NUCLEAR SECURITY SERIES NO. XX

NST047

DRAFT – August-2017

STEP 8: Submission to MS for comment

COMPUTER SECURITY TECHNIQUES FOR NUCLEAR FACILITIES

DRAFT TECHNICAL GUIDANCE

FOREWORD

To be inserted closer to publication

CONTENTS

1. INTRODUCTION

BACKGROUND

1.1 Nuclear security seeks to prevent, detect and respond to criminal and intentional unauthorized acts involving or directed at nuclear and other radioactive material, associated facilities and associated activities. Nuclear security of nuclear material and nuclear facilities includes physical protection measures personnel related security (e.g. trustworthiness determination and measures against insider threats) and information security.

1.2 Groups or individuals wishing to plan or commit any malicious act involving nuclear material or a nuclear facility may benefit from access to sensitive information and sensitive information assets related to the material, the facility or the security measures in place.

1.3 The Nuclear Security Fundamentals [1] and the three Nuclear Security Recommendations publications [2] [3] [4] all emphasize the importance of securing sensitive information. The Implementing Guide Security of Nuclear Information, Nuclear Security Series No. 23-G [5] addresses the security of sensitive information and the implementation of the broader aspects of information security. Ref. [5] provides detailed guidance on the identification, classification and securing of sensitive information with appropriate measures to achieve effective information security within the State's nuclear security regime.

1.4 Cyber-attacks at nuclear facilities have the potential to contribute to physical damage of equipment (i.e. sabotage), theft of sensitive nuclear information, or aid in the unauthorized removal of nuclear material. The application of computer security at nuclear facilities to protect safety and security related functions against malicious acts is therefore vital to a State's nuclear security regime

1.5 The protection of sensitive digital assets[1] (SDAs) within the nuclear security regime is recommended in Ref.) [1], para. 4.10, which states 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". The specific need for protection of computer based systems from insider threats is recognized in Ref. [6].

1.6 General guidance on computer security for nuclear security is provided in the Implementing Guide NST045, and more specific guidance on computer security of instrumentation and control

[1] Sensitive digital assets are computer based systems that are sensitive information assets.

systems in nuclear facilities is provided in the Technical Guidance publication NST036. The current publication is intended to complement this guidance by providing details of computer security techniques for other systems at nuclear facilities.

OBJECTIVE

1.7 The objective of this publication is to assist Member States in implementing computer security at nuclear facilities and in supporting activities and organizations, including contractors, vendors and suppliers.. To meet this objective, this publication provides guidance on how to address computer security considerations in an integrated manner. While the focus of this publication is on the secure management of nuclear facilities, application of this guidance may also benefit facility safety and operational performance.

1.8 This publication addresses the use of risk-informed approaches to establish and enhance policies**,** programmes and security measures in order to protect SDAs and other digital assets. A nuclear facility relies on SDAs and other digital assets for the safe and secure operation of the facility and to prevent unauthorized removal, sabotage and other criminal or intentional unauthorized acts. This publication details the integration of computer security into a facility's or organization's management systems, and includes guidance on definition of policy and requirements, and activities to develop, implement, sustain, maintain, assess, and continuously improve the computer security measures that protect the facility from cyber-attacks consistent with the design basis threat (DBT) or threat assessment [7].

1.9 This publication also provides technical guidance for nuclear facilities to protect digital assets. This guidance is based upon implementation guidance [10] and applicable Recommendations [2].

1.10 This publication is intended for competent authorities, regulatory bodies, and management, engineering, operating, maintenance, security, and support organizations of nuclear facilities (see Figure 5 of NST045 [10]).

SCOPE

1.11 The scope of this publication is the implementation and management of computer security for nuclear security purposes at nuclear facilities. This publication is applicable to all of the stages in the lifetime of a nuclear facility detailed in NST051 [8].

1.12 Computer security at nuclear facilities is intended to protect a range of systems that contribute to different aspects of nuclear security, such as physical protection and nuclear material accounting

and control (NMAC) systems. This publication does not address the design or operation of such systems, except as they relate to their protection by computer security measures.

1.13 This publication does not address in detail computer security considerations for the facility's instrumentation and control (I&C) systems, which is addressed in specific guidance provided in NST036 [9].

STRUCTURE

1.14 Following this Introduction:

- Section 2 introduces key terminology, basic concepts and relationships.
- Section 3 describes general considerations for computer security in nuclear facilities.
- Section 4 presents guidance on computer security risk management (CSRM) at the facility level.
- Section 5 presents guidance on CSRM at the system level.
- Section 6 presents guidance on considerations for facility and system CSRM relevant to different stages in the lifetime of the facility.
- Section 7 presents an overview of a computer security programme (CSP)
- Section 8 presents an implementation of defensive computer security architecture (DCSA) and application of computer security measures.
- The Appendix provides guidance on specific selected elements of a CSP.
- Annex I provides example attack scenarios against systems in nuclear facilities that may be used to evaluate computer security at nuclear facilities.
- Annex II provides an example of security levels classification for a nuclear power plant.
- Annex III provides an example of functional and system analysis for computer security.

2. BASIC CONCEPTS AND RELATIONSHIPS

2.1 This section clarifies the meaning of important terms which are used throughout this publication.

NUCLEAR SECURITY AND COMPUTER SECURITY

2.2 The Nuclear Security Fundamentals [1] state that the targets with respect to nuclear security are "nuclear material, other radioactive material, associated facilities, associated activities, or other locations or objects of potential exploitation by a nuclear security threat, including major public events, strategic locations, sensitive information[2], and sensitive information assets."

2.3 Ref. [1] states that a nuclear security system[3] is "[a]n integrated set of nuclear security measures. Nuclear security measures are defined as "measures intended to prevent a nuclear security threat from completing criminal or intentional unauthorized acts involving or directed at nuclear material, other radioactive material, associated facilities, or associated activities or to detect or respond to nuclear security events."

2.4 NST045 [10] states that "the State should develop and maintain a national computer security strategy as part of its nuclear security regime." As nuclear facilities are within the nuclear security regime, it is important that these facilities are considered within the national computer security strategy for nuclear security. Facility functions that support safety and security need protection from nuclear security threats. Where these functions make use of, depend upon, or are supported by digital technologies, these functions also demand computer security.

2.5 Computer security is concerned with computer-based systems, especially those systems that perform or support nuclear safety, nuclear security, NMAC, and sensitive information management functions. Computer security provides techniques and tools to defend against cyber-attacks. Computer security also protects against human actions or omissions that might affect security.

[2] Sensitive information includes software. Software includes the following: run time software, embedded firmware, development tools, testing tools, maintenance tool software, operating system

[3] Ref. [2] defines "physical protection systems" and "physical protection measures". These are assumed to be equivalent, in the context of nuclear facilities, to "nuclear security systems" and "nuclear security measures" as defined in Ref. [1]. This publication refers to nuclear security systems and measures.

Facility functions, security levels, systems and zones

2.6 Facility functions are activities, actions, processes, and operations that are needed to ensure the safety and security of a facility. Facility functions include but are not limited to functions that are important to nuclear safety, nuclear security or NMAC, or that make use of sensitive information. Facility functions are assigned to systems that perform one or more of these functions.

2.7 A computer security level is an abstract concept that defines the degree of security protection required for a facility function and consequently for the system that performs that function. For each computer security level, a specific set of protective and preventive measures is defined.

2.8 A computer security zone is a logical and/or physical concept that defines the boundaries of groups of systems according to their security levels and, if necessary, additional subordinate criteria, to simplify the administration, communication and application of computer security measures.

2.9 Subordinate criteria for defining security zones may include, but are not limited to, the following:

— Organizational responsibility (e.g. different security zones for systems having different responsible departments); or

— The need to maintain separation (e.g. different security zones for redundant systems at the same security level performing the same facility function).

2.10 The relationship between the concepts of facility function, security level, security zone, and system is illustrated in Fig. 1.

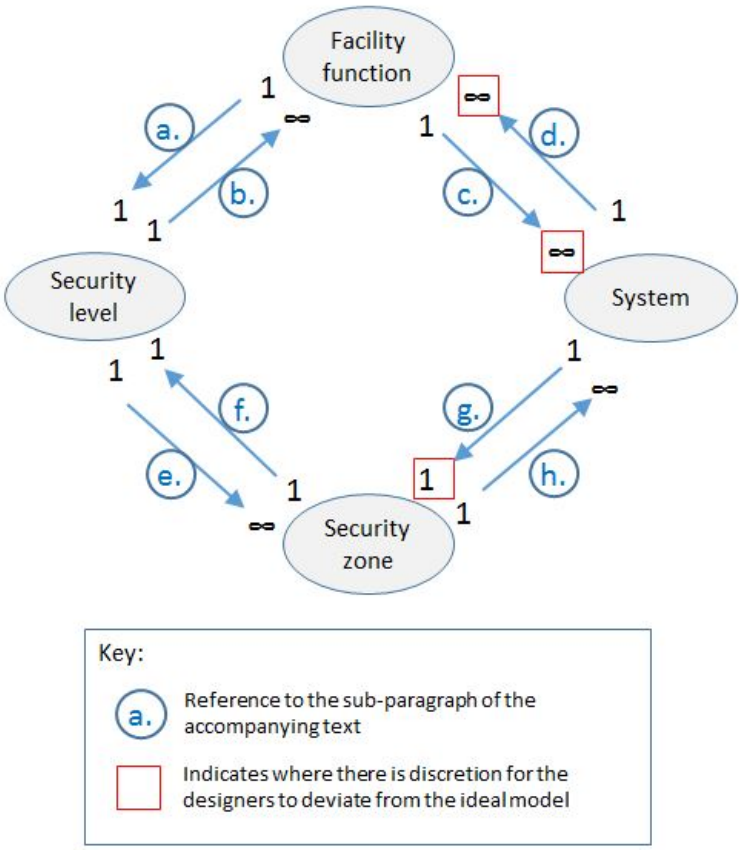

FIG. 1. Relationship between facility function, security zone and security level.

2.11 Fig. 1 above shows that:

(a) Each facility function is assigned to only one security level.

(b) A single security level is applied to one or more facility functions.

(c) Each facility function is assigned to one or more systems. (e.g. two independent, diverse, and redundant shutdown systems are assigned the same function).

(d) A single system performs one or more facility functions (e.g. HMI). Ideally from a security perspective, a single system performs a single facility function, but the designers have discretion to assign one or more facility functions to a system due to other considerations.

(e) A single security level is applied to one or more security zones.

(f) Each security zone is assigned only one security level.

(g) Each system is located within a single security zone. Ideally from a security perspective, each facility function would be defined to allow for implementation by a

single system which is located within a single security zone, but the designers have discretion to deviate from the ideal due to other considerations (e.g. fire protection, physical protection systems).

(h) A single security zone contains one or more systems.

2.12 The computer security risk management (CSRM) processes for the facility (see Section 4) address facility functions, and determine the assignment of these functions to security levels and the assignment of these function to one or more systems which then inherit the level of the function(s).

2.13 The system CSRM processes (see Section 5) address systems, and determine the boundaries of security zones based upon functions performed and system connectivity as well as the application of computer security measures demanded by the security level of the zone.

2.14 Implementation of facility functions, systems, security zones, and security levels needs to balance the competing demands for simplicity and efficiency.

2.15 A demand for simplicity in the implementation of functions in systems may lead to a preference to assign single functions to a single system. Assuming that these systems would need interconnections to enable integration of separated functions, the demands on security levels and zones become more complex due to both the increase in number of distinct zones (to encapsulate single systems) and the number of interconnections between these zones. Although this may result in a DCSA that allows for the efficient tailoring of computer security measures applied within the zone for each facility function, the increase in the number security zones and interconnections may produce a more complex architecture.

2.16 A demand for efficiency in the implementation of functions in systems may lead to a preference to assign multiple functions to a single integrated system. While this may result in a smaller number of zones, the complexity of the system may increase, making it difficult to apply effective computer security measures within these zones. Additionally, assigning a security level to the zone based upon the most important function may further reduce the efficiency of the zone model because a higher level of protection may be afforded to less important functions that have been integrated into the system or zone. These less important functions or systems would be applied more stringent computer security measures than required by their inherent security levels based upon their location within a zone assigned a higher security level.

2.17 The balance between efficiency and simplicity can also include balancing the implementation of facility functions through systems with the assignment of systems to security zones and security levels. Therefore, implementation will usually involve iterations of zone definitions (including associated computer security measures) to find the optimum balance between simplicity and efficiency. These iterations are between the facility and system CSRM.

Typical nuclear facility zone model

2.18 A standard approach to protect systems is to structure the facility architecture for all systems using the concepts of security levels and security zones. The security level assigned to the zone is based upon the highest degree of security protection required by any facility function performed by a system within that zone. The zone concept demands that the same security level is assigned to all systems within that zone. Typically, a nuclear facility zone model consists of many different zones wherein several zones may have the same security level assigned, as shown in Fig. 2.

2.19 System boundaries can be useful in informing the identification and definition of zone boundaries. One or many Facility functions may be assigned to a single system. In practice, a zone may comprise one or more systems, each system comprising one or more digital assets to support or perform the assigned facility function. .For simplicity, digital assets are not shown in Fig. 2 as each system can be assumed to comprise of one or more digital assets.

2.20 Zone boundaries have decoupling mechanisms for data flow (e.g. packet-filters, gateways, firewalls and data diodes), in order to prevent cyber-attacks, other forms of unauthorized access and also to prevent errors propagating from one zone to another and particularly propagating from a zone with lower protection requirements to a zone with higher ones.

2.21 A general facility zone model example is shown in Fig. 2, with the following characteristics:

— The number of security levels is limited to five, with level 1 having the greatest demands for protection, and level 5 having the least;

— Each system is placed within a zone;

— Each zone (including its systems) is assigned a security level. Two or more zones may be assigned the same security level;

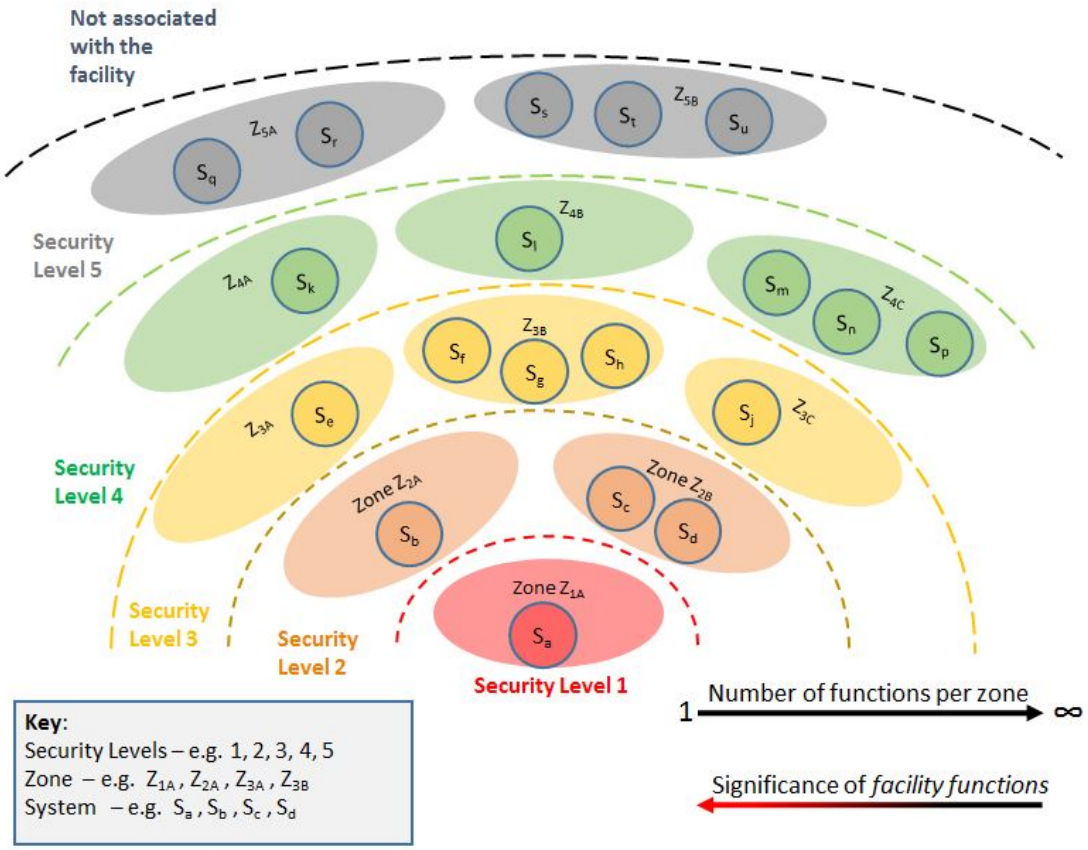

FIG. 2. Illustration of security levels and zones within a nuclear facility.

2.22 In this approach, a cyber-attack would need to traverse multiple security levels before having the opportunity to compromise a system level 1, 2 or 3, e.g. an attack originating outside the facility, the measures from the lower levels can also contribute to the protection of the higher levels. This zone model provides for implementation of a graded approach and defence in depth [1].

COMPUTER SECURITY MEASURES

2.23 In a graded approach [1], the strength of computer security measures given to a facility function is in direct proportion to the potential worst-case consequence of a compromise of the facility function.

2.24 Computer security measures are used to:

— Prevent, detect, delay, and respond to potentially malicious or other unauthorized acts;

— Mitigate the consequences of such acts.

2.25 Computer security measures may also:

— Decrease the susceptibility of digital assets to malicious acts;

— Prevent non-malicious acts from degrading nuclear security.

2.26 Computer security measures address vulnerabilities in digital assets. They can be assigned to one of three categories: technical control measures, physical control measures or administrative control measures (see NST036 [9]).

2.27 The computer security measures may also take credit for or be supported by other measures implemented for physical protection, personnel related security, and information security. Section 8 provides an example implementation of the application of computer security measures within a DCSA that has five levels.

COMPUTER-BASED SYSTEMS, DIGITAL ASSETS (INCLUDING SDAS)

2.28 Computer-based systems are those systems that make use of, depend upon or are supported by digital technologies. Computer-based systems play an ever-expanding role in the performance of important functions at nuclear facilities and associated operations. Increasingly computer-based systems are integrated into new designs and may be introduced to existing facilities during modernization, or to increase productivity.

2.29 Computer-based systems are associated with technologies that create, provide access to, process[4], compute, communicate, store, or control services involving digital information. These systems may be tangible or virtual. These systems include but are not limited to desktops, laptops, tablets, and other personal computers, smart phones, mainframes, servers, virtual computers, software applications, databases, removable media, digital I&C devices, programmable logic controllers, printers, network devices, and embedded components and devices. Computer-based systems are susceptible to cyber-attacks.

2.30 In the context of this publication, the term digital asset (DA) refers to a computer-based system that is associated with a nuclear facility. Any digital asset that has an important role in the safety or security of a nuclear facility will be considered a sensitive digital asset (SDA) [5].

2.31 Throughout this publication, the term computer security is used to cover the security of digital technologies, computer-based systems, and interconnected systems and networks.[6] Computer security is a subset of information security (as defined, for example in ISO/IEC 27000 [13]) with which it shares many of the goals, methodology and terminology.

[4] Some computer-based systems are programmable, which provides the option to modify processing steps without changing the hardware

[5] Some Member States may use designations similar to SDA, such as “critical digital assets” (CDAs) or “cyber essential assets” (CEAs). These terms may not be directly equivalent to SDAs.

[6] Terms such as “IT security” and “cyber security” are considered to be synonyms of computer security and are not used in this publication.

2.32 The relationship between information security, sensitive information, sensitive information assets, digital assets and SDAs is shown in Fig. 3 below.

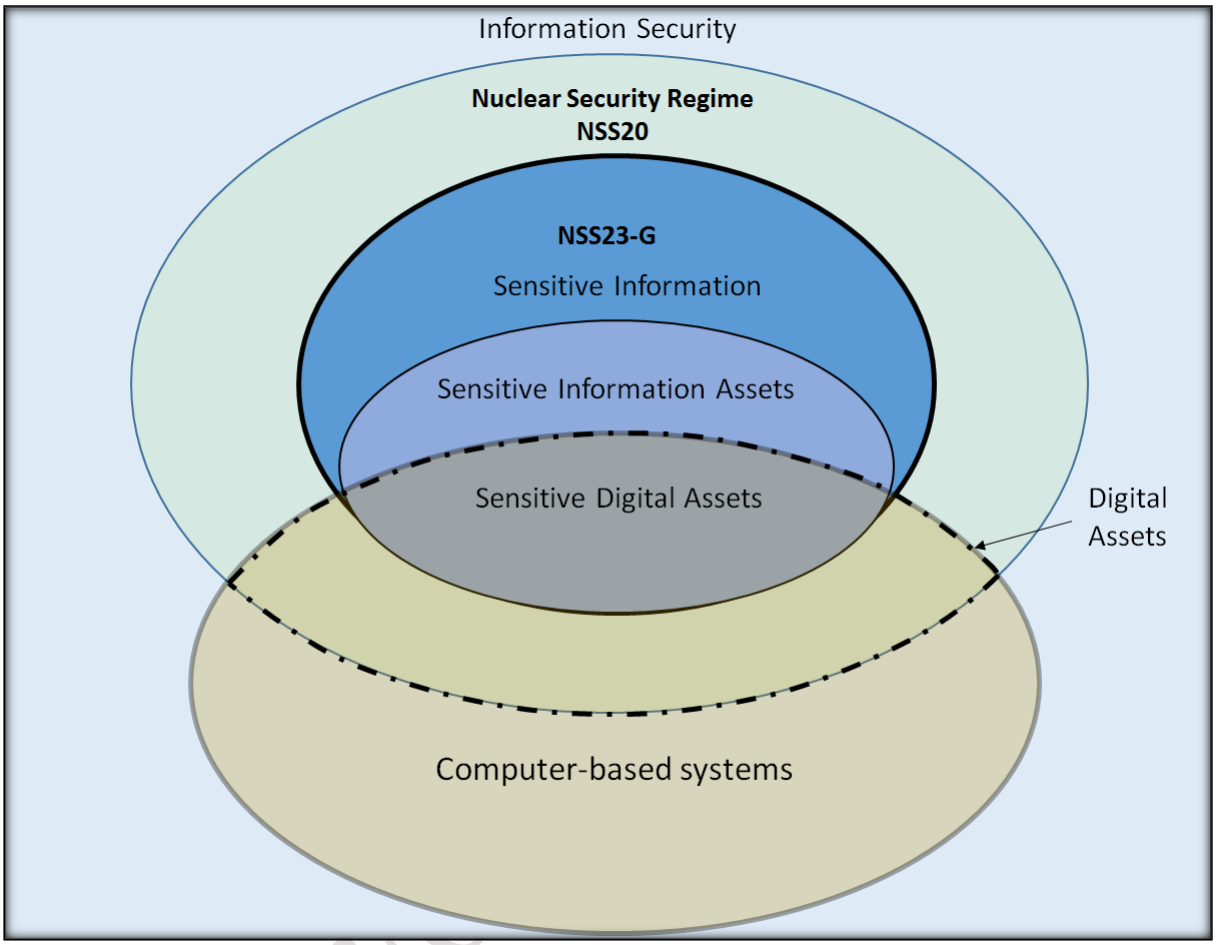

FIG. 3. Overview of information security within a nuclear facility.

CYBER-ATTACK

2.33 A cyber-attack is a malicious[7] act by individual(s) or organization(s) that targets sensitive information or sensitive information assets with the intent of stealing, altering, preventing access to or destroying a specified target through unauthorized access (or actions) to a susceptible system [9]. Cyber-attacks have special characteristics that:

— They can be hidden;

— Their execution can be delayed, condition-based, or remotely initiated;

— People (e.g. staff, contractors) can be deceived into unwittingly supporting the attack.

[7] Malicious acts do not include events caused by human error or random equipment or component failures [NST036] [9].

2.34 Cyber-attacks against digital assets may facilitate or assist in compromise of nuclear security or the subsequent compromise of SDAs. The compromise of an SDA degrades nuclear security and may result in a nuclear security event[8] that can range from (arranged from best to worst cases):

- No consequence;
- Negligible consequences;
- Limited consequences (including safety consequences such as an anticipated operational occurrence, and operational effects such as plant performance);
- Moderate consequences (such as degraded capabilities to prevent, detect and respond to nuclear security events);
- High consequences (such as unauthorized disclosure or loss of sensitive information);
- Severe consequences (such as unacceptable radiological consequences due to sabotage, unauthorized removal of nuclear or other radioactive material).

