to nuclear and other radioactive material and their associated facilities and operations. The cyber threat is not limited by proximity to the location, by numbers of attackers, nor by the boundary of the targeted facility. An understanding of the characteristics of the cyber threat as well as the possible attack scenarios provides valuable insight into both prevention and response measures. The cyber adversary and their tools, tactics, and targets are dynamic elements and diligence needs to be maintained in assessing the current threat condition.

I-2. Prevailing trends include [I-1, I-2]:

- Increasing number of adversaries with cyber capability
- Cybercrime-as-a-service is likely to increase reducing the barriers for entry for adversaries who previously lacked cyber skills
- Sophistication of the current cyber adversaries will increase, making detection and response more difficult
- Social engineering will continue as a major technique - spear phishing will continue to be popular with adversaries and watering-hole techniques will increase
- Increasing focus by adversaries on finding vulnerabilities in industrial control systems
- Securing the supply chain against malicious cyber acts will continue to be difficult

I-3. The competent authority for cyber threat assessment and competent authority and operator participating in the threat assessment process should consider at least the following attributes and characteristics for each identified internal and external threat. Characterization and knowability of the cyber threat is hard due to challenge of attribution and the often anonymity of attack. Value is added, however, in the development of ongoing threat profiles.

CYBER THREAT ATTRIBUTES AND CHARACTERISTICS

I-4. The following are cyber threat attributes and characteristics for use in developing threat profiles;

- Motivation: political, financial, ideological, personal;

— Intentions: radiological sabotage of material or of a facility, theft, causing public panic and social disruption, instigating political instability, causing mass injuries and casualties; sensitive information theft;

— ‘Cyber’ skills: skills in using computer and automated control systems in direct support of physical attacks, for intelligence gathering, for computer based attacks, for money gathering, etc.

— Knowledge: targets, site plans and procedures, security measures, safety measures and radiation protection procedures, operations, potential use of nuclear or other radioactive material;

— Funding: source, amount and availability;

— Tactics: use of stealth, deception, or force.

DESCRIPTION OF BASIC CYBER THREAT ACTORS

I-5. While many categorizations of threat may exist, the following are presented as an example. Some categorizes may additionally overlap.

I-6. **Insider threat -** One of the most challenging attackers to defend against is the insider threat. This is someone, who has been trusted and trained on internal systems, that for whatever reason uses this access and knowledge in a compromising and potentially malicious manner. The specific rational for insider activities vary greatly ranging from disgruntled employees to covert agents.

I-7. **Extremist** – Extremism (demonstrators, activists, etc.) in general terms refers to groups that go beyond the norm in expressing nominally political or social agendas, i.e. activism which has exceeded accepted behaviours. When computer-based systems are used as a tool of extremism, it is often referred to as “hacktivism”. Extremism may be a solitary act or it may be a loose coordination of similarly minded individuals using a provided cyber tools set against a designated target. Such collectives may not be tightly controlled by a central figure nor may they be operating under specific rules of engagement.

I-8. **Recreational hacker** – The recreational hacker represents an individual or group whose purpose in conducting an attack may not be the desire to inflict damage or for monetary gain, but whose motivation may be that of fame or notoriety. Compromise from the recreational hacker may be non-targeted (i.e. the nuclear facility was not the specific target), but may result from a hostile cyber environmental. An example of this would be a control system at a nuclear facility infected with a common virus due to insecure management of mobile media.

I-9. **Organized crime** – Organized crime has developed very sophisticated and targeted cyber campaigns against multiple sectors of industry. The purpose is monetary gain, which may be in the form of direct monetary theft or it may be in the form of information theft or the marketing of a compromise as a commodity for sale to other threat actors.

I-10. **Nation State** – Nation States often represent a very capable and persistent threat. The motivations and objectives are normally confined to information collections and bound by structured rules of engagement.