2.35 The capabilities of potential nuclear security threats may include the effective use of cyber-attacks. Therefore, SDAs are both targets for their effect on facility functions and a means for threats to facilitate and achieve their goals, and may be specifically targeted by threats.

INTERFACE WITH SAFETY

2.36 A safety function is "[a] specific purpose that must be accomplished for safety for a facility or activity to prevent or to mitigate radiological consequences of normal operation, anticipated operational occurrences and accident conditions." [11]

2.37 For example, the following fundamental safety functions that are required for all plant states (SSR-2/1 – requirement 4 [12]) are:

(a) Control of reactivity;

(b) Removal of heat from the reactor and from the fuel store;

(c) Confinement of radioactive materials, shielding against radiation and control of planned radioactive releases, as well as limitation of accidental radioactive releases.

2.38 Para. 3.46 of Ref. [2] identifies physical protection functions as detection, delay, and response. Physical protection functions use defence in depth and apply a graded approach to provide appropriate effective protection.

[8] Nuclear security events can have consequences affecting safety or security or both.

2.39 Physical protection functions and fundamental safety functions are not necessarily inherently related to each other, making it difficult to treat safety and physical protection functions equally in risk assessment methodologies. Therefore, description of facility functions important to security in a manner similar to the above facility functions important to safety will simplify the determination of significance of facility functions and will enable the equal treatment of safety and security functions having equivalent significance. Some examples of facility functions important to security may be:

- Intrusion detection (including assessment) at critical detection point
- Control of access of persons and equipment to Category I material or vital areas
- Communications to coordinate response forces during a nuclear security event.

3. GENERAL CONSIDERATIONS FOR COMPUTER SECURITY

IDENTIFICATION OF FACILITY FUNCTIONS

3.1 NST045 [10] states that the identification "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." Computer-based systems that meet the criteria of Ref. [2] para. 4.10 are SDAs.

3.2 The competent authority[9] should require the operator to identify and list facility functions[10] for the entire facility in a consistent manner to ensure that the identified set of facility functions can be assessed holistically. The application of computer security at nuclear facilities is determined by the facility functions that need protection. The computer security requirements[11] for these facility functions should be considered independently from their implementation (e.g. specific technology, whether analogue or digital).

3.3 The performance of facility functions will rely upon or be supported by related sensitive information, sensitive information assets, and associated digital assets.

PROTECTING SENSITIVE INFORMATION AND DIGITAL ASSETS

3.4 The competent authority should require the operator to apply computer security measures to ensure the appropriate protection (including traceability) of sensitive information, sensitive information assets, and SDAs. Computer security is provided by a programme or set of rules in place to ensure the confidentiality, integrity and availability of digital assets.

3.5 The operator should identify sensitive information taking into account the effects of compromise and the State's policy for the security of sensitive information. Ref. [5] provides detailed guidance on State development of policy for sensitive information.

[9] In this publication, "the competent authority" means whichever the authority to which the State has assigned the responsibility for computer security in the context of nuclear security. This may be the competent authority for nuclear security or the competent authority for computer security (see NST045 [10]).

[10] Facility functions include safety, security, operational and administrative (or organizational) functions.

[11] In this publication, "computer security requirements" include specific written requirements imposed by the relevant competent authority, or by the operator to comply with the regulatory requirements.

3.6 Sensitive information can be determined by considering both its functional significance (e.g. accurate and timely data on boiler pressure), and its intrinsic significance (e.g. security arrangements information).

3.7 For example, the information detailed within the site security plan may be classified as sensitive information and measures implemented to protect its confidentiality for an extended period of time. This is the result of the information retaining its sensitivity during the time period for which the site security plan is valid. In this example, the information detailed within the site security plan has intrinsic significance.

3.8 Alternatively, an I&C system may confer priority to those measures that ensure availability and integrity over those that ensure confidentiality of its process data. In this case, the process data has significant functional and intrinsic significance during a very limited time interval when the I&C system is performing a control action based upon this data. However, once the process data is historical (i.e. not the basis of a control action), the historical process data has only its intrinsic significance. Therefore, the security benefit arising from the increased assurance of confidentiality (to protect its intrinsic significance) is exceeded by the decreased assurance of availability (negatively affecting its functional importance).

3.9 While protecting the confidentiality of process data from these systems may not need stringent measures, the loss of confidentiality of administration passwords, source code, and other key specifics would provide the adversary with a significant benefit in the planning and execution of cyber-attacks targeting the system and consequently may lead to a need for stronger measures. Additionally, classification of the historical process data (e.g. logs) to limit their distribution (e.g. application of administrative control) may be sufficient to reduce the risk of unauthorized disclosure to an acceptable level.

RISK INFORMED APPROACHES

3.10 Computer security should be implemented using a risk-informed approach [10]. Figure 4 from NST045 [10] provides an overview of a risk-informed approach to computer security measures.

3.11 Risk, in the computer security context, is the risk associated with a nuclear security threat exploiting vulnerabilities of a digital asset or group of digital assets. It is expressed in terms of a combination of the likelihood of an event and its consequence if it occurs.

RISK ASSESSMENT AND MANAGEMENT

3.12 The operator should implement a computer security risk management process (or the process may be performed by the competent authority). The competent authority may require a specific risk

assessment methodology or policy be used, or may consent to the use of a facility's assessment methodology [10]. The facility process may follow the example of the organization computer security risk assessment as described in paras 7.10–7.16 of NST045 [10].

3.13 The operator should establish a continuous and cyclical risk management process[12] for the assessment of and handling of risks associated with cyber-attack to the facility.

3.14 Periodic and iterative risk assessments are used to support decision making within a risk management process. Computer security risk assessments are typically qualitative and involve relative measurements. The result of a risk assessment will assist in determining appropriate computer security requirements.

3.15 The competent authority should require that the operator perform computer security risk management for the facility in two complementary ways (NST045 para. 7.12 [10]):

(a) Assess and manage aggregated computer security risks to facility functions for the whole facility. This will ensure the operator performs a complete assessment of the facility and will provide the competent authority with the primary means to assess the overall effectiveness of computer security risk management at the facility. Section 4 provides guidance on performing facility CSRM.

(b) Assess and manage risks associated with each system that implements or supports those facility functions. This will ensure the operator performs a detailed assessment of each system that implements or supports a facility function**.** The competent authority may require the detailed assessments as a means to review the effectiveness of specific instances of computer security risk management at the facility. Section 5 provides guidance on performing system CSRM.

3.16 The competent authority should ensure the operator maintains independence between the teams responsible for performing computer security risk management to set the requirements, those implementing the requirements and those validating that the requirements have been met.

3.17 Risk management is relevant at all phases of the facility and system lifecycles to inform the development, implementation and maintenance of computer security measures. Section 6 identifies risk management activities, throughout the lifetime of a facility.

[12] An example of a continuous and cyclical process is the 'plan, do, check, act' cycle.

3.18 A review of the risk assessment should be performed**,** and the risk assessment updated, whenever one or more of the following conditions occur:

(a) New information or important findings invalidate assumptions stated in the current computer security policy, CSP, DCSA or choice of computer security measures; for example, when a vulnerability is discovered that invalidates the assumptions stated within a system risk assessment.

(b) The DBT or threat statement is modified. This may include enhanced threat capabilities (e.g. tactics, equipment, weapons, skills and knowledge) and resources that may increase the likelihood of successful cyber-attacks targeting facility functions, sensitive information and/or SDAs.

(c) There is a change to a facility function, system, SDA or computer security measure. This should cover any activities that involve the introduction of new equipment, software, procedures, or a major change in operator skill sets. The level of effort to update the risk assessment may be informed by the assigned level of protection of the SDA (e.g. computer security level).

(d) Regulatory requirements have changed.

3.19 Records produced from the risk management process, activities, and corresponding risk treatment decisions should be available for review by the competent authorities upon request to allow for the performance of regulatory oversight activities to assess whether the regulatory requirements are met. Furthermore, activities such as licensing, inspection and enforcement should include considerations for computer security.

3.20 The overall structure and approach for risk management process should include the following steps:

(a) Facility CSRM

— Scope definition

— Facility characterization

— Threat characterization

— Specification

— Verification and validation activities

— Competent authority acceptance

(b) System CSRM

— Definition of system boundaries

— Identification of digital assets

— System computer security architecture

— Verification of system computer security risk assessment

3.21 Many methods (see ISO/IEC 27005 [14]) exist for conducting a risk assessment. Organizations need to choose a method and customize it to their specific organizational environment and objectives, while observing the need for separate facility and system level risk management. An example is shown in Fig. 4.

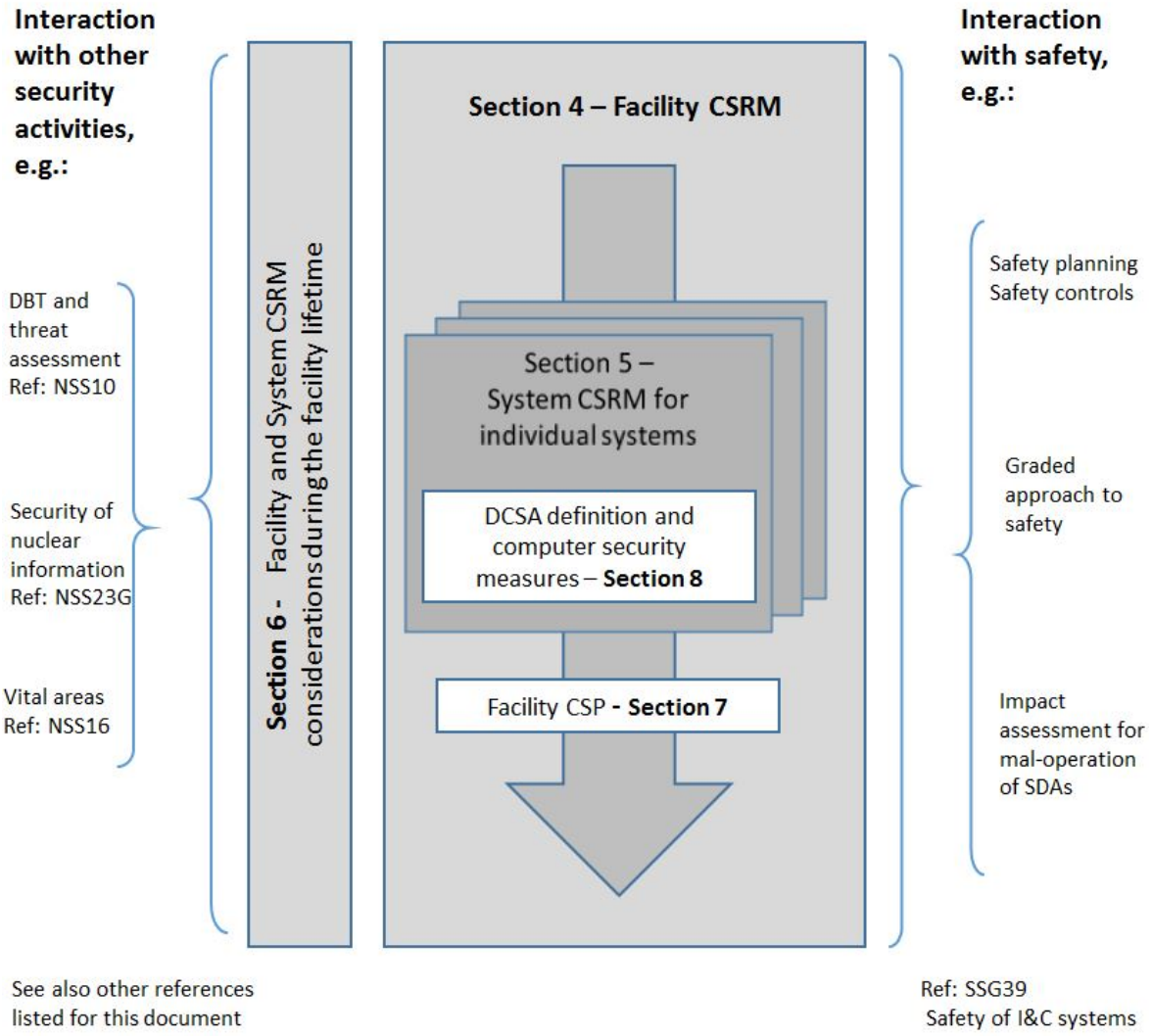

FIG. 4. Overall structure for this publication.

SECURITY LEVELS BASED ON A GRADED APPROACH

3.22 Computer security requirements and their implementation should be based on a graded approach, where computer security measures are applied in direct proportion to the potential consequences arising from compromise of the facility function. One practical implementation of the graded approach is to assign security levels to facility functions, where each security level is characterized by graded preventive and protective requirements, based on which distinct security measures can be selected to achieve the security objectives of the respective level, as shown in Fig. 5.

3.23 While the requirements (such as communication constraints between SDAs that are assigned to different levels) are fixed by the security level model and not open to interpretation, security measures (such as a distinct firewall type) can be chosen to protect SDAs according to the architectural environment of the security level and the technology of the specific SDA.

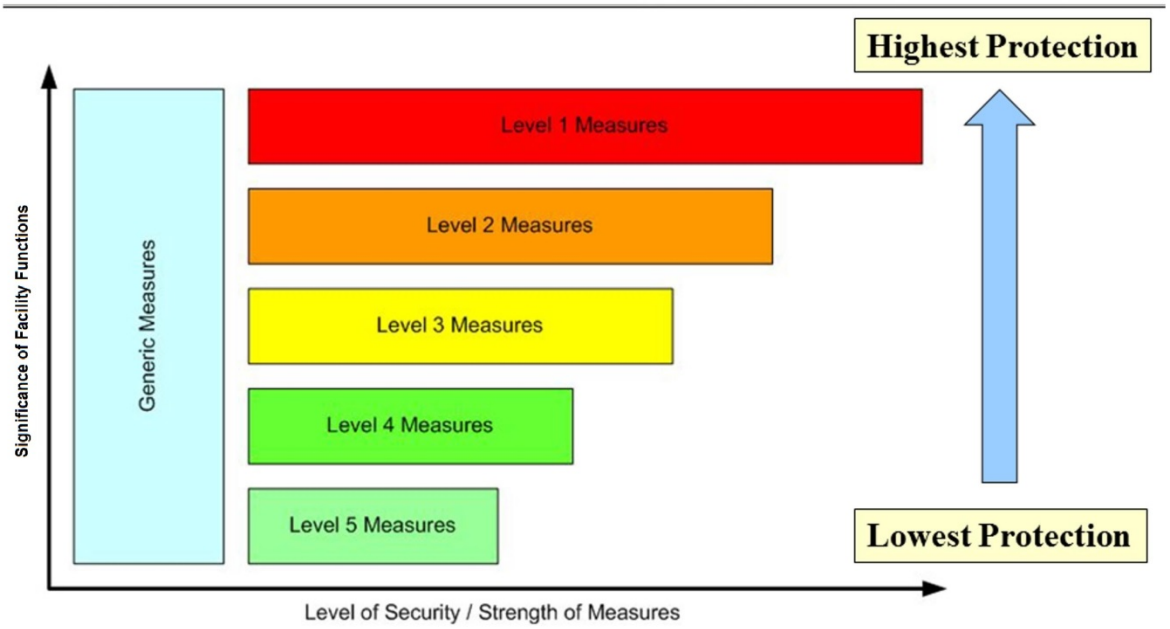

FIG. 5. Level of security/strength of measures.

3.24 The security level model should allow for easier assignment of computer security measures to protect the facility, based on the categorization of the facility function (assigning it to a security level) and the definition of the set of preventive and protective measures appropriate to that security level.

3.25 In this model:

— Generic level measures should be applied broadly throughout the organization and may be applied to all digital assets. Generic measures provide for improved cyber security culture through a greater awareness of computer security. They also improve the

computer security posture and may increase defence in depth. Generic measures cannot be accredited for providing benefit to a specific security level or system because generic measures typically apply to the broadest population of computer-based systems and their users and those measures cannot be relied upon to be operated consistently and effectively.

— Security levels range from level 5 (least protection needed) to level 1 (most protection needed), as illustrated in Fig. 5. In this example, digital assets in security levels 1-3 would have SDAs while digital assets would belong to systems shown in levels 4-5 are digital assets that are not sensitive.

— Graded computer security requirements such as restrictions on the communication between system of different security levels are applied.

— The computer security measures required by each security level should not be considered to be cumulative, thus computer security measures present in one security level may be repeated in other security levels. This is because a security level (e.g. level 1) should not trust a security level with less protection (e.g. level 2, 3, 4, 5) and therefore cannot rely upon computer security activities in those lower levels.

— However, with the correct application of a layered approach and defence in depth, illustrated in Fig. 5, computer security measures on lower-level layers can help protect the higher-level layers.

— Computer-based devices that are outside of the control of the CSP are unassigned and should not be trusted by any digital asset at any security level.

3.26 Section 8 provides guidance on computer security measures for a graded approach using the example of the model with five security levels, plus generic computer security measures.

4. FACILITY COMPUTER SECURITY RISK MANAGEMENT

4.1 Facility FCSRM is a complex process that should be performed by a multi-disciplinary team having skills and competencies in nuclear safety, nuclear security, operations, maintenance, computer security, and engineering13. This team may have a similar composition to that proposed for physical protection evaluations (see NST023 [15])

4.2 Facility CSRM is an iterative process that is conducted in phases. It may be necessary to revisit assumptions, determinations, or results of a previous phase based upon the results of a following phase. Verification activities are expected to be performed between each phase.

OBJECTIVE OF FACILITY CSRM

4.3 The objective of facility CSRM is to assess and manage risks arising from cyber-attacks that have the potential to degrade safety or security of the facility.

4.4 Facility CSRM should be informed by an assessment of identified nuclear security threats to the facility (e.g. DBT), which includes the attractiveness[14] of the target to these threats and their goals (e.g. sabotage, unauthorized removal of categorized nuclear material, radioactive material, or unauthorized access to sensitive Information). The State's assessment of threats may be provided by the DBT or national threat statement.

4.5 Facility CSRM should be based upon the regulatory requirements regarding computer security.

4.6 Facility CSRM should determine the significance of the facility function based upon their importance to either safety or security objectives. These determinations may allow for the development of a hierarchical[15] list to be prepared of potential safety or security consequences (from most severe to no consequence) for the facility resulting from compromise of a facility safety or security function[16]. Figure 7 of NST045 [10] may also inform the development of this hierarchical list.

[13] Some Member States may use designations as cyber security team to identify the required personnel for computer security

[14] Attractiveness of the target may be informed by the DBT or threat assessment and may be augmented by information provided by the State via its competent authorities. The operator is expected to not have the capabilities or authority to make this determination. The competent authority should make this determination.

[15] An ordered list that places facility functions into groups of approximately similar consequence.

[16] These are functions that have significance to the facility's safety or security objectives. The operator may also include other functions identified as having significance to the facility (other than safety or security).

4.7 Facility CSRM should not consider the technical implementation of the systems and digital assets that perform or support the listed facility functions. The facility CSRM considers facility functions. The system CSRM considers systems and digital assets, including their technical implementation. For example, system CSRM would identify that analogue systems may rely upon digital equipment for maintenance and calibration that if compromised could degrade the ability of the system to perform the assigned facility function.

4.8 The results of the assessment of facility risk should inform the application of a graded approach that includes the assignment of computer security levels to facility functions, based upon risk. The assignment should ensure that facility functions associated with the highest level of risk are afforded the highest level of protection.

4.9 The results of the assessments should inform the implementation of defence in depth, which increases the effectiveness of computer security measures to ensure that the required protection is provided. The principle of defence in depth should be applied both within each of the individual security levels by using diverse, independent, and overlapping administrative, physical and technical control measures and between security levels.

4.10 The use of a consistent facility CSRM approach across all facilities within a State may assist the competent authorities in providing effective oversight with respect to the application of computer security at nuclear facilities by minimizing differences in intent and structure of regulatory compliance records. The use of consistent input processes and documents, the establishment of a computer security policy and programme, and preparation of consistent output documents by each facility would assist in this goal.

4.11 The operator should use the following inputs for use within facility CSRM:

(a) Design basis threat (DBT) and associated analysis, if available. The DBT is used to:

— Identify critical dependencies based on facility functional scenario development; and

— Support evaluation for verification of the assumptions documented within facility CSRM; and thus

— Provide an instrument by which the CSP and its implementation are validated.

(b) Applicable regulatory requirements or other documents. This may include the State's information classification policy.

(c) Facility safety analysis (or report) including design basis events: The facility safety analysis may be used to define security requirements, but the safety analysis is not sufficient as it does not account for all mal-operations, notably those caused by malicious actions.

(d) Site security plan (or report) (NST023 [15]): The identification process may use the site security plan to identify the facility security functions and their significance in meeting the safety and security objectives of the facility. The site security plan may incorporate aspects or the entirety of the facility's CSP.

(e) Facility computer security policy, if exists.

(f) Previous facility CSP documents, if they exist, including assignment of systems to functions.

OUTLINE OF FACILITY CSRM

4.12 The following are the phases of a facility CSRM:

(a) Scope definition: Defining the scope of the assessment – e.g., based on function (Safety, Security, Operations, and Emergency Preparedness), physical and logical footprints, stage of the lifetime of the facility, and comprehensiveness. During the scope definition phase, the inputs and prerequisites should be identified and produced.

(b) Facility characterization: Identifying facility functions, and corresponding interactions and dependencies between them, to support the specification phase. Identifying sensitive information that could aid a threat in conducting an attack against the facility. Identifying targets from those facility functions and from sensitive information.

(c) Threat characterization: Analysing the national threat statement (or DBT) to identify potential threats using specific tactics, techniques and procedures along with adversaries' cyber skills to direct cyber-attacks, including blended attacks, on targets at the nuclear facility. This characterization phase provides a threat characterization that bounds the credible attack scenarios.

(d) Specification: facility level computer security requirements on the architecture. The specification phase:

— Develops and documents a CSP;

— May recommend amendments to the computer security policy;

— Assigns facility functions to security levels; and

— Creates or amends requirements on the DCSA.

(e) Verification and validation activities: The overall aim of the verification and validation activities is to determine whether the quality and expected performance of a CSP meets its requirements. Verification confirms that the results of a phase meet the objectives and requirements defined for the phase. Verification activities occur between each successive phase of facility (and system) CSRM. This may involve a number of performance-based

methods or analysis to evaluate the outputs of each phase prior to their use as input into a subsequent phase. Validation is the process of determining that the computer security of the facility provides appropriate protection against the threat characterization and complies with regulatory requirements. Verification and validation activities generally utilize one or more evaluation methods (see para. 4.91 and Fig. 7).

(f) Acceptance by the competent authority: the issue of the (revised) CSP and facility CSRM compliance report, review and acceptance by the competent authority.

These phases are described in Fig. 6 which provides an overview of the facility CSRM process. There is one facility CSRM process per facility, within which there is a separate system CSRM process per system.

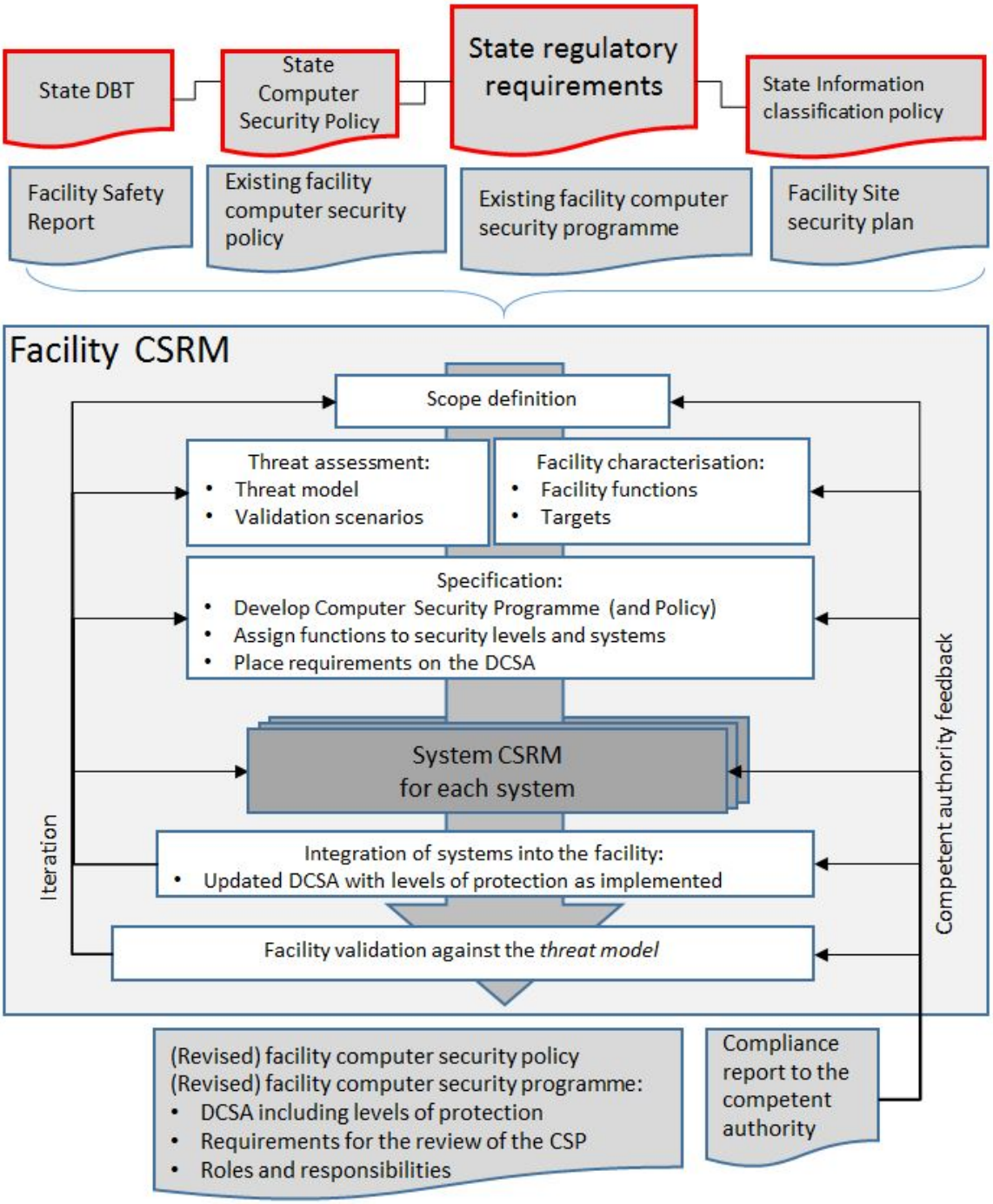

FIG. 6. Overview of facility computer security risk management process.

SCOPE DEFINITION

4.13 The operator should identify the scope boundary of the facility's risk management process. Considerations for scope may include the facility's physical perimeter, approved contractors, vendors and suppliers, head office or corporate offices, offsite data centres, and other strategic locations. The scope of this assessment may vary depending on the stage of the lifetime of the facility as well as the capability and maturity of the organization (see 5.25-5.28 of NST045 [10]).

FACILITY CHARACTERIZATION

Identification of facility functions

4.14 The operator should identify all facility functions without consideration of implementation and design aspects of systems providing those functions. The pervasive presence and use of computer-based systems associated with a nuclear facility, throughout the facility's lifetime, makes it likely that computer-based systems will be used to perform or support the majority of key tasks and activities related to facility functions. .

4.15 The stage in the lifetime of the facility (NST051 [8]) should inform the characterizing the facility and identifying the facility functions. The lifetime stage will demand different facility functions and may also change the significance of these functions.

4.16 Facility functions are characterized based on the following elements:

(a) Intrinsic significance: the importance of the facility function to nuclear security and safety and its associated consequences[17]. Significance is the primary characteristic.

(b) Potential effects of compromise: the manner in which the facility function fails.

(c) Dependencies between functions: the significance of facility function arising from other functions that rely up it.

(d) Necessary timeliness and accuracy for facility function dependencies.

Intrinsic significance of facility functions

4.17 The significance of all facility functions should be compared in order to group together those that have similar significance, if possible using a common scale that combines security and safety.

4.18 For facility security functions, a nuclear security classification scheme based on nuclear security consequences, such as outlined in Figure 7 of NST-045 [10], should be used to determine the significance of the function.

[17] The signficance of the function to nuclear security can often be associated to its consequences. For nuclear security, the consequences that are considered most significant are those that result in unauthorized removal of categorized nuclear material and/or sabotage resulting in unacceptable radiological consequences. Additionally, in some instances (CPPNM Amendment, NSS 20 [1]) unauthorized disclosure of sensitive information is to be considered. Other possible consequences may be associated with other organizational objectives, for example, maintaining reputation, compliance with other environmental regulations. A listing of possible consequences can be found in ISO 27005:2011 [14].

4.19 For facility safety functions, an established safety classification may be used to determine the significance of the function. However, security risks may necessitate the assignment of a higher significance value than demanded by a function's safety classification.

4.20 The determination of significance of facility functions should consider that the implementation of facility safety functions (by systems) may support security; and implementation of facility security functions may support safety. As a result, the assignment of a facility safety function to a significance value for computer security may not follow a direct one-to-one relationship with its safety class.

4.21 For example, a facility safety function accredited with detection of radiation for the protection of personnel may also be accredited with providing a vital facility security function, such as the detection of unauthorized removal of categorized nuclear material. While the radiation protection functions from a safety perspective may have limited consequences, the facility security function is associated with more severe consequences and more critical. Therefore the facility safety and security functions in this example would be assigned a significance value based upon their importance to the security objectives. This would result in these functions being assigned a higher significance of the function than if assessed on safety objectives alone.

Potential effects of compromise on facility function

4.22 In addition to considering the intrinsic significance of the facility function, the operator should consider the effects of compromise on facility function. These are, arranged from worst to best cases:

- The facility function is indeterminate. There are no constraints on the threat to alter the function in any manner and the initial compromise has not been detected.
- The function has unexpected behaviours or actions, which are observable to the operator;
- The function fails; or
- The function performs as expected, meaning the compromise does not adversely affect the facility function (i.e. fault tolerant).

4.23 A facility function may mal-operate in different ways and the effects of this mal-operation depends upon:

- The circumstances and environment,
- The nature of the cyber-attack that is responsible, or
- The status of the facility function.

For example, some less important functions may be used to attack more important functions through interdependencies and interactions.

4.24 For each function and each type of effect of compromise (i.e. mal-operation), there will be different consequences. These consequences should consider the loss of confidentiality or integrity or availability of sensitive information. These consequences should be appropriately identified, and the significance assigned based on those consequences that are most severe.

4.25 The significance of the function should take into account whether the function definition can be deterministically bound or limit all conditions or modes upon which the function may depend. In instances where the function definition cannot bound or limit all conditions, the listing of consequences may be incomplete which would require additional analysis or assignment to higher significance values (using a conservative approach).

Dependencies between facility functions

4.26 The determination of significance of a facility function should also consider the potential consequences its compromise (or mal-operation) on other facility functions, with which it has dependencies. Examples of functional dependencies include:

(a) Information dependency: a facility function provides information to another facility function. Examples of mal-operation include:

- The interruption of the automated control instructions for a facility process.
- The failure of alarms provided to security officers.
- Incorrect plant information displayed to an operator, to support monitoring.
- No dispatch information for emergency responders or nuclear security officers.

The significance of the facility function providing the information is determined from the potential consequences to the nuclear facility of mal-operations that could result, illustrated in these examples.

(b) Engineering or physical resource dependency: a facility function provides a required resource to another facility function. This includes resources required to sustain the facility function directly and the resources required to sustain those resources. Examples of mal-operations include:

- Interruption to the provision of water or power.
- Loss of provision of environmental conditions.
- Failure to schedule performance of preventive maintenance tasks.

The significance of the facility function providing the resource is determined from the potential consequences to the nuclear facility of failures that could result, illustrated in these examples.

(c) Policy or procedural dependency: a change of state in one facility function requires a change to another facility function. For example, if policy requires that a primary and secondary heatsink functions are provided when a reactor is critical then if one of these heat sinks becomes unavailable, the reactor must be put in a sub-critical state.

The significance of the facility function that triggers the change of state is determined from the potential consequences to the nuclear facility of mal-operations that could result.

(d) Proximity effects: this considers the effects on a facility function of the location of the mal-operation or physical failure of other digital assets in proximity to the digital assets that support the facility function.

4.27 The analysis of the interconnectedness and dependencies of facility functions may reveal that an important function has been omitted from the scope of the assessment. In this case, it may be necessary to revise the scope to allow for its inclusion, or consider changes in configuration or processes that remove the dependency.

Necessary timeliness and accuracy for facility function dependencies

4.28 The determination of significance may also take into account the timeliness required for one facility function to respond to another facility function and the necessary accuracy of the response. This can be considered in terms of requirements for the availability and integrity of sensitive information:

— Availability of information implies that, for example, a facility function is required to alert promptly to allow for assessment and response.

— Integrity of information implies that, for example, a facility function is required to provide accurate environmental variables (temperature, pressure, frequency, level), with a specific number of sensor points/samples.

The significance of the facility function is determined from the potential consequences to the nuclear facility that could result when the facility function does not provide the required timely and accurate data.

Target identification

4.29 A target is defined in Ref. [1] as “Nuclear material, other radioactive material, associated facilities, associated activities, or other locations or objects of potential exploitation by a nuclear

security threat, including major public events, strategic locations, sensitive information, and sensitive information assets."

4.30 Some facility functions will be targets and should be identified from the list of facility functions identified during facility CSRM using the definitions of vital areas [16] and sensitive information [5]. Being a target does not alter the significance of the facility function – it is an additional parameter for consideration when determining computer security requirements.

4.31 Targets that are associated with important facility safety and security functions should be identified as SDAs based upon the process (or performance) value (see paras 3.6–3.9). The SDAs should also be analysed for the potential value of any associated sensitive information. This will ensure that the SDAs and their associated information are considered within the facility's information and computer security programmes and afforded the appropriate level of protection.

Documenting facility functions

4.32 The operator should document all facility functions assessed during facility CSRM.

4.33 For facility functions having the greatest significance, identification of all the functions within the facility depends upon having complete and accurate records detailing the interactions and dependencies between functions. These records will allow for the assessment of those functions that may cause a negative impact upon other functions.

4.34 The interactions and dependencies of a facility function may be internal, external, permanent, or temporary. For example, the development process would demand interaction between the development and operational environments through the physical transport of new software, data, or devices.

4.35 The operator should consider, when analysing the consequences of an attack on one facility function, the possibility that it will be involved in an attack affecting multiple facility functions or in a blended attack (e.g. combined cyber and physical attack).

4.36 The preceding analysis may require an iterative assessment of each facility function, whereby an assessment is performed to determine the function's intrinsic significance, followed by an assessment of this significance based upon interactions and dependencies with other facility functions. The highest significance value should be used.

4.37 For the most severe potential consequences, those facility functions having a fundamental[18] relationship to the consequence should be assigned the greatest significance. This assignment should not consider any other parameters or factors.

4.38 The segregation of facility functions that limits the interactions and dependencies between them may also improve the effectiveness and efficiency of implemented computer security measures.

THREAT CHARACTERIZATION

4.39 The facility CSRM process should include an analysis of the national threat statement or DBT to further characterize and detail the nuclear security threat to the facility. The aim of this analysis is to further detail threat capabilities and potential attack tactics, techniques and procedures to determine potential threat objectives and provide a threat characterization as the basis for design assumptions required to formulate and / or validate the effectiveness of the facility's computer security policy and the CSP.

4.40 Ref. [2] para. 3.34 states that "the appropriate State authorities using various credible information sources, should define the threat and associated capabilities in the form of a threat assessment and, if appropriate, a design basis threat (DBT). A design basis threat is developed from an evaluation by the State of the threat of unauthorized removal and of sabotage." Additional information on DBT may be found in Ref. [7].

4.41 The competent authority should identify specific information regarding computer security incidents that may inform DBT development. The competent authority should require the operator to develop measures or processes that capture, retain, and manage specific information this data (e.g. phishing emails, malware samples) to allow for follow-up analysis during the DBT development. The CA/intelligence community is encouraged to provide the analysis capability to the facility in a timely and cooperative manner as well as support the exchange of this analysis and other important information.

4.42 During the development of the DBT or national threat statement, it is recommended that the competent authority and other relevant State authorities cooperatively interact to enable effective analysis of identified specific information regarding computer security incidents that have the potential to be nuclear security events.

4.43 NST045 [10] contains a detailed, but non–exhaustive, description of potential sources of attack and associated attack mechanisms relevant to nuclear facilities, and methodologies used to evaluate and identify threats.

[18] For example fundamental safety relationships.

Threat characterization

4.44 The operator should implement a systematic process to characterize the threat, to produce a threat characterization, to allow for the evaluation of risk to the facility. This process should use the DBT or State's threat assessment as the basis for evaluating credible threat capabilities to access and exploit attack vectors.

4.45 The operator should perform the threat characterization through analysis of the DBT or threat assessment whenever:

- The operator performs a facility computer security risk assessment. This may be a less intensive analysis to confirm previous analysis and assumptions;
- The competent authority issues a new DBT or threat assessment; or
- The operator is in receipt of information that potentially invalidates the assumptions of the current DBT analysis.

4.46 The adversary attributes/threat characterization should be informed by the DBT and define the knowledge, funding, and timeframe of the adversary(s), as well as their skills and capabilities. Additional adversary attributes should be described as vulnerabilities are identified. Defining additional adversary attributes and capabilities, and subsequent defensive strategies is good practice

4.47 The threat characterization should identify potential multiple attack vectors (remote, local, physical), insiders, or blended attacks, based upon the DBT, national threat assessment, open source information regarding adversary tactics, techniques and procedures, and other threat information sources. The evaluation of the DBT should include the potential for sequential cyber-attacks that multiply the consequence including where there are no indications of collusion between different threat actors (non-collaborative attacks).

4.48 The threat characterization should allow for an assessment and listing of credible attack vectors. This listing will form the basis of the computer security requirements and specification of the DCSA.

4.49 The threat characterization should inform the operator as to whether the threat has the capabilities to access an attack vector and whether they can compromise a facility function in such a way that it is indeterminate (i.e. outside its design basis). For functions associated with severe consequences, the objective should always be to eliminate access to the potential attack vector by threats detailed in the model by placing requirements on the DCSA. In cases, where elimination is not possible, requirements should be placed for a very stringent combination of defence in depth layers and computer security measures.

Additional considerations for insider threats

4.50 The threat characterization should consider insider threats. Guidance is provided in Ref. [6]. Insider threats may be categorized as passive or active. Passive insiders could be willing to provide sensitive information to the adversary, or be unaware that their credentials that provide authorized access to sensitive information had been compromised. Active insiders could be willing to initiate compromise, or use force against a target or person.

4.51 Path timelines for insider threats differ due to their authorized access. This allows insiders to use attack paths[19] that may be made up of a non-continuous series of tasks. For example, the gathering of administrative credentials (either through social engineering or compromise of systems) to defeat measures such as segregation of duties could take place over several weeks, months or years.

SPECIFICATION

Computer security policy and programme

4.52 The computer security policy[20] (ref NST045 [10]) is a document which contains the computer security requirements and objectives of the facility that apply the principles of a graded approach and defence in depth. These are the high-level requirements that are specified by the operator, in compliance with applicable regulatory requirements, and cannot be exempted or invalidated. The computer security policy is an input to facility CSRM. The facility CSRM may refine the facility computer security policy or may define it if no policy already exists.

4.53 The operator should develop and document its CSP[21] as part of facility CSRM. The CSP is a framework for implementation of facility computer security policy that will be used throughout the lifetime of the facility. The contents of a typical CSP are detailed in section 7 and will include the set of computer security requirements imposed on the facility in addition to those requirements identified by a risk-informed approach.

4.54 The operator should define computer security requirements in the CSP for the following, which are described in more detail in section 7:

— Organization roles and responsibilities

— Risk, vulnerability, and compliance assessment

— Organizational security procedures

[19] An attack vector is a node in an attack tree. An attack path is path through an attack tree from start to consequence.

[20] Some organizations may refer to computer security policy as strategy.

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

— System security design and management

— Asset and configuration management

— Personnel management

4.55 The operator should specify within the CSP those baseline computer security measures that are mandatory for each security level. These measures are likely to consist of requirements upon organizational processes. As the CSP manages organizational processes, these measures will have relation to governance and procedures.

4.56 Requirements for the strength of computer security measures should be identified and defined for each security level and should comply with national regulatory requirements (if applicable). Exceptions to the application of a specific measure within a security level are strongly discouraged and should be documented and justified within facility CSRM.

4.57 The principal facility CSRM outputs from the specification phase are a compliance report for the competent authority and the CSP (or revised CSP), which should include:

— A statement that indicates the level of computer security protection to be provided. This statement could be a qualitative or quantitative value, but should also be verifiable.

— The requirement to perform and document periodic computer security reviews and risk assessments in each stage of the lifetime of the facility.

— The definition of the roles and responsibilities required to support computer security.

— The specification for the facility computer DCSA should combine the requirements resulting from the risk-informed approach and any computer security requirements imposed on the facility. The DCSA should include:

  - The requirements for a graded approach (e.g. the number of computer security levels);
  - The requirements for defence in depth;
  - Any additional requirements for authenticity, non-repudiation, and traceability necessary to meet the required level of protection by each security level;
  - The requirements that will facilitate and maintain the capability for the facility to prevent, detect, delay, mitigate and recover from cyber-attacks;
  - The requirements for formal logical or physical boundaries such as security zones and security levels in which defensive measures are deployed

4.58 The CSP may consist of a single document or a collection of separate documents.

4.59 The CSP should be reviewed by the competent authority alongside the compliance report.

Assignment of facility functions to security levels

4.60 The facility CSRM should identify or make use of an ordered list of facility security functions arranged by the significance of the facility function as the basis for the application of a graded approach, to provide the highest level of assurance of protection to those functions having the highest potential to lead to the most severe consequences.

4.61 In some cases, facility security functions may not be sufficiently segregated or clearly demarcated to allow for definition of function boundaries[22]. The inability to separate facility security functions from one another greatly increases the complexity of the assignment of the significance of the facility function, which increases the difficulty in applying a graded approach. It is imperative that facility functions are distinct and independent from one another insofar as is possible. Consequently, the operator may consider modification of the facility with the aim of simplifying the application of the graded approach. This simplification may also benefit the implementation of defence in depth.

4.62 The aim of the security level concept is to simplify the application of a graded approach.

4.63 The operator should identify the number of security levels to be implemented, informed by applicable regulatory requirements. For example, a facility could choose to implement distinct and different security levels for each facility function. However, the complexity of policy, design, implementation, training, maintenance, verification and validation increases with the number of security levels. Implementing a limited number of security levels allows for common approaches and methods to be used. Therefore, the facility may choose to implement a smaller number of levels (e.g. 5 levels) to simplify implementation. However, this benefit should be considered along with the penalty of applying more stringent measures to facility functions than absolutely necessary in all cases.

4.64 The operator should document in the CSP:

— The number of security levels and requirements for their associated computer security measures;

— The ordered list of facility functions indicating how they have been assigned to security levels.

[22] The specific implementation of systems supporting these features is assessed and validated in the system level risk assessment.

Defensive computer security architecture specification

4.65 The operator should specify the requirements for a DCSA by which all facility functions are assigned a security level and protected according to the applicable requirements.

4.66 The operator should specify within the DCSA those baseline computer security measures that are mandatory for each security level. These baseline measures may consist of technical, administrative and physical control measures.

4.67 The operator's requirements for the DCSA should aim to eliminate or limit the number of attack vectors, identified in the threat characterization, that the threat may exploit to compromise facility functions. Similar processes may include those detailed within Ref. [16].

4.68 Computer security boundaries[23] should be required between facility functions that have different security levels.

Requirements in the DCSA to implement a graded approach

4.69 The DCSA specification should express the overall requirements (including the number of security levels) and should include the strength of measures for each security level, the strength of measures between different security levels and rules for communication between zones at different security levels.

4.70 The DCSA specification should ensure that facility functions with the highest significance are assigned to the most stringent security level. Requirements for communications between facility functions should be defined. Data flow should be controlled between facility functions of different security levels based on a risk informed approach.

4.71 The DCSA specification should ensure that design complexity is reduced where possible to simplify implementation of computer security measures. Decreasing complexity of computer security measures can increase both performance and reliability.

Requirements in the DCSA to implement defence in depth

4.72 The DCSA specification should require defence in depth through the combination of successive layers of computer security measures that have to be overcome or circumvented by an adversary in order to achieve their objectives through compromise of facility functions.

[23] Computer security boundaries are defined in this publication as the logical and physical boundaries of a system or a set of systems at the same security level, and therefore may be secured by the application of common security control measures (e.g. computer security zones).

4.73 The DCSA specification should require a designed mixture of technical, physical, and administrative control measures to provide defence in depth.

4.74 The DCSA specification should ensure that a compromise or failure of a single computer security measure does not result in severe or unacceptable consequences.

4.75 The DCSA specification should require independence and diversity of the measures to ensure that a common vulnerability cannot allow a threat to bypass multiple layers of defence in depth.

4.76 The DCSA specification should require for the implementation of defence in depth between adjacent layers and within each layer. Layers of defence may use a combination of security levels and zones. For the most severe consequences (i.e. high radiological consequences due to sabotage, unauthorized removal of Category I nuclear material), the requirements for computer security measures should ensure that these measures are implemented within distinct, independent and multiple layers within the level and between adjacent levels with the aim of providing fail-secure[24], deterministic attributes.

Defence in depth between layers

4.77 The DCSA specification should require each layer be protected from cyber-attacks originating in adjacent layers. Layers and their associated computer security measures should prevent or delay advancement of attacks.

4.78 The DCSA specification should require that the computer security measures used in a layer are diverse and independent of the computer security measures used in an adjacent layer, to mitigate common cause failures of protection mechanisms used for isolation between layers.

Defence in depth within a layer

4.79 The DCSA specification should require that each layer employs independent and diverse computer security measures within that layer. In accordance with the principle of a graded approach, the requirements for independence and diversity should be greatest for those layers requiring the most stringent protection (i.e. security level 1).

[24] Fail-secure is a failure of a measure that maintains the security of the function that it protects.

VERIFICATION AND VALIDATION ACTIVITIES - COMMON TO FACILITY AND SYSTEM CSRM

Verification activities

4.80 Verification activities may occur between any two phases of facility or system CSRM (see Fig. 7).

4.81 The objective of the verification activities is to evaluate the quality of outputs of an activity against the specification, to ensure sufficient quality before used by a subsequent phase.

4.82 Verification activities may include:

— Verifying the facility or threat characterization

— Verifying that the DCSA as designed, or as built, satisfies the computer security requirements.

4.83 The consequences of verification activities may include:

— Addressing any system deficiencies in the design or implementation in order to meet the system requirements.

— Analysing and implementing upgrades that may be necessary to address identified deficiencies and improve system performance.

4.84 These verification activities may involve evaluation methods including exercises, performance testing, simulation or analysis (such as vulnerability assessment) (see para. 4.96).

4.85 For example, evaluation of outputs based upon Attack vector analysis considers the path or flow of information between systems, devices, networks, and locations. The exchange of information between systems allows potential threats to exploit these pathways leading to potential compromise of systems and functions. Attack vector analysis at this stage considers generic pathways with the aim to minimize or eliminate threat access to these vectors.

4.86 Specifications of computer security measures should be analysed to ensure that they are effective in reducing the opportunity of the threat to compromise functions.

4.87 The operator should perform verification activities to evaluate the CSP. Specifically, the identification and assignments of functions to security levels, and the assignment of computer security measures to those levels.

4.88 The operator should use a graded approach when determining the level of effort to be applied to verification and validation activities. The greatest level of effort should be applied to those functions or systems assigned to the most stringent security levels (i.e., those requiring the greatest level of protection) as listed in the facility or system computer security risk assessment report.

4.89 Verification activities should be repeated on an annual or other regular basis to take into account any changes in targets, programme or requirements.