I-11. **Terrorist** – Past cyber-attacks attributed to terrorists have largely consisted of unsophisticated efforts such as e-mail bombing of ideological foes, denial-of service attacks, or defacing of websites, but the fear is an increasing technical competence in order to perform network-based attacks. This technical competence may arise from internal expertise or from employing hackers [I-3] The terrorists may target and attempt to sabotage critical infrastructure such as nuclear power plant, but additionally, their focus may be the acquisition of nuclear and other radioactive materials

ATTACK CHARACTERISTICS

I-12. Attack characteristics are also important to understand in build preventative, detection, mitigation, and response measures. Several types of attacks are described below. Note that this categorization is non-exclusive.

NON-TARGETED ATTACK

I-13. Many of the above threats represent directed attacks against specific nuclear security targets. The cyber environment, however, is not benign and non-directed malicious mobile codes, as an example, may be inadvertently introduced into computer based systems and networks that could adversely affect nuclear security. An example of this would be a control system at a nuclear facility infected with a common virus due to insecure management of mobile media.

PERSISTENT ATTACKS

I-14. The cyber-attack may seek immediate impact or it may be part of a sustained campaign against a facility or organizations. A persistent attack may consist of initial computer-base system compromised followed by a lengthy campaign of information collections. The result may be an impactful event or the attack may just establish a presence for future activity.

BLENDED ATTACKS

I-15. Blended attacks are coordinated acts which consist of both a cyber-attack with an associated physical act. An example could be the cyber compromise of a physical access control system to permit the entry of unauthorized individuals. Threat scenarios need to consider the possibility of threat actors operating with such intent.

THREAT PROFILE TABLES

I-16. Tables I-1 and I-2 illustrate a possible set of attacker profiles. Table I-1 focuses on insider threats (see also Ref. [4] for a discussion of the insider threat), while Table I-2 identifies possible external threats. The tables associate general types of attackers with their resources, the time span of the attack, the tools that are likely to be used and the attacker's motivations. Profiles should be adapted to the individual situations.

REFERENCES FOR ANNEX I

[I-1] AUSTRALIAN CYBER SECURITY CENTRE, 2015 Threat Report

[I-2] GEORGIA INSTITUTE OF TECHNOLOGY, Emerging Cyber Threat Report 2016 (2015)

[I-3] THEOHARY, C. A., AND ROLLINS J., 'Terrorist Use of the Internet: Information Operations in Cyberspace', Congressional Research Service, 8 March 2011. http://fpc.state.gov/documents/organization/158490.pdf.

[I-4] INTERNATIONAL ATOMIC ENERGY AGENCY, Preventive and Protective Measures against Insider Threats, Nuclear Security Series No. 8, IAEA, Vienna (2008).

TABLEI-1. INTERNAL THREATS

Threat	Resources (skills, knowledge, access, funding)	Time	Tactics	Motivation	Intentions
Covert agent	Facilitated ‘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 May be directed by an external handler	Political, financial, ideological	Theft of business information, technology secrets, personal information Sabotage
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 May be 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	

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.(may 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/other 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	
Currently contracted – third parties	Local or remote access, possibly high 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 engaged in a larger group of people. May still possess system documentation. May use unmanaged former access. Possible ties to facility personnel.	Varied and depending on the associated group of people.	Possible knowledge of existing passwords. May use unmanaged former access. May have created system backdoors while still an employee. 'Social engineering'.	Personal	Revenge, havoc, chaos. Theft of business information. Embarrass employer/other employee. Degrade public image or confidence.

28 TABLE I-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 IT 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 may center on current or recent events.	Individual or small group hacking activities Distribution of cyber 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 fo target of opportunity. Exploitation of ‘low hanging fruits’.
Organized crime	Strong resources. Employment of cyber expertise	Varied, but mostly short term	Scripts, home grown tools. May employ ‘hacker for hire’. May 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.