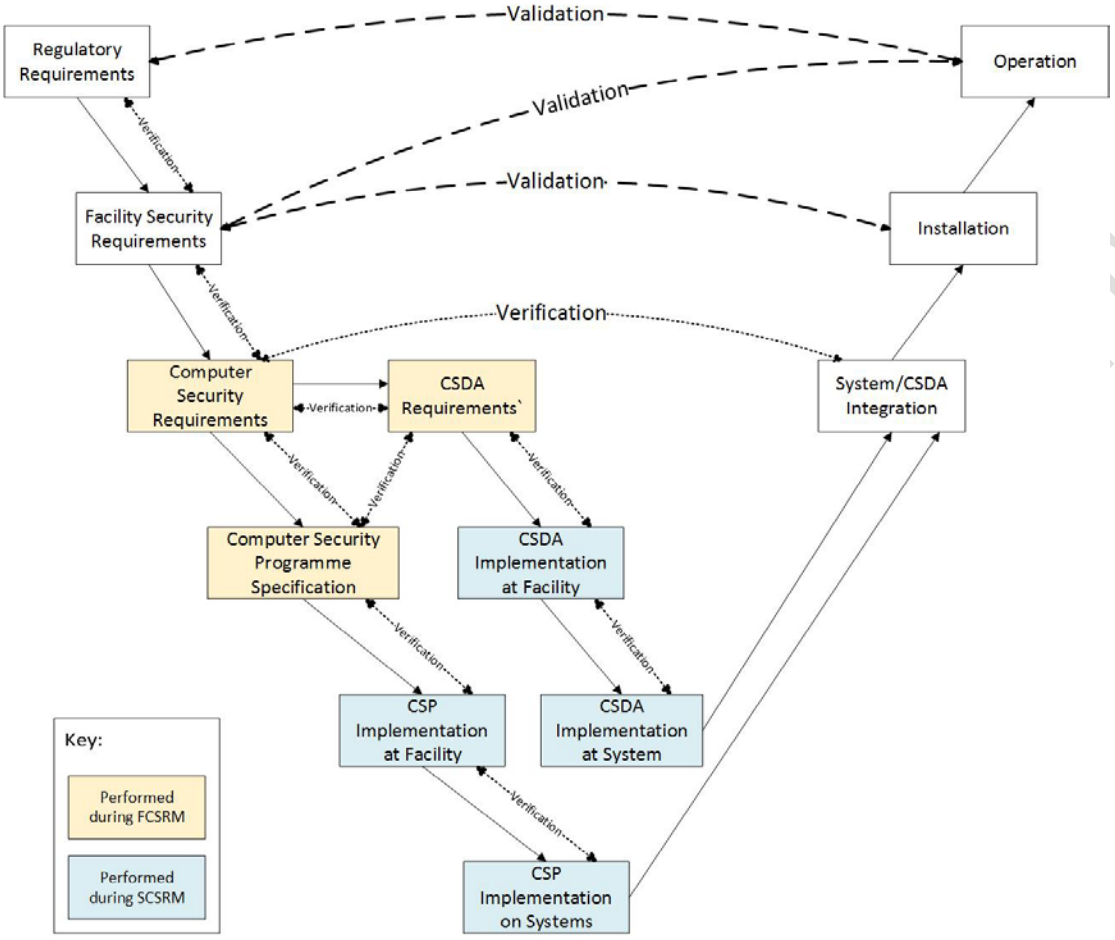

FIG. 7. Overview of verification and validation activities within the computer security risk management process.

Evaluation methods

4.90 The operator should plan, conduct and document the evaluation and performance testing of its CSP in a manner designed and implemented to satisfy the regulatory requirements. Appropriate parts of this activity should be considered for both facility and system CSRM as well as throughout the lifetime of the nuclear facility (i.e. during design, construction, licensing, operations, changes or upgrades, decommissioning and management of radioactive waste and spent fuel).

4.91 The operator should consider using independent experts to review its CSP evaluation.

4.92 The threat characterization provides the basis by which the facility can conduct an analysis to confirm the assumptions made during the assignment of functions to the appropriate security level. The use of credible scenarios may allow for greater level of assurance in the quality of the assessment. These credible scenarios should not consider the technical implementation of the system but consider effects of compromise on the function (see Annex I for sample scenarios).

4.93 The CSP (including DCSA) provides detection, delay and response functions through physical (e.g. structure), technical and administrative (e.g. personnel, procedures) elements. The interaction of these elements with the facility safety and security functions, and their assigned systems, makes the evaluation of CSP effectiveness a challenging task.

4.94 The operator should justify all assumptions involving likelihood (e.g. vulnerability, exposure, opportunity) prior to use. The consideration of likelihood should be equal to 1 when involving postulated scenarios that can result in URC or unauthorized removal of categorized nuclear material (i.e. compromise of SDA).

4.95 A number of methods are available to evaluate the effectiveness of the CSP against insiders who have authorized access to the nuclear facility and outsiders who do not have authorized access. Evaluation methods include:

— Attack vector analysis (or attack tree): This involves building a set of conditions involving different adversary paths, to determine whether there is high assurance the attack will fail (i.e. no attack path) or be detected and responded to prior to the attainment of the objective of the threat actor. The attack vector analysis should be used to assess whether the computer security programme and defensive architecture is effective in eliminating or minimizing the potential for the threat to access the attack vector. The determination should take into account the threat characterization.

— Simulation. These include computer based simulations of the CSP (including DCSA) elements and table-top exercises that allow consideration of security and contingency plans as well as decision-making by the adversary and Computer Security Incident responders. These tools are generally used to judge the overall performance of the CSP, taking all measures into account. For example, table-top exercises may assist in determination of the opportunity available to the adversary based upon their capabilities and characteristics (e.g. insider) or exposure of vulnerabilities of the function.

— Exercises. These range from both facility and system performance-testing (e.g. penetration tests) as well as force-on-force exercises (e.g. blended attacks) in either in-place conditions or in test (e.g. lab environments). These exercises address the effectiveness of the CSP in providing protection to the entire or parts of the facility, specific set of systems, or set of measures against a simulated adversary attack. In this evaluation phase, data are collected concerning the performance of computer security measures and used to evaluate the overall effectiveness of the CSP.

4.96 Simulation and exercises are typically performed as part of scenario analysis, in which very detailed postulated attacks (‘scenarios’) are identified and then simulated or used as a basis for

exercises. Scenario analysis typically builds upon Attack vector analysis by considering specific adversary tactics, techniques and procedures for defeating computer security measures.

4.97 CSP, DCSA, or computer security measure effectiveness may be measured quantitatively or evaluated qualitatively or both. The competent authority may prioritize deterministic evaluation methods be used for different types of targets, threats and scenarios that have the potential to result in unacceptable consequences. It is suggested that the overall CSP effectiveness be conservatively defined as the lower quantitative or qualitative effectiveness of the CSP that still meets regulatory objectives, when all adversary tactics, techniques and procedures and credible scenarios have been considered.

Validation

4.98 The operator should perform validation to ensure that the CSP, the DCSA and specified computer security measures, and other subordinate elements of the CSP provide the appropriate level of protection.

4.99 The CSP should be assessed for its effectiveness in securing functions. This assessment should be verified against the computer security policy and the DCSA requirements to ensure that level of protection required can be assured.

4.100 Where the level of protection indicated in the CSP is not validated through analysis, the operator should revise their CSP and defensive architecture to increase protections. The operator may not lower the level of protection.

4.101 The operator should validate the outputs of both the facility and system CSRM processes. The facility CSRM outputs should be validated against the facility and regulatory requirements. The system CSRM outputs should be validated against the CSP and DCSA and facility requirements.

4.102 The operator should aggregate Facility Risk Level, including reference to applicable regulatory and design requirements. This should also include the System Risk Level for each individual system that contains an SDA.

4.103 The operator should validate the facility and system level risk assessments against the DBT using scenarios that involve multiple systems and the overall architecture. These scenarios differ from those performed in system CSRM (para. 5.6) and those that may be specified in the DBT. These scenarios may include blended attacks involving compromise of multiple, separate systems with the aim of identifying vulnerabilities at the facility level that have the potential to result in severe consequences (e.g. URC, Unauthorized removal of nuclear material).

Facility (aggregate) scenario identification and development

4.104 The DBT provides the instrument by which the facility can conduct a scenario analysis to validate the assumptions made during the assignment of functions to the appropriate security level. The use of credible scenarios may allow for greater level of assurance in the quality of the assessment.

4.105 The facility should identify and develop scenarios based upon the state's assessment of threat as detailed in the DBT. It is strongly encouraged that the facility engages expertise in cyber-attacks and threat capabilities in the development of these scenarios. This expertise may be found in state regulatory bodies, such as intelligence services and law enforcement.

4.106 The facility is responsible for providing these detailed scenarios to the state's CA to allow for a complete and comprehensive review and acceptance.

4.107 Analysis and evaluation of scenarios may provide insight in to the most vulnerable points within the facility, processes, system architectures and procedures. Further analysis may be required to identify essential computer security measures already in place or those requiring implementation to counter the identified vulnerable areas.

4.108 Scenarios should be used to verify the output of the facility computer security risk assessment process, including the analysis possible adversary tactics, likelihood of attack, and potential consequences.

4.109 The scenarios should be periodically evaluated to ensure they are sufficient to meet security objectives against a very dynamic threat.

4.110 The DBT analysis should consider multiple attack vectors (i.e., network, local), insiders, or elements (i.e. blended attack). The DBT should also consider the potential for sequential cyber-attacks that multiply the consequence but where there are no indications of collusion between different types of threat actors (non-collaborative attacks).

4.111 The development of scenarios should not consider the evaluation of potential computer security measures as this should occur only after acceptance by the competent authority.

4.112 Threat scenarios may include, but not limited to:

— Stand–alone attacks, a single threat actor.

— Coordinated attacks, a group of threat actors working together.

— Opportunistic attack, independent threat actors that combine attacks. A vulnerability is publicly disclosed that allow for nuclear security threats to target the facility systems and equipment.

— Specific threat capabilities [7].

— Blended attack, an attack with cyber and physical elements.

Note: Attack trees or attack vector analysis are potential methods for identifying different threat scenarios as well as identifying protective strategies.

4.113 It is recommended that scenarios be periodically reviewed and updated whenever:

— The DBT is updated;

— Significant modification of facility (modernization) is undertaken,

— Changes are made to security processes, critical countermeasures, and architectures,

— New credible attack vectors are identified;

— New regulatory requirements/actions are implemented;

— New critical vulnerabilities become known, especially those involving important computer security measures, and

— The threat characterization changes.

4.114 For the most significant scenarios, specific attack vectors and components should be identified and their risks documented.

FACILITY CSRM OUTPUT

4.115 The facility CSP document(s) should describe the computer security measures required to maintain protection against threat actors analysed during the assessment.

4.116 The output of the facility CSRM should comprise the facility CSP document(s) that defines which functions are critical and important for the safe and secure operation of the facility including those that supports other important functions as identified by the operator or regulator and to identify the possible associated consequences if these functions were subject to cyber-attack. Based on this significance information, these functions can be assigned to the appropriate security level which is used to ensure that sufficient computer security measures are put in place to reduce their susceptibility to cyber-attacks. Finally, a determination of aggregate facility risk based upon an evaluation of the effectiveness of these measures in providing protection against threat actors as detailed in the DBT or equivalent. The assessment should identify whether digital technology is implemented within these systems.

4.117 The facility computer security risk assessment report should include an analysis of security system design and configuration management as detailed in the CSP. This should be a high-level review and analysis only. A more detailed analysis should be performed in the system CSRM.

4.118 Facility functions and their assigned corresponding systems in the facility CSRM should undergo comprehensive system level risk assessments as detailed in the next section.

COMPETENT AUTHORITY ACCEPTANCE

4.119 The operator's assessment of aggregate risk and individual risk values for functions should be provided to the competent authority for acceptance.

Interaction of facility and system CSRM

4.120 The risk management processes detailed in the facility and system CSRM have significant interactions. The facility CSRM results in the assignment of one or more facility functions to individual systems. Therefore, the facility CSRM output sets the scope for all systems' CSRM, but may be informed by the outputs of system CSRM. For example, multiple facility security functions may be assigned to a single system. This assignment may reduce the potential to segregate the system into separate zones, thereby limiting the zone model to either a physical boundary or logical boundary (and not both).

4.121 For legacy facilities or systems, specific structures, systems, and components (SSCs) may not be modifiable or alterable. This limitation at the system CSRM to comply with stringent requirements may demand the operator to revisit the facility CSRM to determine a suitable CSP and DCSA specification that meets the security requirements.

4.122 The facility and system CSRM processes are iterative, as illustrated in Fig.6. The facility and system CSRM outputs should also be considered for review when the following occurs:

- The facility CSRM or facility safety analysis is revised;
- The system is limited in the measures that can be applied (e.g. non-compliance with facility CSRM outputs);
- System modifications are made that have the potential to affect facility CSRM;
- Relevant security events or incidents occur; or
- New or changed threats or new vulnerabilities are identified.

4.123 The review of the outputs of both the facility and system CSRM processes needs to be included in the facility change management process to assure that the outputs are consistent with one another and kept up to date. These analyses also assist on setting the requirements for new systems or implementations (e.g. defining the security levels).

4.124 Risk trends of successive facility and system CSRM outputs should be periodically assessed to identify the following types of adverse patterns:

— A risk is showing a clear pattern of increasing towards or beyond the unacceptable risk threshold (what do we do to prevent exceeding this risk threshold?), or

— A risk has reached or exceeded the threshold (what do we do when that happens – e.g., report to the competent authority, prioritize implementation of compensatory measures,).

When the adverse risk patterns are identified, a mitigation plan should be defined that includes prioritized implementation of compensatory measures consistent with the urgency identified from risk trend data. Adverse risk patterns associated with individual systems should be analysed to ensure the risk pattern has not invalidated the facility CSRM.

4.125 For example, system surveillance assessments may be performed continually, and system performance monitoring reports may be approved periodically. Outputs from the corresponding systems' CSRM should be reviewed in the facility CSRM to ensure there is no change in the overall facility risk.

5. SYSTEM COMPUTER SECURITY RISK MANAGEMENT

GENERAL CONSIDERATIONS

5.1 Facilities should establish a systematic and periodically reviewed process for managing the computer security risk of SDAs within the systems that perform the facility functions, identified in the facility CSRM[25]. Compromise of these SDAs typically has the potential to lead to very high, high, and medium severity consequences (see NST045 [10]). This process may be performed using system CSRM for each system, as described in this section. The system CSRM should consider all digital assets in the system, including SDAs.

5.2 System CSRM is a complex process that should be performed by a multi-disciplinary team similar to the facility CSRM. However, the system CSRM team may be customized to address specific considerations associated with each system.

5.3 The operator should use a graded approach when determining the level of effort to be applied to risk management for each system. The greatest level of effort should be applied to those systems that support or provide the facility functions assigned to the most stringent security levels (i.e. those requiring the greatest level of protection) as listed in the facility computer security risk assessment report.

5.4 The operator should prioritize performance of system CSRM for systems implementing those facility functions that have been assigned to the most stringent security levels.

OVERVIEW

5.5 The primary objective of system CSRM is to evaluate and manage whether the appropriate level of protection (i.e. that required for its security level) is afforded to a specific system according to the requirements defined in the facility CSRM.

5.6 To meet this objective, the system computer security risk management:

— Assesses a facility function that has an assigned security level and identified system(s). The system CSRM considers other facility functions having interactions and dependencies listed in the facility characterization phase of the facility CSRM (i.e. definition of system functional boundaries).

[25] It may be justified to extend this analysis to include other systems excluded from scope of the facility computer security risk assessment that are not directly relevant to nuclear security objectives.

— Identifies the scope of each system including those systems supporting the other facility functions having interactions and dependencies with other systems. This may include analysis of the overall system architecture to identify the locations, boundaries, interfaces and communication paths of systems containing SDAs.

— Identifies (and inventories) digital assets within these systems

— Establishes and defines security zones based on CSP and DCSA requirements,

— Identifies SDAs and other digital assets within the zone boundaries via Asset Analysis. This requires an assessment of the digital assets to determine whether they are vital to the performance of the facility function.

— Assigns SDAs a security level based on their facility safety or security function (i.e. facility CSRM level assignment)

— Applies the most stringent security level to the zone based upon the associated functions provided by digital assets within the zone. Assigns the digital assets within the zone to the same security level. As a result, all SDAs and digital assets within a zone are assigned to the same level.

— Applies baseline computer security measures (see paras 4.55 and 4.66) and additional computer security measures to the SDAs and other digital assets (including at the zone boundaries), taking into account the specificities of the identified system(s) to meet requirements of the assigned security levels.

— Provides a process to determine the technical control measure(s), administrative control measure(s) or physical control measure(s) that can be applied to meet the baseline computer security measures.

— Analyses specific attack vectors, scenarios and vulnerabilities to verify the effectiveness of the applied computer security measures.

— If the analysis shows that the system is not sufficiently protected by the baseline computer security measures, then additional or compensatory measures should be applied to reduce the risk to an acceptable level. For example, scenario analysis confirms that the system is exposed and vulnerable to specific attack vectors, scenarios or vulnerabilities.

— Issues a system CSRM report for the identified system.

5.7 The above processes may result in the identification of digital assets that are not part of systems assigned to facility functions (i.e. during facility CSRM) or were not identified as being within a system or zone boundary (i.e. during system CSRM). Therefore, an additional analysis

should be performed to ensure the inclusion of all digital assets in a facility's assessment and CSP to ensure completeness in the coverage of the facility.

5.8 Output of system CSRM should include the prioritization of risks to determine the appropriate implementation of computer security measures. The assessment should consider the location of the elements that make up the system, vulnerabilities, and security levels and zones if defined, as well the significance of SDAs within the system under assessment.

SYSTEM CSRM PROCESS

5.9 The operator should perform system CSRM:

- When a facility is first constructed (to apply to every system);
- When a facility is modified (to apply to every system);
- When a new system / digital asset is deployed (to apply to every affected system);
- When a system / digital asset is modified (to apply to every affected system);
- When the facility CSRM is reviewed (to apply to every system).

5.10 The following inputs should be identified and made available for use within the system CSRM:

- Facility CSRM outputs (e.g. CSP and the DCSA)
- Safety report
- Site security plan
- Computer security policy

Overall DCSA requirements for computer security

5.11 The operator should use the DCSA requirements set out during facility CSRM to facilitate and maintain the capability for systems and digital assets to prevent, detect, delay, mitigate and recover from cyber-attacks. Defensive architectures include, but are not limited to, logical or physical boundaries such as security levels and security zones in which defensive measures are deployed.[26]

5.12 Computer security measures should be effective throughout the lifetime of the facility, for example during periods of maintenance and decommissioning, when significant configuration changes will be made. Monitoring, maintenance and recovery activities should not provide a vector by

[26] An example of such a defensive architecture is one that includes a series of concentric defensive levels of increasing security and considers both hardware and software components

which a threat may bypass computer security measures, for example bypassing the protection on communication pathways between facility functions having different security levels.

5.13 Computer security boundaries[27] should be implemented between zones that have different security levels and are protected using different computer security measures.

5.14 Data flow should be controlled between zones of different security levels and between zones on the same security level, based on a risk informed approach to ensure that the defensive architecture remains effective.

Definition of system boundaries

5.15 The scope boundary for each system's CSRM encompasses the systems identified as providing the facility function based upon the facility characterization. This should include considerations for those functional dependencies with the identified systems.

5.16 The system CSRM process should identify and document the system boundaries. These include all components, subcomponents, interfaces, and environments of the target system during all stages in the lifetime of the facility, as well as those systems that provide support or auxiliary functions.

5.17 The following is a listing of steps to define the boundaries of the system under assessment: operation

- Identify all the interfaces of the system
- Identify all the ingress and egress data points of the system. Any means of injecting malicious code or 2 into the system should be considered in the system security risk assessment. For example, malicious code could be injected via communication connections, supplied products and services and/or portable devices that are temporarily connected to target equipment.
- Identify the procedures that require interaction (e.g. for normal usage or patching) with the system.
- Identify which (if any) data pathways are not covered by procedures or system operation and maintenance. Unused data pathways are a significant risk and should be identified.
- Identify the assigned security level of the system

[27] Computer security boundaries are defined in this publication as the logical and physical boundaries of a system or a set of systems at the same security level, and therefore may be secured by the application of common security control measures (i.e. computer security zones).

— List security measures applied to the system or its environment

Identification and construction of computer security zones

5.18 The CSP and the DCSA specification produced during facility CSRM will place computer security requirements on the implementation of the zone model. The CSP will also include a list of facility functions and the systems assigned to them.

5.19 The operator should implement the requirements placed in the DCSA specification. Additional considerations (see NST036 [9]) for implementation of security zones should include the following:

— Systems belonging to the same zone form a trusted area for internal communications between those systems (i.e. internal trusted zone area); should follow the most stringent computer security requirements assigned to those systems;

— Safety architecture requirements (e.g. redundancy, diversity, geographic and electrical separation, single failure criterion) are maintained;

— The principle of defence in depth should be applied both within each of the individual computer security zone by using diverse, independent, and overlapping administrative, physical and technical control measures and between computer security zones.

— The ability of technical control measures to provide continuous or automatic preventive or protective actions (i.e requiring no human intervention) should be considered to complement physical or administrative control measures (i.e. requiring human intervention).

— All connections between zones require decoupling mechanisms for data flow, built on zone-dependent policies, to prevent unauthorized access and undesired interactions between the zones. Those connections may comprise continuous network connections or intermittent connections, for example using removable media.

— The level of decoupling between zones is dependent on the security levels of the two zones. This includes technical control measures, e.g. packet-filters, gateways and data diodes, implemented at zone boundaries to restrict data flow and communication between different zones.

— When security policy permits and when systems or digital assets from two adjacent security levels need to communicate, the initiative to establish the connections should be allowed only from the higher security level to the lower one.

— If the initiative to communicate must unavoidably come from the lower security level to the higher security level, exceptionally stringent decoupling mechanisms should be used.

— Authorized mobile devices or other temporary equipment that need logical or physical access to digital assets in a zone should be treated as a form of intermittent connection to that zone and subject to additional computer security measures when used in more than one zone.

— Zones can be partitioned into subzones to improve the configuration and to prevent undesired interactions with other systems.

5.20 Digital assets should be considered for separation into distinct zones when any of the following conditions are present:

— Systems perform different functions,

— Systems with the same functionality are assigned different security levels,

— Systems with the same functionality and the same security level are assigned to different people who are responsible for the system,

— Servers that are communicating to multiple clients (for instance those used with distributed control systems and programmable logic controllers). The objective is to ensure that the zone requiring the most stringent protection contains the least number of unique assets.

— Systems that require communication with common infrastructure components used by multiple systems (for example directory service, time server, security log collector) but not requiring communications between these systems. This ensure communication between zones containing these types of systems and the zones containing the common infrastructure components external to the systems are monitored and controlled.

— Administration systems (especially when the same systems are used to administer several functional systems)

— Where regulations require distinct zones.

5.21 Digital assets may be considered for assignment to different zones, despite being of the same security level, for any of the following conditions:

— The digital assets are assigned to different facility functions. This improves the separation of the zones and systems assigned to facility functions.

— Different organizational units or work groups are responsible for the digital assets.

— Isolated computer-based systems or several computer-based systems of the same functional system hosted on an isolated network, and

— Individual zones assigned to separate redundant systems performing the same facility function

— If regulation requires separation.

5.22 Network connections and local exchange (i.e. removable media, mobile devices) of data between two systems of a different zone should be limited to allow only those needed. Zone borders require decoupling mechanisms for data flow built on zone dependent policies to prevent unauthorized access and undesired interactions between the zones. Network connections across zone borders should be established from the higher-level zone into the lower-level zone. Restrictions can be applied using not only a technical control measure (i.e. a filtering device), but also organizationally (i.e. a procedure defining rules for the use of removable medias on a specific system). Authorized network connections and disconnected exchange of data should be documented.

5.23 A specific zone can only include systems (and digital assets) of the same security level. The zone is assigned with the security level of the hosted systems within the zone. A given security level can and should include different zones. However, technical specificities might make it difficult to separate systems assigned to different security levels into different zones and apply boundary measures. In this case, the systems of the less stringent security level could remain with the zone of a more stringent security level, provided that the systems assigned to the less stringent security level are considered as being assigned to the higher security level and that the security measures defined for this the more stringent security level are applied to the systems assigned to the lower level.

5.24 Necessary communications should be allowed only between zones of the same or zones of an adjacent security level. Necessary communications between zones of two different security levels should be limited to specific zone entry points (for example: one entry point filtering connections between several security level 2 zones and several security level 3 zones). Security solutions for all entry points should be defined in an efficient and consistent manner to enforce an overall secured architecture. A zone entry point should implement specific checks, for example on the content of data or its digital signature. It should also have specific event log monitoring.

5.25 Because zones are comprised of systems with the same or comparable significance for facility safety and security, each zone should have a computer security level assigned, indicating the computer security measures to be applied for all systems and digital assets in that zone. There may be one or many zones with the same security level because those zones require the same computer security measures. Zones are a logical and physical grouping of computer systems, while levels are a policy concept that represent the degree of protection required.

Identification of digital assets

5.26 The following records may be useful in assisting with the identification and listing of the system's digital assets:

— System asset database (including all digital components);

— Software and firmware inventory

— Sensitive information relevant to the system e.g. configuration files [5]

— System network and architecture diagrams;

— Design documents and records such as safety hazard analysis, and test reports;

— Data flow diagrams;

— Associated user and system accounts and privileges; and

— Procedures related to the identified systems.

5.27 The list of digital assets should be classified and security-protected (i.e. sensitive information). If management of digital assets is centralized, the inventory may exist as a single record that is structured at the system level.

5.28 The list of digital assets may include computer-based systems identifiers, key technical specifications and data, their interfaces, references to facility level and system level risk assessments, and their assigned owners.

5.29 The list of digital assets should be maintained during the lifetime of the facility and periodically reviewed. The listing should also be reviewed for potential update whenever a system level risk assessment is performed.

5.30 Digital assets that are also sensitive information assets (e.g. associated with unacceptable consequences) should be designated as SDAs. However, digital assets that may facilitate or contribute to adverse effect on the function of SDAs, should also be identified and considered within the scope of the Asset Analysis. This analysis should determine whether to designate these components or systems as either digital assets or SDAs. This determination should be consistent with the CSP.

System computer security architecture - including digital asset analysis

5.31 The operator should identify key tasks and activities necessary to provide computer security for the facility. These tasks and activities should be associated with computer security levels and their corresponding computers security measures.

5.32 The operator should specify the necessary computer security measures that provide the required capabilities to allow for the performance for those tasks and activities associated with the computer security level.

5.33 The system CSRM process should identify all SDAs. Digital assets that are not SDAs may be considered during analysis when specific threats or risks are identified that could adversely affect an SDA. However, the level of effort associated with the system level risk assessment should be graded

to ensure that those systems assigned the highest level also benefit from the most robust assessments (i.e. Security Level 1)

5.34 In general, independent, diverse, and redundant systems that perform the same function should be assigned the same security level. The assignment of either (or both) of these systems to less stringent security level is strongly discouraged and may only be considered on a strict case by case basis and if supported by a complete justification and security risk analysis.

5.35 Asset analysis of a SDA should include hardware, firmware, and software information that can be used as input to a vulnerability analysis. The vulnerability analysis may recommend system hardening of the SDA to reduce attack surface.

5.36 An analysis of the interfaces of the systems (including its digital assets) should be performed and categorized with respect the zone boundary. It may be beneficial to use the following categories:

— Trusted internal communications (e.g. communications within and between systems or its digital assets within a zone, including internal pathways to security zone boundary devices): there exist no effective computer security measures that monitor or protect internal trusted communication pathways from cyber-attack. Boundary devices may include technical control measures such as firewall and data diodes.

— External authorized communication pathway (e.g. interconnection between zones using authorized pathways via authorized boundary devices): these interfaces are normally between separate systems providing different functions. Computer security measures implemented in authorized boundary devices ensure that all communication pathways are continually monitored and only those that are authorized are permitted. These pathways could be either analogue or digital interfaces.

— Potential unauthorized communication pathway (e.g. the capability to make an unauthorized connection between zones using network cables, wireless connections, removable media): these unauthorized communication pathways can be made between systems or their digital assets that have physical or logical proximity, for example, systems that are physically located in the same area with no physical barriers controlling access between them.

5.37 All digital assets with internal trusted communication pathways within a zone should be assigned the same security level (i.e. the zone's security level). This security level of the zone should be the most stringent level required for any of the systems or its Das within that zone.

5.38 Zone boundary devices should be assigned a security level equivalent to the highest (most stringent) level of equipment for which they are accredited for providing protection.

5.39 For example, a firewall between two zones of different levels has an internal trusted communication pathway with the zone assigned the higher security level while providing an external authorized communication pathway with the zone assigned the lower security level.

5.40 Another example of a zone boundary device may be a malware-detection kiosk (e.g. Anti-virus scanner) that is used to scan removable media and mobile devices prior to entering and exiting the zone. This kiosk would be assigned based upon the highest security level of the zone it is accredited with providing protection. In this example, the operator needs to ensure that the kiosk does not provide a common vector for the compromise of multiple zones and systems (i.e. kiosk vulnerability is exploited which then propagates compromise to the equipment intended to be protected by it).

5.41 All SDAs that are connected via an internal trusted communication pathway should comply with the overall DCSA requirements.

5.42 All SDAs that are connected via an internal trusted communication pathway should be at assigned equal or sequential security levels. The assigned security levels should be the most stringent level required any of the SDAs connected and the next level (e.g. Level 1 and 2; Level 3 or 4)

5.43 SDAs may be allowed to have proximity to other SDAs providing that computer security measures are in place to ensure these systems cannot interact though potential unauthorized communication pathways. These measures may be solely administrative control measures. Typically, SDAs are assigned to the highest security levels or the adjacent lower levels (e.g. Levels 1 to 3).

5.44 Digital assets which are not authorized to communicate with SDAs, should not be allowed access to locations (logical or physical proximity) where there is the potential to have access communication pathways of SDAs. The DCSA should consider the design and maintenance of robust computer security measures to eliminate or create compensating measures to reduce the potential for these systems to be provided with access to these pathways (i.e. proximity).

5.45 Unassigned digital assets (i.e. digital assets not assigned a security level) should never be in proximity to SDAs. For example, personal mobile devices or vendor equipment not evaluated and assigned should be treated as malicious devices to SDAs and not be provided with proximity to facility SDAs.

5.46 Asset analysis should evaluate the effects of cyber-attack on the system and the risk to the facility. The credible scenarios may be used as an input into the evaluation. The evaluation should consider that cyber-attacks may occur during any stage of the lifetime of the facility or any phase of the system life cycles.

5.47 Attacks may affect an individual system or multiple systems and could be used in combination with other forms of malicious acts causing physical damage. These potential specific component-level interactions should be listed within the assessment report.

5.48 Malicious actions that could change process signals, equipment configuration data or software should be considered in the system level risk assessment.

5.49 The analysis should identify the locations and pathways where information exchange occurs within the system (including its digital assets). The analysis should also identify and justify the implemented measures to protect required data flows and communications and identify any possible remaining vulnerabilities. The analysis may be supported by:

— Analyse or supplement by testing the effectiveness of the implemented security measures

— Document the status and define possible improvement points.

— For identified systems, ensure that the software has been subject to a vulnerability assessment,

5.50 For example, consider the exchange of software deliverables (e.g.. source code or object code) between a software development environment and a security system. When determining the effect of a software compiler upon the security system, if no measures are in place, then the compiler (hardware and software) would be assigned to the same zone (and level) as the security system itself since no boundary exists. However, by providing measures to the outputs of the compiler at the system boundary, for example, security testing of the code output, the compiler could be a placed within a separate zone and assigned a different security level than the system itself. The measures placed upon the compiler output are accredited with protecting the system. These measures would be assigned the same level as the system to which they are providing the protection.

5.51 The analysis of digital assets should list and detail the specific computer security measures that are implemented for each system. The control measures should be a combination of technical, administrative, and physical measures.

5.52 The analysis of digital assets should provide a qualitative or quantitative value of the acceptable risk.

Verification of the system computer security risk assessment

5.53 The operator should perform verification and validation of the system computer security risk assessment for each system as defined by the boundaries of the assessment. The verification of system CSRM outputs may utilize the evaluation methods outlined in paras 4.91–4.98 above.

System scenario identification and development

5.54 The DBT allows for the generation of credible scenarios based upon the motivation, capabilities, intentions, and opportunity of potential adversaries (including adversaries using cyber techniques).

5.55 The operator should develop credible scenarios for the individual system based upon the threat characterization to inform the validation of the identified computer security measures that are accredited with providing protection to the system. The credible scenarios should identify potential sequence(s) of adversary actions that may result in compromise of SDAs.

5.56 Development of scenarios is recommended to evaluate protection against common attack vectors. These may include but are not limited to:

— Social Engineering – including phishing attacks;

— Malicious emails;

— Malicious websites;

— Infected mobile media devices;

— Compromised maintenance and inspection equipment;

— Remote Access;

— Insiders (witting and unwitting); and

— Supply chain

5.57 Scenarios should be developed consistent with the DBT or national threat assessment to identify those SDAs that may be exposed to the nuclear security threats. It may be beneficial to commence scenario development by considering the most likely or the highest consequence cases.

5.58 The development of scenarios should have the following aims (in order of significance):

— To determine the highest consequence scenarios involving SDAs; and

— To determine the most likely scenarios involving SDAs.

5.59 Evaluation methods (para.4.96) should use credible scenarios to verify the effectiveness of implemented computer security measures

5.60 The operator should verify that SDAs are appropriately protected against the DBT.

System computer security risk management report

5.61 The output of the system level risk management process should be documented in the system computer security risk management report which includes:

- Identification of all SDAs including the identification of all hardware and software components (to the greatest degree possible) of each SDA.
- Identification of digital assets that are components, interface, support, or have the potential to access communication pathways belonging to SDAs. These may include components of systems assigned a security level.
- Identification of vulnerabilities, deficiencies, or weaknesses in the systems or components. For example, identification of procurement non-compliance (counterfeit or substandard parts), human actions or omissions that might affect security.
- Identification of technical, administrative, and physical control measures.
- Recommendation for implementation of countermeasures
- Recommendations for improvements to countermeasures (i.e., additional technical, administrative, or physical control measures).
- Identification of deficiencies in facility documents or records.
- Classification of sensitive information
- Access control lists for personnel and services
- Corrective actions
- Assessed system-level risk
- Identification and description of other metrics that will assist in evaluation of computer security (e.g., mean time between failures, mean time to repair, mean time to detect, mean time to recover, security quality metrics).

5.62 The system CSRM report should be classified as sensitive information and protected accordingly.

6. FACILITY AND SYSTEM CSRM CONSIDERATIONS DURING SPECIFIC STAGES IN THE LIFETIME OF A FACILITY

6.1 The specific stages in the lifetime of a facility with associated guidance are listed below:

Planning

6.2 The competent authority should provide the State's regulatory requirements relating to computer security and a DBT or threat assessment. The operator should review its plans for the facility to ensure that the regulations can be met.

6.3 During the planning stage, the competent authority should ensure that the facility has a formalized methodology to perform a detailed facility CSRM process.

6.4 The competent authority or the operator should perform the facility CSRM:

— Scope definition

— Development or refinement of the Computer Security Policy

— Threat assessment including development of the threat characterization

— Facility characterization including identification of facility functions

— Development of the CSP including the DCSA specification

6.5 By assuming that the DCSA specification can be met, the competent authority or the operator should verify that the residual risk does not exceed acceptable levels.

6.6 The operator should plan the development of the competencies required to support computer security during all stages in the lifetime of the facility.

6.7 The planning stage may take place in many different locations away from the intended facility site. The competent authority and operator apply computer security measures to the inputs and outputs of the planning lifecycle that contain sensitive information and make use of sensitive information assets.

Siting

6.8 The operator should include computer security in plans from the outset of the siting stage of the facility because some activities involving computer security can only be performed on-site, not remotely (e.g., the use of isolated networks, accessibility for computer emergency response teams, the availability of expertise in computer security when evaluating the capability of the local workforce).

6.9 Siting plans for the location of major equipment should consider the operation of physical control measures that will be necessary to complement computer security measures for security zones, systems and SDAs.

6.10 Siting should consider the availability of local infrastructure necessary to support computer security measures (e.g., emergency communications networks).

Design

6.11 The operator should use the output of the facility CSRM work conducted during the planning stage to ensure that the facility design process considers computer security requirements for facility functions (expressed in the DCSA and in the CSP) as an integral part of the system engineering activities for the facility. This applies for new construction, refurbishment or modification of the facility, as also occur during the operations stage of the facility.

6.12 The design process should automatically consider computer security requirements that arise due the dependencies between facility functions, as identified during the facility CSRM process.

6.13 Computer security requirements should be provided in sufficient detail and if necessary developed, to allow design decisions to be made, the design to be verified and to evaluate design changes.

6.14 The operator should perform the system CSRM process for each system, performing verification on each step of the design of the computer security measures.

6.15 Logical and physical accessibility to the SDAs within vital areas by an insider should be considered in the design stage.

6.16 The operator should develop computer security validation criteria for the commissioning stage. Systems or functions assigned the highest security levels should be independently[28] validated.

6.17 Stakeholders knowledgeable in computer security should be involved in the design process to ensure that:

- Appropriate computer security requirements are included
- Design changes improve and do not reduce computer security,
- The changes as implemented, meet the defined computer security requirements
- The effectiveness review includes computer security.

[28] Independence means the activity is performed by an individual or organization that is independent from the party under review.

6.18 The design stage should generate the necessary direction for the implementation of the computer security requirements. Design information, such as analysis, should be controlled so that it is available in the future to authorized users of the design.

6.19 Design documents may contain sensitive information related to computer security, so all design documents should be classified according to the information classification scheme, and controlled accordingly.

6.20 The operator should place any computer security requirements as a part of the contractual negotiation with suppliers[29].

Construction

6.21 The operator should ensure that physical, administrative and technical security control measures are established during the construction process in order to maintain the preventive and protective measures required by the CSP and DCSA. For example, if lockable doors are to be installed on an enclosure, the locks should be installed, and control over locks established prior to installing SDAs within the enclosure, or appropriate compensatory measures put in place.

6.22 The operator should ensure that computer security activities are performed during the construction stage, including:

— Assurance activities – testing, assessments and audits.

— Use of staging areas – process and security control to verify the SDAs have not been tampered with.

— Management and verification of staff of contractors, vendors and suppliers (both onsite and remote) – from fabrication to installation.

— Supply chain evaluation and management – ensuring the verified procurement process matches expectations and is not tampered with.

Commissioning

6.23 The operator should include the testing of computer security measures in its acceptance testing for the delivery of systems from the system provider to the facility.

6.24 The operator should perform system and DCSA integration (see F) configuration and testing activities to meet computer security requirements. For example:

[29] The ISO/IEC 'common criteria' standard ISO/IEC 15408 [17] is a possible tool to inform potential security requirements.

— Passwords and secondary authentication methods for digital assets should be changed according to approved procedures;

— Development and construction accounts for digital assets should be removed and technical control measures should be enabled.

— System support tools (software/hardware) should be submitted for testing and application of appropriate computer security measures.

6.25 The operator should perform computer security validation testing. Computer security and physical protection validation should be completed jointly to ensure appropriate integration.

6.26 If there is a conflict between safety and security, then design considerations taken to assure safety should be maintained, provided that the operator seeks a compatible solution to meet computer security requirements. Compensatory computer security measures should be implemented to reduce the risk to an acceptable level and be supported by a comprehensive justification and security risk analysis. The implemented measures should not rely solely upon administrative control measures for an extended period. The absence of a security solution should never be accepted.

6.27 Review and approval of programme operational documents and supporting materials (system level) should be completed prior to operation.

Operations

6.28 The operator should appoint an individual, supported by the necessary skilled resources, with the ongoing responsibility for design change, management, maintenance, and operations of the entire CSP.

6.29 The operator should maintain documentation that describes how a computer security measures are implemented, in compliance with the CSP, the DCSA and with any externally imposed requirements.

6.30 The operator should ensure that operations requirements remain appropriate, based on the security level of the device or system being maintained. For example:

— Access restrictions, access control and monitoring may be different for equipment at different security levels.

— Different levels of trustworthiness checks may be required for personnel working on particular systems.

— Duties may be segregated.

6.31 Vulnerability assessment involving actions on the systems may lead to plant or process instability, and should therefore only be considered using test beds, spare systems, during factory acceptance tests or during long planned outages.

Maintenance

6.32 This applies to short-duration maintenance activities that are routinely performed during the operations stage. Considerations for extended maintenance (e.g., refurbishment, replacement of systems, or repair) are contained in the Cessation of Operations, Design and Construction stage.

6.33 The operator should ensure that maintenance activities are performed in a manner consistent with the security level of the digital asset or system being maintained. For example:

- The permitted maintenance activities should be specified.
- The required access should be identified and controlled.
- Maintenance devices may be restricted for use within a specific security zone or security level or to a specific system or digital asset.
- Access restrictions, access control and monitoring may be different for systems and digital assets at different security levels.
- Different levels of trustworthiness checks may be required for personnel working at different security levels.
- Secure maintenance environments may be required for some systems or digital assets.
- Duties may be segregated.

6.34 Systems may be at greater risk during maintenance periods when computer security measures may be removed or disabled to allow for maintenance. Furthermore, there may be additional access vectors available during maintenance – for instance arising from the need to enable remote maintenance interfaces, or the introduction of media to configure or upgrade software components.

6.35 The operator should put adequate compensatory measures in place to address removal of the primary measures. For instance,

- Compensatory measures to provide physical protection when equipment is unlocked.
- The need for remote interfaces should be identified (and justified) prior to maintenance and appropriate computer security measures identified and implemented in accordance with the CSP.
- Computer-based tooling (such as measurement and testing equipment, calibration equipment) should be controlled and monitored to ensure that it is not compromised by cyber-attack and that it does not provide a vector for compromise of systems on which it

is used. Computerized equipment, such as test equipment or equipment used for configuration which may be temporarily connected to the system should be protected against malicious software and unauthorized data transfer. Minimization of use of external equipment for these purposes is recommended. Inspection of externally-provided equipment prior to bringing it into the facility is also recommended.

— Software to be used should be checked to confirm it is free from malicious software prior to loading it on the target system. This may include verification that the software has not been tampered with using cryptographic hashes, or some other method, for example, use of software signing to verify source authenticity.

— Safety controls (e.g., concurrent verification by a second party) may be leveraged for security purposes.

Cessation of operations

6.36 During the cessation of operations stage large scale modifications to multiple systems may be conducted in parallel. This is a very dynamic environment when compared to the operations stage.

6.37 The operator should consider applying compensating measures to address increased risk arising from alterations to or degradation of security systems resulting from environment or structural changes. This may result in a greater reliance on administrative control measures and on contractors, vendors and suppliers.

6.38 Examples of alterations to the facility for which compensating measures may be applied include:

— Computer security architectures and measures may need to be modified or disabled to allow the required work to take place.

— There could be large fluctuations in staffing levels during this stage. This could include large number of new personnel being brought onsite to perform activities involving SDAs. This may require additional trustworthiness evaluations or other mitigation be put into place to address the insider threat.

— Additional measures may be required for secure storage, handling and cleansing of affected SDAs.

— There may be significant replacement of components. This could require the creation of a secure installation environment.

Decommissioning s

6.39 When computer-based systems are decommissioned, the effect of this decommissioning (including the potential integration with other computer-based systems outside the facility) on computer security must be evaluated and documented. If retirement of a system or digital asset diminishes the effectiveness of computer security measures, the operator should put mitigating measures in place.

6.40 As the set of required facility functions changes, the digital assets supporting these functions may be reassigned to a different security level (including unassigned). This may result in the modification of computer security measures for those digital assets.

6.41 The operator should ensure the secure destruction of any digital assets containing sensitive information that cannot be securely declassified when they are decommissioned.

7. ELEMENTS OF THE COMPUTER SECURITY PROGRAMME

COMPUTER SECURITY POLICY AND PROGRAMME REQUIREMENTS

7.1 The computer security policy and programme requirements should be informed by the results of the facility and system CSRM (Sections 4 and 5 respectively) processes and the considerations for the specific stage of the lifetime of the facility (section 6).

7.2 Computer security at nuclear facilities should be recognized by senior leadership and management as a cross-cutting discipline requiring specialized knowledge, expertise and capabilities.

7.3 Senior leadership have overall responsibility for computer security at a nuclear facility, have an awareness and understanding of the cyber threat and the potential adverse effect of a cyber-attack on nuclear security.

7.4 Senior leadership should ensure that the interfaces, interactions and processes addresses all stakeholder requirements (including laws and regulations) related to information and computer security.

7.5 Management should be promulgated the beliefs and values of security culture, as they pertain to computer security. This includes espousing the belief that a credible threat exists from adversaries having cyber skills, and that these adversaries (including insider threats) are targeting nuclear facilities via cyber-attack or blended attack.

Computer security policy

7.6 A computer security policy sets the high level computer security goals and objectives of an organization. A recommended starting point for the computer security policy is to begin with a clear purpose statement which clearly states why the CSP is being established, defines the issue being addressed, the goals of the CSP, and the consequences if the policy is not met.

7.7 The operator should have a computer security policy based upon the results of the facility CSRM (see section 4). The computer security policy should require the protection of SDAs against compromise from cyber-attacks.

7.8 The computer security policy should be endorsed and enforced by the facility's most senior manager, and specifies the overall computer security goals at the facility. Individual policy clauses should be clear and concise in identifying these requirements. Implementation processes will be addressed in procedures as detailed within the CSP. The policy should meet appropriate regulatory requirements.

7.9 The computer security policy should be part of the overall facility security policy and should be coordinated with other relevant security responsibilities. When establishing a computer security policy, its effect on legal and human resources also needs to be considered. The computer security policy should interface with other policies in an integrated and efficient manner.

7.10 The computer security policy may identify potential penalties and disciplinary actions resulting from personnel not complying with the policy requirements.

7.11 Computer security policy should be traceable in the CSP and other lower level CSP elements which will be used to implement policy and manage computer security. Additionally, the policy should be enforceable, achievable, measurable and auditable.

7.12 In order to be measurable, the policy needs to set out clear metrics that will be considered to demonstrate that policies are being met in all aspects and that each aspect is being performed satisfactorily.

7.13 The computer security policy should identify the organization or individual that owns the policy and the CSP.

Computer security programme

7.14 Computer security policy outlines what is to be achieved. The CSP contains details of how these goals and objectives are achieved. The CSP establishes the organizational roles, responsibilities, processes and procedures for implementing the computer security policy. The CSP normally uses layered computer security measures to create a defence in depth security framework. A CSP is normally facility (includes associated buildings or equipment) or organization-specific (includes sites, departments, and sections).

7.15 The CSP should be developed, exercised, and maintained within the framework of the facility's overall security plan.

7.16 The specification of the CSP should be informed by the results of the facility CSRM (section 4). The CSP specification may include personnel involved in computer security, physical protection, safety, operations and IT.

7.17 The CSP should be regularly reviewed and updated to reflect nuclear security events (including computer security incidents).

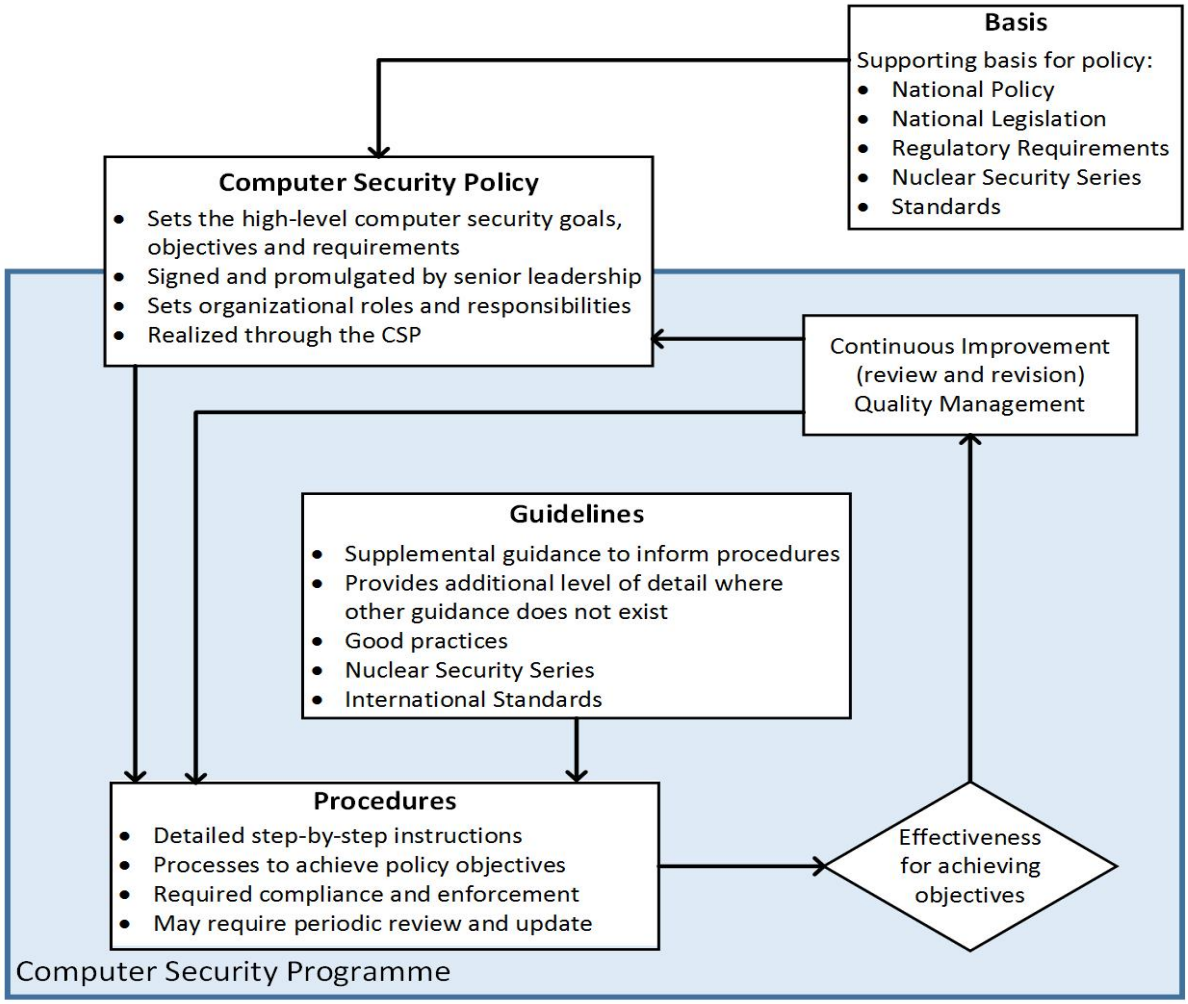

FIG. 8. The computer security programme.