Threat	**Resources** **(Skills, Knowledge, Access, Funding)**	**Time**	**Tactics**	**Motivation**	**Intentions**
Nation State	Strong resources and expertise. Intelligence gathering activities. Possible training/operating experience on the system Teams of trained cyber experts.	Varied, but able to support sustained attacks.	Sophisticated tools. May employ former/current employee. ‘Social engineering’.	Political Intelligence collection. Building access points for later actions.	Technology theft.
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. May employ hacker for hire. May 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.

ANNEX II: ASSIGNMENT OF RESPONSIBILITIES

II-1. The following table illustrates typical assignment of responsibilities to competent authorities and operators. It may be advantageous to develop a table of typical computer security responsibilities that correspond to these typical nuclear security responsibilities.

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 (licensees) Establish a system of security-based categorization Develop and maintain 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 security system (in the authorization process)
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 III: ILLUSTRATION OF A FRAMEWORK OF COMPETENCES AND LEVELS OF CAPABILITY

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

III-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.

III-3. The framework should identify for each organization or individual the competence required from the specific domains of computer security. An example listing of such domains is as follows. (Alternatively, the international standard ISO-27002 [III-1] offers a list of control areas that can be adapted for use as competence domains.):

- Management (capacity, strategic)
- Incident Response (computer forensics, network defence)
- Legislative and regulatory framework (criminal law, regulations)
- Information security and management (cryptography, encryption, storage)
- Procurement (contracts, supply chain)
- Assurance activities (testing, certification, configuration management)
- Computer security architecture
- International coordination and assistance

III-4. The framework should identify the specific computer security skills and knowledge required within each competence, informed by the threat assessment of cyber-attack, knowledge of the nature of computer-based systems available to the nuclear regime, and of the vulnerabilities of those computer-based systems.

III-5. Organizations and individuals exhibit various levels of maturity in computer security competences. The framework should categorize each level of capability for their required 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:

- Fundamental (novice): Exhibiting automatic, rule-based behaviour that is strongly constrained and inflexible
- Intermediate (practitioner): acting consciously to meet long-term goals and plans within established policy

— Advanced (expert): intuitively understanding the situation, able to focus immediately on the key aspects.

III-6. Higher levels of capabilities are required 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.

III-7. The framework should ensure that organizations and individuals responsible for design of computer security measures demonstrate higher levels of the relevant competences than those that operate those measures.

III-8. Some organizations require those capabilities to be continuously available, on-site while others can rely on the assistance from other organizations

III-9. The framework should specify 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 nothing more than a supporting role in the national threat assessment. Table III-1 illustrates this.

TABLE III-1 ILLUSTRATIVE TABLE OF THE CAPABILITIES OF INDIVIDUALS AND ORGANIZATIONS ACCORDING TO THEIR ACTIVITIES

Activity type	**Fundamental stakeholders**	**Intermediate (adds to fundamental)**	**Advanced (adds to intermediate)**
Activities regarding knowledge of the threat environment.	Maintaining basic awareness of threat behaviours, e.g. phishing attacks.	Understand 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 scenario 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.

REFERENCE FOR ANNEX IV

[III-1] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, Information Security Risk Management, ISO/IEC 27005:2011.

GLOSSARY

blended attack. A coordinated attack that utilizes both cyber and physical measures in an unauthorized act.

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

computer-based systems. The computation, communication, instrumentation and control devices that make up functional elements of a facility or activity. This includes desktop computers, mainframe systems, servers and network devices, but also lower level components such as embedded systems and programmable logic controllers.)

computer security plan (CSP). A plan for the implementation of the computer security policy specifying organizational roles, responsibilities and procedures.

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

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

contingency plan. Predefined sets of actions for response to unauthorized acts indicative of attempted unauthorized removal or sabotage, including threats thereof, designed to effectively counter such acts.

cyber-attack. A malicious act that targets sensitive information or sensitive information assets with the intent of stealing, altering or destroying a specified target through unauthorized access (or actions) to a susceptible system.

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

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

sensitive digital assets (SDAs). Sensitive information assets that are computer-based systems and need computer security measures for their protection.

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.