Elements of the computer security programme

7.18 NST045 [10] provides guidance for minimal essential components of a CSP for organizations within the nuclear security. The following provides amplification specific to nuclear facilities.

7.19 The CSP elements should contain details for addressing system vulnerabilities, applying computer security measures, performing risk analysis, conducting assurance activities, to manage risk to a level that is below the threshold of the operator's acceptable computer security risk.

7.20 The CSP elements should be seen as a dynamic set of activities that are adapted and applied during specific stages of the lifetime of a facility as well as individual system life cycles phases. The specifics of implementation should be detailed in the CSP.

7.21 While each facility will customize its own CSP, it is recommended that as a minimum the following areas be included:

(a) Organization and responsibilities:

— Organizational charts;

— Responsible persons and reporting responsibilities (paras A.3–A.13 of the Appendix)
— Periodic review and approval process.
— Interfaces with other programmes (e.g., human resources, personnel related security, physical protection, training) (see paras A.14–A.37 of the Appendix)

(b) Risk, vulnerability, and compliance management
— Facility CSRM (see section 4)
— System CSRM (see section 5); including the process for the classification and identification of SDAs
— Security plan(s) review and reassessment periodicity;
— Self–assessment practices;
— Audit procedures and deficiency tracking and correction;
— method for and occasions to start/repeat risk and vulnerability assessment
— Regulatory and legislative compliance.

(c) Security design and management:
— Fundamental security architecture (i.e. DCSA)
— Fundamental security design approaches (i.e. security levels and zones);
— Baseline computer security measures assignment to each security level;
— Formalization of computer security requirements for contractors, vendors and suppliers, including maintenance contracts;
— Security considerations for the stage in the facility lifetime (see Section 6).

(d) Digital asset[30] management:
— Digital assets attributes (identification, security level, zone, location, associated consequence);
— Configuration management (hardware, firmware, software applications, equipment status, and associated configurations)
— Data flow and network diagrams, identifying all external connections other systems.
— Supplier information for assets

(e) Security procedures:
— Security incident handling;
— Business continuity;`
— System backup, restoration, and recovery.
— Supply chain;

[30] Digital assets include technical control measures that use digital technologies.

— Access control;
— Information and communications management;
— Platform and application security (e.g. hardening);
— System monitoring;

(f) Personnel management:
— Trustworthiness checks (personnel vetting);
— Awareness and training;
— Qualification;
— Termination/transfer.

7.22 The above provides a framework for a CSP and specific elements are detailed in Section 8 (e.g. fundamental security architecture and design approaches) and the Appendix.

7.23 Many references are available to supplement the CSP framework and elements provided in this publication, such as IEC 62645 [18], ISO/IEC 27001 [19] for information security management systems, and ISO/IEC 27002 [20] for guidance on implementing CSP elements.

ORGANIZATIONAL ROLES AND RESPONSIBILITY

7.24 The operator should define computer security authorities, roles and responsibilities within the organization. This is vital to the organization effectiveness in achieving the computer security objectives stated within the computer security policy with the implementation detailed within the CSP.

7.25 Management should ensure that all staff understands who, within the organization, is responsible for leading the CSP at its multiple levels. Likewise, staff needs to understand the processes associated with the CSP.

7.26 Computer security management should be integrated and implemented within the facility's existing management system (see paras 7.33–7.37) to the extent possible and practicable.

7.27 For existing facilities, the management system includes well-defined authorities, roles and responsibilities, and these should be adjusted to incorporate computer security.

7.28 The personnel assigned to significant roles having computer security responsibilities should not have conflicting interests with other functions of the organization or with their other duties. Management should put in place policies and processes that mitigate any potential conflicts.

7.29 The operator should ensure that individuals or organizations performing key assessment and verifications activities are qualified and independent.

7.30 Computer security has strong work-sharing demands, consequently many people in differing roles and organizational units will be involved. The organization should put in place a formalized framework with the aim to ensure inter-disciplinary cooperation.

7.31 The organization need to identify the external and internal interfaces involved in the CSP. This includes (but is not limited to):

- Interface between the facility and relevant competent authorities (regulators, technical support organizations, law enforcement, intelligence agencies and security services).
- Security incident reporting and response.
- Internal interface (incident response team)
- Public relations.
- External providers:
- Supply chain (e.g., electronic procurement)
- Externally provided services (e.g., banking, payroll, cloud-based services)
- Contractor support (e.g., off-site maintenance)

RISK, VULNERABILITY AND COMPLIANCE ASSESSMENT

7.32 The operator should manage risk through a formalized process (i.e. facility and system CSRM) that assesses and manages risk and vulnerabilities at the facility. The operator should use the results of these processes within their management systems.

Management systems

7.33 A management system is responsible for establishing policies and objectives and enabling the objectives to be achieved in an efficient and effective manner. Management systems are a vital support element to a nuclear security culture. Many activities at nuclear facilities are controlled by management systems. These ideally integrate computer security, physical protection, safety, health, environmental, quality and economic elements in a single management tool or a set of integrated and mutually reinforcing systems.

7.34 The management system should have formal and established interfaces with the facility and system CSRM as this is one of the key tools in implementing a sustainable and effective CSP in an operational environment.

7.35 The computer and information security objectives should be defined managed within the management system in a similar manner to other business objectives. For example:

— Develop methodology to identify and estimate and evaluate risk

— Identify risk to the computer and information security objectives and manage that risk

— Establish plans

— Set targets

— Develop metrics to measure the effectiveness of computer and information security

— Establish measures and monitoring to ensure objectives are met

— Adjust and improve as required

7.36 Management systems should be reviewed to ensure completeness and compliance with facility security policies. More generally, management systems are by nature dynamic and must adapt to changing conditions in the facility and in the environment; they cannot be implemented as a one–off measure but need periodic assessment and improvement. Figure 3 of Ref. [21] illustrates the continual improvement cycle for management systems.

7.37 The CSP elements (including the facility and system CSRM) should be reviewed and the necessary provisions for computer security integrated into the management system.

Computer security metrics

7.38 Metrics can be an effective tool for security managers to quantify the maturity of the management system, the cyber risk associated with SDAs and discern the effectiveness of various components of their security programmes, the security of a specific system, product or process, and the ability of staff or departments within an organization to address security issues for which they are responsible.

7.39 Metrics should support senior decision-makers with regards to acceptable risk and inform a risk registry.

7.40 An analysis should be performed to identify parameters and establish metrics that allow for effective management of the CSP. Potential metrics that may be beneficial are mean time to recover (from cyber-attack), number of computer security incidents, number of restoration of SDAs (potential reoccurrences), security backlogs, and vulnerability tracking (common scoring system, mitigation effectiveness, control deployment time, patch deployment).

7.41 The metrics should be integrated and their use established within the organization’s management system.

7.42 The ability to measure or check the effectiveness of computer security measures is an integral part of process improvement. Organizations are encouraged to identify and track meaningful metrics

that will provide timely indication of the effectiveness of computer security measures. Metrics may be created for example for threat, vulnerability, risk, and effectiveness of computer security measures.

SECURITY DESIGN AND MANAGEMENT

7.43 Facility and system security design is specified and managed by the facility and system CSRM (see Sections 4 and 5 respectively) processes. One practical implementation of these outputs is detailed in section 8 (i.e. DCSA and measures assigned to security levels).

Computer security requirements

7.44 Facility or system modifications should be analysed to determine potential effects on security prior to change implementation to allow for risks to be managed.

7.45 Computer security should be considered as a factor when determining the design inputs, which include, but are not limited to:

- Functional requirements,
- Interface requirements
- Operational requirements
- Location of equipment
- Environmental considerations,
- Codes and standards to be used
- Contractual considerations
- Supply chain considerations
- Logistics (e.g., coordination of complex operation involving many people, facilities or supplies).
- Past operating experience;
- Introduction of new technologies[31]
- Human factors considerations
- Design requirements for each engineering discipline (including computer security).
- Fabrication considerations
- Installation

[31] New technologies refer to those technologies that have yet to be implemented or operated by the operator.

— Commissioning

— Decommissioning

— Economic considerations.

DIGITAL ASSET MANAGEMENT

7.46 The operator should for each digital asset, document attributes that have significance for computer security. These attributes may include, but are not limited to:

— Functions/tasks and operational modes;

— Identification of relevant interconnections, including power supplies;

— Dataflow analysis, including internal and external connections.

— Procedures that initiate communication, frequency of communication and protocols;

— Asset identifier and location;

— Asset configuration

— Analysis of user groups;

— Ownership (for data and computerized systems);

— Corresponding security level and zone, and associated consequences.

7.47 Digital asset management should take into account the equipment status of technical control measures that use digital technology. Computer security operations and physical protection operations may have joint responsibility for integrated security measures, systems, and procedures. Joint operational control includes control over physical security devices used to protect computer equipment (e.g., rooms, doors, keys, locks, cameras, motion sensors, tamper systems)

Configuration management

7.48 The goal of configuration management is to have detailed up-to-date records of the installed software and hardware components and how they are configured. Configuration management should include considerations required for:

— Identifying the need for computer security measures

— Verifying that the computer security measures are implemented and configured correctly

— Managing changes throughout the lifecycle of the systems and

— Supporting computer security assessments

— Providing traceability to understand the reason or purposes of changes to the computer security measures.

Therefore, configuration management is one of the cornerstones for computer security.

7.49 Configuration management includes the change management process. Computer security should be included into this process in a way that all changes are also evaluated from computer security point of view before implementation. For instance, this could prevent changes that bypass or diminish the implemented computer security measures. This is generally seen as a technical issue but it is good to keep in mind that personnel changes may require some computer changes, i.e. credential cancellation and management.

7.50 Configuration management should be implemented to ensure that changes to the security posture of computers and the organization's security architecture are performed in a manner that does not adversely affect the organization's computer security posture.

SECURITY PROCEDURES

7.51 The operator should develop security procedures to support facility and system computer security design and management.

7.52 Facility procedures should be developed or modified to address the computer security concerns. For example, maintenance instructions that provide details on how to disable the computer security measures required to allow for the performance of a particular task. The procedure may also provide instructions for the application of alternate or compensatory computer security measures when the baseline computer security measure is disabled.

7.53 These procedures may be new standalone procedures, or integrated within existing procedures that meet one or more safety, security, or organizational objectives.

PERSONNEL MANAGEMENT

7.54 Personnel management includes the necessary provisions for establishing an appropriate level of trustworthiness, confidentiality undertakings, and termination procedures and for defining required job competencies.

7.55 Computer security and personnel related security activities should be coordinated to provide protection against insider threats. In particular, staff with key security responsibilities (system administrators, security team) may require a higher level of trustworthiness.

7.56 The CSP should include training and awareness processes for personnel management to develop and maintain personnel and organizational competencies and qualifications that are necessary for computer security.

7.57 Personnel management provides protection from insider threats. For guidance on the protection from insider threats, see Ref. [6].

8. POTENTIAL DCSA AND COMPUTER SECURITY MEASURES

8.1 Implementation of DCSA having five different security levels is presented below. This is just one possible implementation of the graded approach; the exact choice of levels, DCSA, and their constitutive security measures should be tailored according to the considered environment, the facility specificities, and the dedicated security risk analysis.

POTENTIAL DCSA IMPLEMENTATION

8.2 When implementing the DCSA, the operator should consider limiting the dynamic elements of both the composite networks and their individual systems to increase the determinacy of their behaviour. This increase in determinacy may assist the implementation of effective computer security measures for detection of potential computer security incidents.

8.3 Zones requiring the highest level of security (i.e. most stringent security level) should only be connected to zones requiring lower levels of security (i.e. weaker security levels) via fail-secure, deterministic, unidirectional data communication pathways[32]. The direction of these data pathways should be limited to transmission of data from the most stringent security level to the devices in the weaker security levels. Exceptions are strongly discouraged and may only be considered on a strict case by case basis and if supported by a complete justification and security risk analysis[33].

8.4 Digital devices or communications used for monitoring, maintenance and recovery activities should not bypass technical control measures used to protect communication pathways between devices having different security levels.

8.5 Systems assigned to the most stringent security level should be placed within the most secure zones boundaries[34].

8.6 Data communications between systems within the facility and the emergency centre (either onsite or offsite) should be protected and controlled by computer security measures.

[32] Remote access to the systems in the most stringent security level unable to be implemented due to the uni-directional limitation of outbound traffic from the I&C system.

[33] Some Member States do not permit exceptions in any case.

[34] Wireless communications functions are problematic when implemented in I&C systems that are assigned to the most stringent security level as it is difficult to provide a secure boundary for such communications.

DECOUPLING BETWEEN ZONES

8.7 Computer security measures that ensure the logical and physical decoupling of zones are based upon to the requirements of the zones' security levels. Additionally, in order to maintain defence in depth, a direct path connecting through several zones should not be allowed.

8.8 Technical control measures that provide security at the boundaries of zones should be designed to be resilient to cyber-attack and to provide indications or alerts of potential compromise or malicious activity.

External connectivity

8.9 Where external connectivity is provided, security should be applied based on the graded approach. The provision of external connectivity should meet the requirements for confidentiality, integrity and availability consistent with the security level assigned to the zone.

8.10 Appropriate access restrictions (including monitoring of access) should be implemented to provide protection based upon the graded approach because these external connections can serve as a vector for compromise.

8.11 Examples of externally accessible systems could include:

- Environmental monitoring systems; building automation systems
- Fire protection systems
- Communications with emergency centres
- Remote vendor access where authorized
- Field devices located outside of the physical security perimeter.
- Visitor control

8.12 Fig. 9 shows an illustrative example of one implementation of a DCSA showing levels, zones, systems, and digital assets. This is based upon the DCSA shown in Section 2.

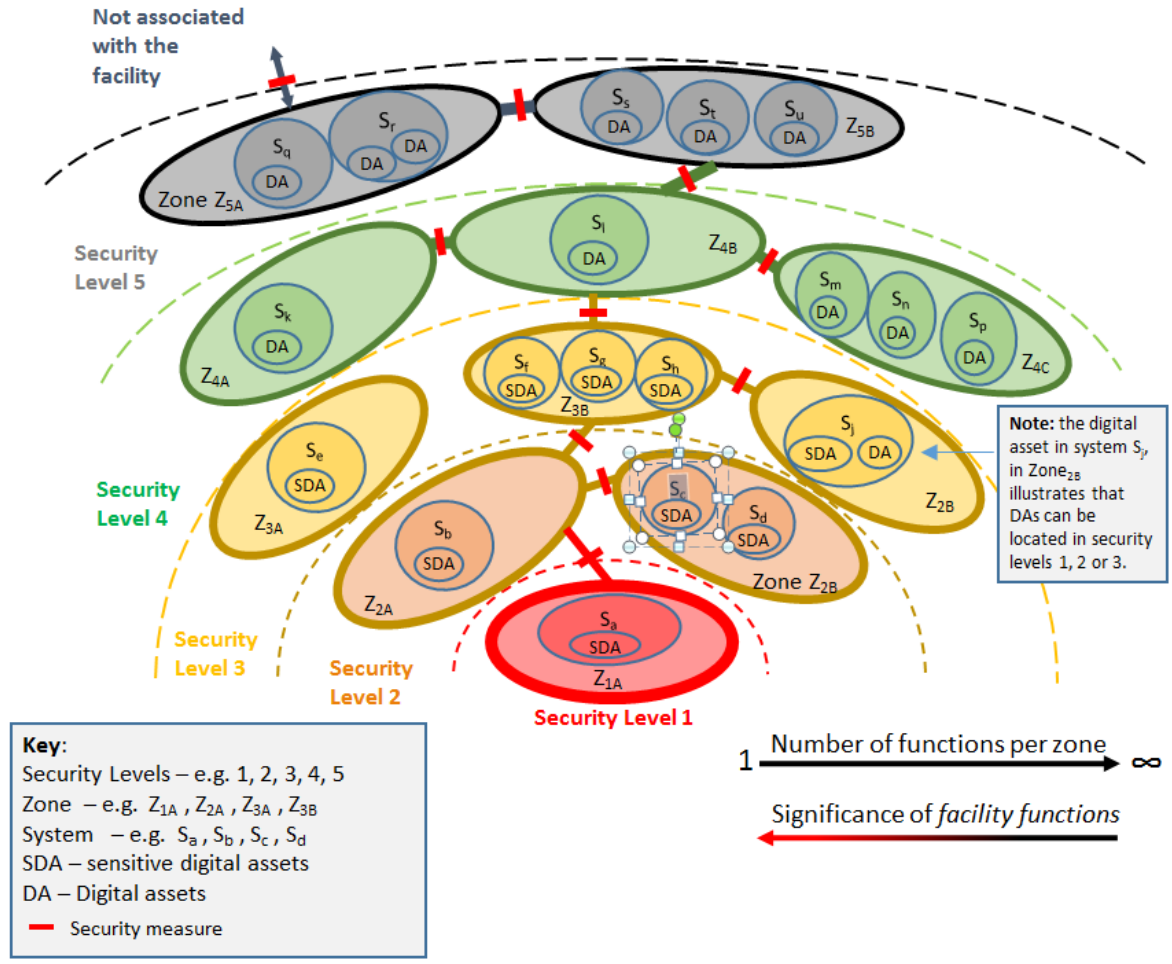

FIG. 9. Illustrative example of implementation of DCSA.

POTENTIAL MEASURES

8.13 Implementation of security measures applied within each security level is presented below. This is just one possible implementation of the graded approach; the exact choice of levels and their constitutive security measures should be tailored according to the considered environment, the facility specificities, and the dedicated security risk analysis.

UNASSIGNED DIGITAL ASSETS

8.14 Unassigned digital assets are digital assets that do not have an assigned security level. This includes devices which are not owned by the operator (including employees' personal mobile devices).

8.15 Unassigned digital assets may be encountered from either of the following ways:

— Restricted or proscribed equipment. There are restrictions placed upon the operator where the operator is unable to assess the security of the digital assets. This may be the

result due to licence, contractual, regulatory, or national law that prohibits the operator from inspecting and modifying the equipment (e.g. safeguards).

— Unannounced equipment. The equipment may be brought to the facility by a private individual or external party in the absence of a previous announcement. In these cases, the equipment is considered contraband until a proper computer security risk assessment can be completed.

8.16 The facility may place restrictions upon unassigned assets until they can be assessed, assigned to the appropriate security level and the required computer security measures put in place. Devices that are unassigned, for instance, may not be brought into proximity of systems having medium to very high security levels.

GENERIC LEVEL

8.17 For applicable systems and levels, the following generic measures should be applied:

— All IT-technical, physical, personnel and organizational security measures for systems and networks should be planned and implemented in a systematic manner and under the direction of approved processes and procedures.

— Measures are designed and operated in consideration of insider threats.

— Policies and practices are defined for each level.

— It is ensured that users are obliged to comply to security policies and security operating procedures.

— Staff permitted access to the system must be suitably qualified and experienced and security cleared where necessary.

— Users and administrators are given access only to those functions on those systems that they require for carrying out their jobs. An accumulation of access rights for individual person must be avoided.

— The system’s functionality and interfaces are limited to the extent possible with the objective of reducing overall system vulnerability (i.e. attack vectors, attack surface).

— Appropriate access control and user authentication are in place.

— Protection against infection and spreading of malware is in place.

— Security logging and monitoring including procedures for adequate response are in place.

— Application and system vulnerabilities are monitored, and appropriate measures are taken.

— The adequacy and effectiveness of measures is reviewed periodically.

— System vulnerability assessments are undertaken periodically.

— Removable media must be controlled in accordance with security operating procedures. It is not allowed to connect privately owned devices to systems and networks.

— Computer and network security components should be strictly maintained using change management procedures.

— Appropriate backup/recovery procedures are in place.

— A service device is assigned to exactly one security level.

— Physical access to components and systems including services devices is restricted according to their functions.

— Measures to prevent unauthorized introduction of systems into security zones are in place.

— Only approved and qualified users are allowed to make modifications to the systems.

LEVEL 1 BASELINE MEASURES

8.18 In addition to the generic measures, level preventive and protective measures must be used for systems which are vital to the facility and require the highest level of security (e.g. protection systems). These measures may include the following:

— Systems must be designed and implemented to be verifiable and testable against a potential misuse by an adversary.

— No networked data flow of any kind (e.g. acknowledgment, signalization) from systems in weaker security levels should be authorized to enter level 1 systems. Only strictly outward communication should be possible. Exceptions are strongly discouraged and may only be considered on a strict case by case basis and if supported by a complete justification and security risk analysis.[35]

— No remote maintenance access is allowed.

— Physical and logical access to systems is strictly controlled, monitored and recorded.

— The number of staff given access to the systems is limited to an absolute minimum.

[35] Some Member States do not permit exceptions in any case.

— The two-person rule is applied to prevent unauthorized actions by an insider threat (e.g. modifications to computer systems).

— All activities must be logged and monitored.

— Connecting external storage devices is approved and verified on a case by case basis.

— Strict organizational and administrative procedures apply to any modifications, including hardware maintenance, updates and software modifications.

LEVEL 2 BASELINE MEASURES

8.19 In addition to the generic measures, level 2 preventive and protective measures should be used for systems, e.g. operational control systems, which require a high level of security. These measures may include the following:

— Only an outward, one way networked flow of data is allowed from level 2 to level 3 systems. Only necessary acknowledgment messages or controlled signal messages can be accepted in the opposite (inward) direction (e.g. for TCP/IP).

— Remote maintenance is not allowed.

— The number of staff given access to the systems is kept to a minimum, with a precise distinction between users and administrative staff.

— Physical and logical access to systems is strictly controlled and documented.

— Administrative access from other security levels should be avoided. If this is not possible, it must be strictly controlled, e.g. by adopting the two-person rule and two factor authentication.

— All reasonable measures to ensure the integrity and availability of the systems have been taken.

LEVEL 3 BASELINE MEASURES

8.20 In addition to the generic measures, level 3 preventive and protective measures should be used for supervision real time systems not required for operations, e.g. process real time supervision systems in a control room, which have a medium severity level for various cyber threats. These preventive and protective measures may include the following:

— Access to the Internet from level 3 systems is not allowed.

— Logging and audit trails for key resources are monitored.

— Security gateways are implemented to protect this level from uncontrolled traffic from level 4 systems, and to allow only specific and limited activity.

— Physical connections to systems should be controlled.

— Physical and logical access to systems is controlled and documented.

— Remote maintenance access is allowed on a case by case basis provided that it is robustly controlled; the remote computer and user must respect a defined security policy, contractually specified.

— System functions available to users are controlled by access control mechanisms, and based on the 'need to know' rule. Any exception to this rule has to be carefully studied and protection should be ensured by other means (e.g. physical access).

— Administrative access from other security levels should be avoided. If this is not possible, it must be strictly controlled, e.g. two factor authentication.

LEVEL 4 BASELINE MEASURES

8.21 In addition to the generic measures, level 4 measures should be used for technical data management systems used for maintenance or operation activity management related to components or systems required by the technical specification for operation (e.g. work permit, work order, tag out, documentation management), which have medium severity level for various cyber threats. Level 4 measures include the following:

— Access to the Internet from level 4 systems is not allowed.

— Security gateways are implemented to protect this level from unauthorized data communications from trusted and approved external company or facility networks, and to allow specific activities that are authorized.

— Physical connections to systems should be controlled.

— Remote maintenance access is allowed and controlled; the remote computer and user must respect a defined security policy, contractually specified and controlled.

— System functions available to users are controlled by access control mechanisms. Any exception to this rule has to be carefully studied and protection should be ensured by other means.

— Remote external access is allowed to selected services and for approved users provided that appropriate access control mechanisms are in place.

LEVEL 5 BASELINE MEASURES

8.22 Level 5 measures should be used for systems not directly important to technical control or operational purposes, e.g. office automation systems, which have low severity level for various cyber threats. Level 5 measures include the following:

— The minimum security level must not fall below a baseline protection level according the latest state of the art.

— Only approved and qualified users are allowed to make modifications to the systems.

— Access to the Internet from level 5 systems is allowed provided adequate preventive and protective measures are applied. –Remote external access is allowed for authorized users provided that appropriate measures are in place.

— Physical connections of third party devices to systems and networks must be regulated and technically controlled. Those interfaces to higher level systems must be characterized and evaluated independently to ensure compliance with the computer security architecture.

APPENDIX

SELECTED ELEMENTS OF A COMPUTER SECURITY PROGRAMME

A.1. Examples of selected CSP elements for use with the performance based approach are provided in this Appendix. An operator may need to modify these elements to reflect its own particular circumstances, but the examples contain all of the information that the operator needs in order to perform and validate these computer security activities of nuclear facilities.

A.2. Operators should require these elements or elements similar to this to facilitate understanding between organizational departments, contractors, vendors, suppliers, and regulators, both domestically and internationally

FACILITY ORGANIZATION AND RESPONSIBILITIES

Management

A.3. A facility's senior leadership initiates computer security by establishing a computer security policy along with adequate process and support organizations. To achieve this, the management should:

- Assume overall responsibility for all aspects of computer security;
- Define the facility's security objectives;
- Ensure compliance with laws and regulations;
- Maintain awareness of the current nuclear security threat and associated attack trends;
- Set the risk acceptance level for the facility;
- Assign organizational computer security responsibilities;
- Ensure adequate communication between different aspects of security;
- Ensure an enforceable computer security policy is established;
- Provide adequate resources to implement a viable CSP;
- Ensure periodic audits and updates of computer security policy and procedures; and
- Ensure support for training and awareness programmes.

Computer security specialist

A.4. The operator should assign overarching computer security oversight to one well defined role or body. In this publication, the title computer security specialist is used to define that role.[36]

A.5. The computer security specialist role should be closely coordinated across the facility, but in an independent manner. Additionally, to be effective, this role should have clear and accessible reporting lines to senior management as computer security touches almost all facility activities.

A.6. Computer security responsibilities within different organizational departments, individual responsibilities should be clearly defined to prevent conflict and to ensure that oversight is implemented in a cohesive manner. This is especially true where the computer security specialist role is assigned to multiple officers. Ideally, one single authority within the operator is designated as responsible for addressing organizational wide issues and resolving conflicts when they arise.

A.7. The computer security specialist should have in–depth knowledge of computer security and good knowledge of other aspects of security in nuclear facilities. Further requirements are knowledge of nuclear safety and project management, and the ability to integrate people coming from different disciplines into an efficient team.

A.8. The computer security specialist should have the authority and responsibility for administering the CSP.

A.9. The typical responsibilities of the computer security specialist include:

— Advising the senior leadership on computer security.

— Leading the computer security team.

— Advocating for improving computer security within the organization.

— Coordinating and controlling the development of computer security activities (e.g. implementing security policy, directives, procedures, guidelines, measures).

— Coordinating with physical protection and other security and safety disciplines to specify and plan security measures and response to security incidents.

— Identifying systems critical to computer security within a facility (i.e. the computer security baseline). Asset owners should be informed of their equipment’s role in computer security.

[36] In other instances, this function may be referred to as “Computer Security Officer (CSO)” or Chief Information Security Officer” or “IT Security Officer” or “Information Security Officer”, or may be assigned to multiple roles.

— Conducting periodic computer security risk assessments, ensuring independence from the implementing groups including operational staff.

— Conducting periodic inspections, audits and reviews of the computer security baseline and providing status reports to top management.

— Developing and implementing computer security training and evaluation.

— Developing and leading computer security incident response, including coordination with relevant internal and external organizations.

— Investigating computer security incidents and developing post–incident procedures and preventive actions.

— Participating in facility security assessment initiatives.

— Participating in requirement analysis in the acquisition/development of new systems.

Computer security team

A.10. The operator should identify and assign personnel to a computer security team. This team may be a dedicated team or ad hoc access to specific expertise within the organization. The goal of this team is to support the computer security specialist in fulfilling their responsibilities. This is vital to both proactive and reactive CSP components and encompasses all stakeholder activities. It is essential for the computer security specialist to have access to adequate interdisciplinary expertise associated with computer security, facility safety, and plant operations as well as physical protection and personnel related security.

A.11. Members of the team should be responsible for bringing the security aspects into their respective functional units.

Other management responsibilities

A.12. The various levels of management within an organization should ensure the appropriate level of computer security within their areas of responsibility. Typical responsibilities include:

— Understanding the significance and the role of computer security in nuclear security;

— Operating within the guidance of the CSP;

— Providing operational requirements and feedback to senior management relevant to computer security and resolving potential conflicts between operational, security, and safety requirements;

— Notifying senior management of any conditions that may lead to changes in the computer security posture, such as personnel changes, equipment changes, or process changes;

— Ensuring that staff are sufficiently trained and briefed on computer security issues relevant to their roles;

— Ensuring that subcontractors and vendors working for the contracting unit operate within the context of the CSP;

— Tracking, monitoring, responding to and reporting computer security incidents; and

— Enforcing computer security measures.

Individual responsibilities

A.13. Each person within an organization should be responsible for carrying out the CSP. Specific responsibilities include:

— Understanding the significance and the role of computer security in nuclear security;

— Understanding company policy for computer security;

— Knowledge of job specific computer security procedures;

— Operating within the parameters of the computer security policies;

— Notifying management of any changes that may lead to a reduced computer security posture;

— Notifying relevant points of contact and management of any incidents or possible incidents involving a compromise of computer security;

— Attending initial and refresher security training on a regular basis.

Cross department responsibilities

A.14. Computer security is a cross cutting discipline that touches many different departments and activities within an organization. Computer security demands close interface and coordination between multiple functional departments to be effective. The following paragraphs discuss some of the departmental responsibilities and cross cutting issues.

Physical protection

A.15. The site security plan and the CSP are both essential in developing a comprehensive security plan for the facility, and thus both need to complement each other. SDAs have physical access control requirements and likewise, electronic compromise can lead to degradation or loss of certain physical protection functions. Attack scenarios may well include the coordination of both cyber and physical attack.

A.16. The organization(s) responsible for the site security plan and the CSP should inform each other and coordinate their efforts to ensure consistency of plans during the development and review process.

A.17. The operator should recognize that physical protection personnel have important roles and responsibilities in the development, implementation and maintenance of the CSP. This includes:

- Ensuring only authorized access to SDAs is permitted.
- Identifying contraband removable media and mobile devices entering the facility
- Identifying unauthorized removal of information or assets from the facility
- Ensuring that policies applicable to removable media and mobile devices entering the facility are applied (e.g., scanning for malicious software prior to entry into the facility).
- Reporting computer security incidents (e.g., detection of malicious software, unauthorized removal of information assets) according to the incident response procedure.
- Assessment of secure information management practices (e.g., desk checks, checking locked rooms and cabinets, providing standards for devices providing physical protection of information assets, access control and monitoring).
- Supporting incident response activities that involve computer security incidents related to PPS

Information technology (IT)

A.18. IT personnel perform support, management, and administrative processes within the nuclear facility. These processes may include, but not limited to, activities involving digital assets which are used to prepare and store operational and maintenance procedures, work instructions, configuration management systems, design documents, and operating manuals.

A.19. The CSP should clearly identify the digital assets and their associated networks that are the responsibility of the IT personnel. IT personnel should monitor the identified digital assets and their associated networks and report computer security incidents to senior management and the computer security specialist according to the incident response plan to ensure a coordinated response.

A.20. IT personnel should take actions to ensure that computer security incidents on IT systems (not containing SDAs) and networks do not propagate to systems containing SDAs (i.e. nuclear safety, nuclear security, nuclear material accountancy and control).

Engineering

A.21. Engineering personnel should have formalized interfaces and processes to ensure that other stakeholder organizations are engaged to ensure that considerations for security and safety are designed and implemented in an integrated manner consistent with the requirements detailed within the CSP. Engineering personnel should recognize that safety, physical protection, and computer security are distinct domains that require support from experts in different disciplines.

A.22. Engineering personnel should provide evidence that the effectiveness of the computer security architecture (i.e. DCSA) is maintained consistent with the results of the facility and system CSRM. Engineering personnel have a responsibility in implementing computer security measures with respect to the DCSA.

A.23. Engineering personnel should support or lead the performance of the system CSRM for specific facility systems for which they are the owner.

A.24. Engineering personnel should provide direction to contractors, vendors and suppliers regarding requirements for computer security within facility systems. Engineering personnel are responsible for reviewing vendor designs to ensure that they meet the security requirements. Engineering personnel should seek confidence that the delivered product has been developed in a secure environment. Engineering personnel should establish and use a procedure for reviewing the technical product documentation, onsite product consignment acceptation, and product testing to ensure computer security requirements are met.

A.25. Engineering personnel should ensure that performance monitoring activities are put in place to confirm that computer security measures are not degraded and continue to be effective.

Operations

A.26. The CSP should clearly identify the facility systems and networks that are the responsibility of the operations personnel. Operations personnel are responsible for complying with the requirements for these systems according to the CSP.

A.27. Operations personnel should ensure that DCSA and computer security measures under their responsibility are maintained and remain effective.

A.28. Operations personnel should ensure that procedures are in place for identification of computer security incidents and to initiate response to potential computer security incidents for systems and networks under their responsibility.

A.29. Operations personnel should promote situational awareness to ensure that only authorized removable media and mobile devices are used within the operating environment.

Procurement/supply chain organization

A.30. The procurement process is based upon the specification of the equipment, device, or component. This specification includes computer security requirements.

A.31. Procurement processes should ensure that SDAs developed by vendors within the procurement supply chain contain the appropriate computer security measures commensurate with the digital asset's assigned security level.

A.32. Procurement personnel should be made aware of and understand the importance of specific computer security requirements in the procurement arrangements of the equipment. These arrangements should be made through legal agreements such as a licence or contract and should include appropriate computer security requirements.

A.33. Procurement and engineering personnel may not know that a device will be classified as an SDA if the operator keeps a number of general purpose devices on site. Under these circumstances the device should be procured taking into account the possibility that it may be deployed as an SDA.

A.34. Procurement personnel should work with engineering personnel to ensure that computer security requirements are translated into contractual requirements for contractors, vendors or supplier and to ensure that design submittals from contractors vendors or suppliers meet the security requirements. Procurement personnel should also contact engineering personnel when support for the SDA is no longer available from the developer/vendor.

A.35. Procurement personnel should consider conducting reviews of contractors, vendors or suppliers prior to entering into contractual agreements. This review may include analysis of supplier processes used to design, develop, test, implement and support SDAs, or assessment of supplier training and experience in developing SDAs with the required security capability. This review may also help determine whether primary suppliers have in place security measures to properly evaluate the trustworthiness of subordinate suppliers and ensure traceability/provenance of SDAs, SDA components and/or software and updates to the organization.

A.36. Procurement personnel should ensure that all contractors, vendors or suppliers of SDAs have programmes in place to notify the organization in case of supply chain incidents with the potential to affect SDAs (for example, compromises involving SDA components, SDA technology, development processes, sensitive information).

A.37. Procurement personnel should consider ensuring that contractors, vendors or suppliers of SDAs establish or have a trusted distribution path for delivering SDAs, SDA components and/or software and updates to the organization.

External relationships and interfaces for risk management

A.38. Risk management processes should include analysis of external relationships (with contractors, vendors and suppliers) and interfaces. Risk treatment and management should be specified in contractual arrangements. The CSP should ensure that assignment of accountability and responsibility is clearly defined within the contracts.

A.39. The operator should perform audits and other oversight and inspection activities of the external entity to ensure computer security requirements of the CSP are being met, and contractually obligate the external entity to allow the performance of these activities by the operator.

A.40. The operator risk management processes should be informed by regulatory requirements and other external requirements affecting computer security. The operator should address the need for the competent authority to perform oversight activities and inspections when performing and documenting tasks that are put in place to meet these requirements.

Computer security assurance activities

A.41. Computer security assurance activities should be conducted throughout the lifetime of the facility as described in Section 4 and 5. The specific assurance activities will vary depending upon the lifetime stage. NST036 [9] provides details of life cycle assurance activities applicable to I&C systems.

A.42. The types of computer security assurance activities that an operator may employ are assessments (including audits) and reviews, exercises[37] and testing.

A.43. The operator should perform assurance activities provide verification that the CSP meets the computer security policy (i.e. objectives). For example, the goal of computer security assessment is to ensure that computer security requirements as detailed in the organization's policy are met. This can be accomplished through the performance of multiple complementary assessments that evaluate programme elements and their implementation. The outputs of the assessment activity will include, identification of programmatic deficiencies and best practices, and suggestions for improvements.

A.44. These activities should form the basis of a continuous improvement process for the CSP. To support this, assurance activities require the development of repeatable and effective processes which should be conducted on a periodic basis, whenever a computer security incident occurs or when the threat changes.

[37] Exercises and testing also have significance to other CSP elements such as security procedures and personnel management.

A.45. Assurance activities should include the evaluation of the organizational effectiveness and the computer security measures in place to ensure correct implementation and effectiveness.

A.46. Assurance activities may be performed by both internal and external organizations. Internal organizations need to be able to verify the results of activities performed by external organizations. For example, computer security assessment may be performed by an internal team as a self-assurance activity.

A.47. Assurance activities involving additional independent evaluations should be performed by external parties are also recommended as to ensure that the computer security management system has been implemented effectively. Independent assessors will require access to workers, documents and the work. The independent assessor may be internal or external to the organization, however, they must be independent: they cannot be the person who performed, verified or supervised the work being assessed.

A.48. The trustworthiness of independent or external assessors should to be determined prior to their being permitted access this information, as computer security assurance activities likely require access to sensitive computer security information For further information on trustworthiness evaluations and checks, see Ref. [6].

A.49. The independent assessment process should include appropriate restrictions on removal, use, storage, and distribution of sensitive information, and should provide for destruction of that information when no longer needed.

A.50. The capabilities required to conduct assurance activities should be developed and maintained to keep pace with changing technologies, and the dynamic aspects of the cyber threat. This applies to the facility staff who is performing the assurance activities, and to the competent authority who may review the results of these activities.

Assessment scope

A.51. To ensure an effective review, the operator should identify the scope of the review in terms of the functional domains and the security domains.

A.52. The selected scope should be appropriate to the stage of the lifetime of the facility. For instance, during some stages a complete assessment of computer security may be required, whereas in other stages, assessment of specific functional domains or security domains may be more appropriate (NST036 [9] identifies assessment activities at various points in the I&C system lifecycle).

Assessment evaluation techniques

A.53. An assessment team should use all or some of the following techniques to acquire the information they need to develop their conclusions and recommendations:

— Review of documents and records, e.g. legislation, regulations, facility.

— Interviews with personnel from the relevant organizations such as competent authority personnel, facility operators and representatives of other organizations.

— Direct observation of the organization, its practices and systems, and the implementation of computer security measures.

Assessment report development

A.54. During the review of field notes, the operator should identify observations that can be linked to findings. The grouping of similar observations together to indicate trends or reoccurring instances may assist in this determination. The data collection component of the assessment consists of recording the observations of data of interest found during the document/record review, interviews and direct observations. Observations are individually significant, but may also act as a collective indicator of trends at the facility or organization that may need to be addressed.

A.55. The observations should then analysed against requirements such as national regulations, organizational procedures and/or international standards as appropriate. A finding is determined if there is noncompliance with or variance from a regulatory or internal procedure. The basis used for finding determination needs to be well defined and agreed in the preliminary planning meetings.

A.56. Good practices may be identified and reported as potential tactics for other similar organizations to improve their own security programmes. Observations do not always result in findings and not all findings are adverse. One additional outcome is the identification of ‘good practice’, i.e. an organizational process or procedure that provides a novel and effective method for meeting security objectives.

A.57. In addition to findings and good practice, the assessment team may also provide recommendations and suggestions in the report associated with the findings.

A.58. Recommendations provide conformance guidelines for legal and regulatory requirements (national laws/regulations) and/or international norms when appropriate. Recommendations do not normally provide information on how to correct a problem, only that a problem needs to be corrected.

A.59. Suggestions provide an additional level of information regarding a finding, including corrective or mitigation strategies. Such information is not necessarily derived from regulatory guidance, but rather from technical standards and industry good practice.

Example assessment method

A.60. The example method provides in a cross-domain examination of the facility’s functional operations and its computer security. This assists in ensuring coverage of processes and systems that

perform primary functions, including operations, business, safety, security, and emergency response. An example method is provided in Ref. [22].

DIGITAL ASSET MANAGEMENT

Configuration management plan

A.61. A configuration management plan should be developed, documented, and implemented by the operator for SDAs that

- Addresses roles, responsibilities, and configuration management processes and procedures;
- Defines the configuration items and interfaces for SDAs;
- Identifies at what time in the system development life cycle the configuration items are placed under configuration management; and
- Establishes the means for identifying configuration items and a process for managing the configuration items.
- Computer security measures which protect SDAs should be managed under a configuration management plan.

Baseline configuration

A.62. A current baseline configuration of the SDAs should be developed, documented, and maintained under configuration control. The baseline configuration should consider system hardening, effect of modifications on security, and system performance monitoring.

System hardening

A.63. The operator should consider putting in place a systematic process for system hardening of SDAs. System hardening consists of a combination of administrative and technical control measures designed to make computer system components less vulnerable to cyber-attack by removing and disabling hardware and software components that are not required for the operation and maintenance. The hardware and software removed and/or disabled includes, but is not limited to:

- Unused network interfaces or protocols (including disabling of driver software)
- Unused peripherals (including disabling of driver software)
- Removable media support
- Wired and wireless blocking with appropriate authorization
- Peer-to-peer messaging services

- Social media services and applications
- Servers or clients for unused services
- Software compilers in user workstations and servers except for development workstations and servers
- Software compilers for languages that are not used in the control system
- Unused networking and communications protocols
- Unused administrative utilities, diagnostics, network management, and system management functions
- Backups of files, databases, and programs used during system development
- Unused data and configuration files
- Sample programs and scripts
- Unused document processing utilities
- Games

A.64. The system hardening process should be mandatory for SDAs that use commercial off the shelf components. In such cases, the aim is to limit the functionality of the component to that required to perform its facility functions (or system functions). Additional functionality and services could be a path for compromise.

A.65. System hardening methods should have the aim to reduce the data to be monitored and analysed in order to determine the security posture of the protected digital asset or system. In addition, system hardening methods facilitate the plant operator's ability to identify normal behaviour and functionality within the system.

A.66. System hardening may include the use of application whitelisting technology to ensure that only the approved versions of authorized computer programs are allowed to run on the SDA.

A.67. System hardening methods should use only secure, trusted update mechanisms. These update mechanisms should be assessed to ensure they eliminate or minimize potential attack vectors to the system being updated. For example, limiting system updates to those updates that are cryptographically signed by authorized vendors.

Considerations on software updates

A.68. Computer vendors issue computer security updates to address vulnerabilities identified in their systems. Since modification to safety systems requires exhaustive (time-consuming) engineering

processes to be performed, the installation of the patch may not be possible in a timely manner, leaving the system at risk for an extended period of time.

A.69. The operator should have a formal process in place to ensure that computer security updates to equipment and components are identified for applicability and assessed.

A.70. The operator should assess the computer security update (e.g. patch) to determine if it is required for installation to mitigate the associated vulnerability. If required, the operator should install the update or provide for effective compensatory measures that are accepted as being appropriate to protect against exploit of the vulnerability.

A.71. The operator should identify and implement computer security measures within its processes and architecture to allow for assessment of the vulnerability in a timely manner with the aim to ensure that the vulnerability cannot be exploited during the period required to assess and install the patch. For example, system hardening may reduce the number of security updates that are necessary for assessment and installation.

SECURITY PROCEDURES

System monitoring

A.72. All systems covered by the CSP should be assigned an owner (for instance a system engineer) who is responsible for system monitoring.

A.73. System monitoring activities should include monitoring of status and effectiveness of computer security measures.

A.74. The system owner should be responsible for ensuring that recovery media and configuration information is up-to-date and that system recovery plans exist and can be executed (for instance through regular exercise of the recovery plan).

Configuration change control

A.75. Configuration-controlled changes to the SDA should be approved with explicit consideration for security consequence analyses.

A.76. Approved configuration-controlled changes to the SDA should be documented.

A.77. Records of configuration-controlled changes to the SDA should be retained and reviewed.

A.78. Activities associated with configuration-controlled changes to the SDA should be audited.

A.79. Oversight of configuration change control activities should be performed and coordinated.

Computer security exercises (including drills)

A.80. The effectiveness of a CSP is only seen in the practice of its actual execution. An important and continuous activity is the evaluation of CSP components through exercises. This corresponds to the ‘check’ in the ’plan, do, check, act’ model for continuous improvement.

A.81. Physical protection exercises are a common method for both assessment and training. The same methods should be applied to information and computer security. Additionally, physical protection exercises should incorporate cyber-attacks as part of a coordinated physical-cyber-attack at facilities.

A.82. The information and computer security management system may be exercised in a graded approach at various levels within an organization or a State. The value of exercises as assurance activities is that they examine the work flow process and communications in responding to a computer security incident. Additionally, the exercises provide an excellent training mechanism at all levels of management and response.

A.83. The operator should consider the dual benefit of performing exercises and drills which are:

— The exercise of security procedures to test the effectiveness of the procedure in meeting the objectives of the CSP.

— The performance of drills to train personnel on the conduct of the security procedures and thereby improve awareness of the procedures, the rational for the critical tasks within the procedure, and response to computer security incidents.

Intrusive assessment testing

A.84. The operator should evaluate whether to preform intrusive testing is another consideration for evaluation of a system’s or digital asset’s computer security. This evaluation should consider whether it is safe and secure to perform these tests, and whether the operator has the capability to ensure that adverse effects are not brought about, or if caused can remediate the digital asset and system with no effect on safety or security of the facility.

A.85. NST036 [9] identifies further restrictions on intrusive testing of I&C systems.

A.86. Since computer attacks rely heavily on specific configurations, the system under test must be as close to the production systems as possible. Full backup & restore procedures must be in place to return the system to a known stable state should the assessment work create abnormal conditions.

A.87. A test plan should contain the specification of a schedule and budget, identifications of targets and goals, expected deliverables, hardware, software, and resource requirements, rules of engagement, and a recovery procedure.

A.88. Many types of testing are possible. Testing techniques may include, but are not limited to:

— ‘Fingerprinting’, which identifies and quantifies all communications within and between components in a system. Effects of these communications are analysed as to their effect on the target list. Mapping or fingerprinting a network provides the following:

  - Network baseline
  - Network diagram accuracy
  - Identification of potential rogue devices or malicious data communications
  - Verification that boundary protection devices are working as designed
  - Identification of opportunities or areas to improve zoning and perimeter protections

— Fuzz testing or ‘fuzzing’, a black box software testing technique that consists of finding implementation bugs using malformed/semi-malformed data injection in an automated fashion. This technique identifies poor software coding and determines system hardness.

A.89. Metrics are an important part of security testing. Metrics provide a common methodology for evaluating vulnerabilities. With well-developed and common metrics (e.g, common vulnerability scoring system), end users have a common base for vulnerability comparison. Vulnerabilities should be immediately reviewed for identification in a national vulnerability database and explored for potential exploits.

Computer security incident response

A.90. Computer Security Operations should have the responsibility to report suspected computer security incidents according to the incident response plan. Specialized awareness training is encouraged for key roles that would enable the operator to look beyond the basic trust indicators (e.g. suspect of system compromise).

A.91. The operator should recognize that the main aim of computer security is to prevent computer-based systems from being compromised, but organizations need to also be prepared to respond if an external or internal adversary succeeds in compromising their systems.

A.92. Facilities and State organizations should put in place a contingency plan for nuclear security events that involve computer security incidents and the associated response. This plan has the aim to address isolating the danger, mitigating damage, notifying competent authorities and carrying out restoration processes.

A.93. Computer security is not solely a matter of prevention. It must also involve detection and response. States, organizations, and system owners or operators should have processes and contingency plans in place to detect and respond to computer security incidents that might potentially

affect SDAs. Incident response is not an individual activity, but is a collection of activities (see Figure A-1) each of which should be considered.

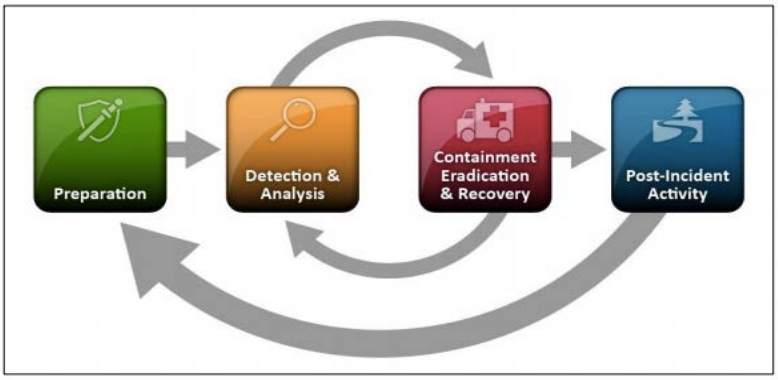

FIG. 10. Computer security incident response from NIST SP 800-61.

A.94. Computer security incidents have the potential to jeopardize the confidentiality, integrity and availability of a computer system and the data it processes, stores or transmits. A security incident might also be a violation — or the imminent threat of a violation — of an explicit or implied security policy, an acceptable use policy, or standard security practice. While certain adverse events (e.g. floods, fires, electrical outages and excessive heat) can cause a system outage, they are not the malicious acts of individuals or organizations and therefore are not considered to be computer security incidents.

A.95. A computer security incident becomes an information security incident or breach when it involves the actual or suspected compromise or loss of information or data. The most serious of these incidents involve sensitive information. The IAEA Nuclear Security Series No 23-G, Security of Nuclear Information, [5] discusses and provides examples of potentially sensitive information associated with nuclear and other radioactive material facilities.

A.96. The facility should create a local computer security incident response team (CSIRT) which is responsible for responding to computer security incidents within their own organization. The size, composition and capabilities of a CSIRT may vary greatly depending on the nature of the organization and the computing infrastructure. The CSIRT should consider the importance of experts on nuclear safety, nuclear security, and emergency preparedness during formation.

A.97. A computer emergency response team (CERT) is an example of a technical authority whose sole purpose is to provide assistance and response capabilities when a computer security incident occurs. CERTs may exist at many levels (national, local or sector). The CERT is available to supplement the internal computer security response capabilities of an organization in responding to any computer security incident.

A.98. The facility should ensure the participation in exercises of CERT team members alongside CSIRT. Important interfaces between the CERT and the CSIRT, including preparatory activities (e.g., pre-clearance of CERT members) should be considered.

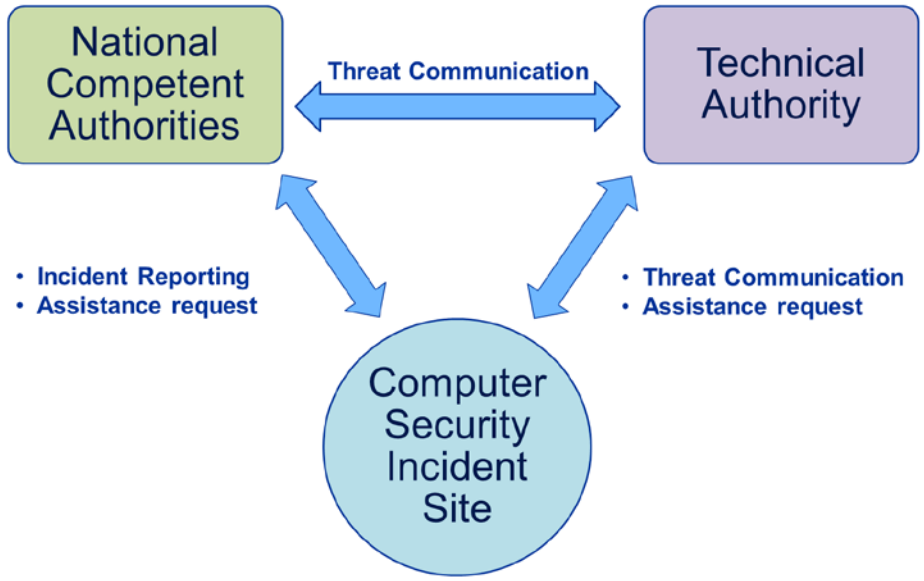

FIG. 11. Computer security incident response interfaces.

Computer security incident response phases

Preparation

A.99. The preparation phase is made up of key planning functions. These include: establishing a policy that will inform the operational processes for responding to computer security incidents and clearly define the roles and responsibilities of all parties involved in the incident response process; drafting and implementing procedures to carry out the policy actions; and the identification of assets. It is important that the criteria for computer security incidents are clearly defined along with the associated response requirements. It is also essential that senior management has agreed these planning and response functions.

Detection and Analysis

A.100. During the detection and analysis phase, the CSIRT should be responsible for determining the technical characterization of the incident. Detection activities include ensuring there is an adequate data monitoring infrastructure in place that supports the detection, collection and preservation of information related to an incident or potential incident. The CSIRT may use a test and evaluation environment for the analysis of incidents so as not to affect operational systems or damage potential forensics evidence.

A.101. Analysis activities may take place at many levels and may extend beyond the initial CSIRT and the initial technical characterization of the incident. Certain aspects of the analysis may require extensive time and effort. The priorities for the analysis may be:

- Determining the potential consequences of the incident on safety, security and emergency preparedness and identifying actions to place the organization or facility in a safe condition.
- Identifying the extent of the incident to establish an adequate response.
- Determining the potential damage from the incident in terms of potential information loss, physical damage to the facility, and public perception.
- Determining the nature of the incident with regards to the adversary's intent and the ongoing threats, including possible future propagation paths.
- Identifying the root cause of the incident and the efforts needed to prevent or mitigate future occurrences.
- Identifying the source of the attack, the adversary and developing a profile of the adversary.

Mitigation (containment, eradication and recovery)

A.102. Given the cyclic and ongoing nature of the computer security incident response process, mitigation activities are ongoing and adapted as additional information is collected and analysed during the detection and analysis phase. The goals for mitigation are: (1) containment of the computer security incident, (2) eradication of any malware from the affected systems, and (3) recovery of system function, which may require other compensatory measures. Even if the compromised components or systems do not provide a critical safety or security function, they would still need to be checked and cleared to guard against the attack propagating to a component or system that does provide a critical safety or security function.

A.103. When planning a containment strategy, the operator should recognize that a number of components may be identified during the incident investigation as having been compromised. If any compromised component provides a critical safety or security function to the organization — such as contributing to the protection of essential computer assets, safe operation of the facility, or nuclear or other radioactive materials — it will be necessary to implement measures to ensure continued protection until the component can be brought back into operation.

A.104. Such measures may include like-for-like replacement of a service (such as a backup firewall), isolation of safety components, systems, and architectures, or a stopgap measure such as a security guard who provides access control protection for part of a facility for example if the digital access

control system become unavailable. It is the function that needs to be recovered, not necessarily the computer system itself.

Post-incident activity

A.105. The last phase of response is to carry out post-incident activities. The goal is to implement measures for the future that will prevent the reoccurrence of this type of computer security incident, enable its rapid detection, or minimize its consequences. This phase may include learning lessons for internal use and possibly to be shared with the wider computer security incident response community to help prevent a similar attack from succeeding elsewhere. Key findings may ultimately allow the Implementation of new security measures to prevent re-infection, as well as threat and vulnerability profiles to be updated within the cyber threat assessments. Other activities include evaluation of the effectiveness of the CSP and identification of training to address gaps in performance. This may also include an assessment of the resources required to address the computer security incident.

Reporting

A.106. During the computer security incident response process there may be a number of situations or phases that require reporting to various agencies, not only on initiation of the incident response, but throughout the process. The goal of reporting is to ensure that everyone who needs to know about a computer security incident is informed in a timely manner, recognizing that in certain types of incidents those responding are likely to be busy. A challenge that organizations often face is determination of the frequency of reporting and the level of detail required.

Activity planning

A.107. Activity planning should ensure that the computer security requirements for the performance and verification of the activities are identified and planned.

A.108. Required personnel and contractor qualifications related to computer security should be identified for the activities being performed, and this should be taken into account in the planning. Each responsible organization has the responsibility to report suspected computer security incidents according to the incident response plan.

A.109. Need to ensure that work instructions include computer security requirements. This could include:

— Instructions for removal of computer security measures (to allow for maintenance)

— Instructions for provision of alternate or compensatory measures (while normal measures are unavailable)

— Instructions for reapplication of computer security measures (following maintenance)

— Instructions for confirming computer security measures have been correctly re-established

A.110. Maintenance instructions should include instructions for configuring the security settings on devices.

A.111. If maintenance requires disposition of equipment that is no longer required, this equipment should be sanitized or securely destroyed.

A.112. Procurement requirements related to computer security should be identified and implemented in the work plan.

PERSONNEL MANAGEMENT

Awareness and training

A.113. While computers are used in nearly all aspects of work and personal life, a general lack of awareness and knowledge exists as to the technology, the cyber threat, security measures and the adverse effect of compromise. Awareness activities and training are key for personnel at all levels within organizations that have nuclear security responsibilities.

A.114. Human error causes or adversely contributes to computer security incidents. Staff at all levels need awareness, but also constant reaffirmation of computer security.

A.115. Awareness of the importance of computer security is a valuable and necessary component of nuclear security culture can support computer security by:

— Recognizing that security supports safety, and that safety and security are both objectives of the organization;

— Ensuring a common understanding of the key aspects of computer security within the organization;

— Encourage and promote good behaviours such as observation and coaching, self-reporting of potential computer and information security incidents, and situational awareness.

— Recognizing that cyber-attacks can affect multiple defence in depth provisions.

— Providing a means by which conflicts between safety and security objectives are reconciled.

— Recognizing and promoting good practices by staff in computer security.

— Raising awareness of the human causes of computer security incidents.

A.116. The following indicators may be used to evaluate awareness of computer security in an organization:

- Computer security requirements are clearly documented and well-understood by staff (as demonstrated by sign off or training)
- Clear and effective processes, protocols and procedures exist for operating computer systems both inside and outside the organization;
- Staff members understand and are aware of the importance of the computer security measures within the CSP;
- Computer systems are maintained secure and operated in accordance with computer security baseline and procedures
- Breaches are regarded by all as serious and undesirable
- Results of observations, evaluations, tests or exercises. For example, testing for response to phishing e-mails.
- Management are fully committed to and supportive of security initiatives whether they are related to cyber or physical systems.

A.117. The aim of the computer security training programme is to ensure that the personnel and contractors have the required knowledge and capability to work according to the facility computer security procedures when performing the tasks assigned to them. Computer security training should be incorporated into an existing training management system.

A.118. The organization should have a training programme with the following elements:

- Successful completion of a computer security training and/or awareness programme should be a precondition for access to computer systems. Training should be commensurate with system security levels and the expected role of users.
- Specialized training and qualifications should be provided to individuals with key security responsibilities (e.g. CSO, computer security team, security officers/personnel, project managers, IT administrators, system engineers, designers, technicians, document management personnel, project personnel, procurement personnel, contractors and senior management).
- Training materials should be updated on a regular basis to include new procedures and emerging threats.
- Employee training should be repeated on a regular basis for all staff to ensure that they are familiar with the new material

— Staff should be required to acknowledge that they understand their security responsibilities.

— Practical evaluations should be considered as a method to evaluation employees understanding of their computer security responsibilities.

A.119. A variety of training approaches should be used, such as e-learning, classroom training, practical exercises and discussion forums[38]. The IAEA, and other external institutions can be a resource for these materials and activities.

A.120. The training programme should include metrics to evaluate computer security awareness, training effectiveness, and processes for continuous improvement and to identify personnel requiring retraining. Metrics may include level of knowledge assessment. Assessment techniques could include computer security awareness exercises and practical evaluations.

EXAMPLE PROCESS FOR PLANNING RESPONSE TO COMPUTER SECURITY INCIDENTS

A.121. An example of a process for planning for computer security incidents can be found in Ref. [23].

[38] Discussion forums may result in information leaks that could assist the adversary, therefore posting of information on publicly available and open discussion forums is discouraged.

1 **REFERENCES**

2

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

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

[4] 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).

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

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

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

[8] INTERNATIONAL ATOMIC ENERGY AGENCY, Security during the Lifetime of a Nuclear Facility, Draft Implementing Guide NST051.

[9] INTERNATIONAL ATOMIC ENERGY AGENCY, Computer Security of Instrumentation and Control Systems at Nuclear Facilities, Draft Technical Guidance NST036.

[10] INTERNATIONAL ATOMIC ENERGY AGENCY, Computer Security for Nuclear Security, Draft Implementing Guide NST045.

[11] INTERNATIONAL ATOMIC ENERGY AGENCY, IAEA Safety Glossary: 2016 Revision.

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

[13] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION AND INTERNATIONAL ELECTROTECHNICAL COMMISSION, Information technology — Security techniques — Information security management systems — Overview and vocabulary, ISO/IEC 27000:2016, ISO, Geneva (2016).

[14] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION AND INTERNATIONAL ELECTROTECHNICAL COMMISSION, Information technology — Security techniques — Information security risk management, ISO/IEC 27005:2011, ISO, Geneva (2011).

[15] INTERNATIONAL ATOMIC ENERGY AGENCY, Physical Protection of Nuclear Material and Nuclear Facilities (Implementation of INFCIRC/225/Revision 5), Draft Implementing Guide NST023.

[16] INTERNATIONAL ATOMIC ENERGY AGENCY, Identification of Vital Areas at Nuclear Facilities, Technical Guidance, IAEA Nuclear Security Series No. 16, IAEA, Vienna (2013).

[17] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION AND INTERNATIONAL ELECTROTECHNICAL COMMISSION, Information technology — Security techniques — Evaluation criteria for IT security, ISO/IEC 15408:2009, ISO, Geneva (2009).

[18] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Nuclear power plants - Instrumentation and control systems - Requirements for security programmes for computer-based systems, IEC 62645:2014, IEC, Geneva (2014).

[19] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION AND INTERNATIONAL ELECTROTECHNICAL COMMISSION, Information technology — Security techniques — Information security management systems — Requirements, ISO/IEC 27001:2013, ISO, Geneva (2013).

[20] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION AND INTERNATIONAL ELECTROTECHNICAL COMMISSION, Information technology —

Security Techniques — Code of practice for information security controls, ISO/IEC 27002:2013, ISO, Geneva (2013).

[21] INTERNATIONAL ATOMIC ENERGY AGENCY, The Management System for Nuclear Installations, IAEA Safety Standards Series No. GS-G-3.5, IAEA, Vienna (2009).

[22] INTERNATIONAL ATOMIC ENERGY AGENCY, Conducting Computer Security Assessments at Nuclear Facilities, IAEA-TDL-006, IAEA, Vienna (2016).

[23] INTERNATIONAL ATOMIC ENERGY AGENCY, Computer Security Incident Response Planning at Nuclear Facilities, IAEA-TDL-005, IAEA, Vienna (2016).

1
2
3

ANNEX I

POTENTIAL ATTACK SCENARIOS AGAINST SYSTEMS IN NUCLEAR FACILITIES

I–1. In support of activities related to computer security techniques for nuclear facilities, and in particular technical guidance provided by IAEA in the main text, it is important to understand how potential adversaries can craft attacks that exploit vulnerabilities within critical operational environments. To that end, this material has been created to encourage readers to think differently about computer security in nuclear operations and have a greater understanding of how threat actors and other adversaries may operate.

I–2. This material is derived from numerous conversations with member states and subject matter experts and is intended to be only examples of possible scenarios. This material is not intended to be interpreted as a recipe for attacking nuclear facilities but rather a starting point for stakeholders and member states to create activities and plans to address the dynamics of the changing threat environment.

I–3. A well-orchestrated computer attack consists of multiple phases:

— Target identification;

— Reconnaissance;

— System access/compromise;

— Attack execution;

— Covering of tracks to maintain deniability.

I–4. Adversarial techniques include some or all of these tactics and should be considered when developing cyber risk profiles specific to nuclear instrumentation and control environments and SDAs. The scenarios presented here assume that these tactics are used and illustrate several use cases that are derived from common themes suggested by industry subject matter experts and member states.

I–5. Threat types are identified and described in IAEA NST045.

SCENARIO I – COMPROMISE OF SUPPORTING ENTITY LEADING TO ACCESS TO CRITICAL OPERATIONAL ENVIRONMENTS

Goal of the attack: To gain access to nuclear information and critical assets by exploiting a trusted path used by support entity.

Discussion: The target of interest is the remote access function used by vendors to access sensitive information and facility SDAs. The adversary compromises the Internet facing remote access portal

that is used by vendors. By attacking the portal (and gaining administrative control via privilege escalation) the adversary modifies the database and changes the email address associated with a specific vendor. This vendor not only has remote access but, when using the remote access, has direct accessibility to critical nuclear operational information and some of the SDAs. The adversary then uses the 'forgot password' function on the portal and the portal sends a password refresh link to the email address implanted by the adversary.

The adversary uses this link to modify the vendor's password and logs in to the portal under the identity of the authorized vendor. Once inside the portal the adversary has access to all vendor information that resides on the portal and can connect directly to those SDAs that the vendor has access to.

From there the adversary begins to modify settings and operational parameters of SDAs leading to operational instability and ultimately to the shutdown of the facility.

SCENARIO II – EXPLOIT THE TRANSITIVE TRUST BETWEEN REPORTING SERVERS ON THE DMZ AND INTERNAL SDAS

Goal of the attack: To access internal sensitive digital assets and systems.

Discussion: Using a variety of open source tools and search engines the adversary locates the Internet facing demilitarized zone (DMZ) servers that are used to report production information related to nuclear isotopes. This server resides on the DMZ but is populated by a master database server that resides on the same network as the control system that produces nuclear isotopes. The master database server collects information from the internal manufacturing production environment and sends this information to the database located on the DMZ servers. The DMZ is separated from production network using a firewall, which is configured with an access control lists (ACLs) that ensure only the database on the DMZ server can communicate to the master database on the production network.

The adversary exploits a vulnerability to get administrative access to the server in the DMZ and takes control of the communication channel between the DMZ server and the master database server that resides on the control system network. Due to the fact that there is a transitive trust that exists between the two servers, and the firewall is configured to allow communications between the DMZ and the master database, the adversary who has control of the server on the DMZ can connect directly to the database that is on the control system network.

Once the adversary has connected to the master database the adversary 'pivots' off of the database and begins to perform reconnaissance and enumeration on the control system assets that are on the same network. Since there are no security measures on the control system network, the adversary is able to take control over vital and sensitive digital assets. This includes compromise of the technology responsible for isotope development, management, transportation, storage and inventory.

SCENARIO III – MALWARE INFECTS NUCLEAR POWER PLANT INSTRUMENTATION AND CONTROL.

Goal of the attack: To force the shutdown of a nuclear power plant (NPP).

Discussion: An engineer at a nuclear power plant takes her work PC home with her, the same computer that is used to support plant engineering and optimization. At home she uses the computer to update performance programmes as well as 'tune' the software responsible for safety monitoring.

While at home she uses the computer to go to a vendor website and obtain a software update for I&C systems - an update that is instrumental in supporting plant operations. While the update is downloading she performs other activities including online banking, visiting her corporate website and checking her social media feeds. Unknown to her she inadvertently downloads malicious software to her computer. This malicious software, or malware, is very new and is unknown to the antivirus companies. Consequently, there is no capability for the antivirus program in her computer to detect this malware and so it not detected and resides on her computer.

Since corporate policy prohibits her from taking her engineering computer into the plant she copies the downloaded control system update to a USB stick, with the intention that the next day she will take the removable media into the plant and apply the software updates to the instrumentation and control assets. However, the malware has also copied itself to the USB stick. The next day the engineer takes the USB stick into the plant control equipment room and inserts it into the engineering workstation. Her intent is to update the system with the vendor supplied software, but along with the software update the malware moves from the removable media into the engineering workstation. The company has assumed that the physical protection countermeasures in place will prevent an authorized computer from connecting to the plant control system network. No consideration has been made for the possibility that infected removable media could be an attack vector to the plant operations.

After the malware infects the engineering workstation it replicates and moves to all of the other networked components within the plant. Since the company has not deployed cyber security countermeasures at the plant level, and has not deployed antivirus within critical plant systems, the malware infects critical digital assets on the network, introduces failure, and forces the plant to shut down.

SCENARIO IV– OBTAIN STRATEGIC AND SENSITIVE INFORMATION ABOUT NUCLEAR PLANT OPERATIONS DIRECTLY FROM INAPPROPRIATELY DECOMMISSIONED EQUIPMENT

Goal of the attack: Obtain enough information to develop an accurate and strategic attack on plant operations.

Discussion: An adversary follows the process of a nuclear power plant going through a system upgrade. Social media and look reporting inform the adversary that the nuclear plant will be procuring a control system in the form of an 'upgrade'. In addition, the company decides to sell off old operational equipment to help pay for the new control system that will be used for plant operations.

Since the facility has no formal decommissioning procedure related to information security the system that was used to run critical instrumentation and control operations is sold off without appropriate sanitization and content review.

The adversary buys the computer systems that formerly operated the plant and discovers up-to-date project files, network diagrams, username and password information and other data that provides a complete and comprehensive understanding of the nuclear facility operations.

The adversary exploits this information and develops a strategic and accurate plan of attack against sensitive digital assets used at the facility. In addition, the adversary uses this information to help populate the content of emails used in a spear phishing campaign to help provide credibility in the communications. Ultimately, the adversary is able to use both the information obtained from the systems purchased and information exfiltration from the spear phishing campaign to launch a blended cyber/physical attack on the facility.

SCENARIO V – STRATEGIC SOCIAL ENGINEERING ON THE FACILITY SECURITY OFFICER

Goal of the attack: A social engineering attack on the facility security officer leads to exfiltration of information that can be used to further an attack.

Discussion: A dedicated and focused social engineering campaign is launched against a facility security officer. Through this campaign the adversary uses a number of different techniques including phishing, physical reconnaissance, open source intelligence and exploitation of the target's social media presence.

The adversary exploits information that is openly available to begin communicating with the security officer, the result being that the security officer trusts the adversary (thinking that it is someone else). As the adversary continues correspondence with the security officer they add well-crafted email attachments that are actually malicious software, software that, when activated, opens up a

communication back to the adversary's computer or packages up specific files on the security officer's computer and sends them (covertly) to the adversary. With this information the adversary is able to create well-crafted attacks related to penetrating physical security systems and intercepting nuclear materials in transit.

ANNEX II

EXAMPLE OF SECURITY LEVELS CLASSIFICATION FOR A NPP

II–1. The assignment in security levels is fundamentally based on the consequences of an attack on the considered system in terms of safety and production availability of the plant: the less tolerable the consequences, the stringer the security level.

II–2. In order to avoid case-by-case analyses of theses consequences, several criteria can be established in order to facilitate the assignment of the security levels.

II–3. One of the fundamental inputs is the safety classification of the considered system. However, it should be stressed that there's not a one-to-one mapping between security levels and safety classes. If a high relevance for safety will involve a stringent security level, it is possible to assign a stringent security level to non-safety classified systems, as some systems may have a critical role or potential consequences from a security point of view. Moreover, performance issues have been considered in the security level assignment criteria.

II–4. The example graded approach relies on the following high-level criteria:

II–5. The **security level 1** is assigned to plant digital systems for which compromise of their integrity or availability could lead to radiological consequences towards the population. This is the case of 1E / F1A safety classified systems (corresponding to systems supporting category A functions in the sense of the International Electrotechnical Commission safety scheme [II–1]).

II–6. The **security level 2** is assigned to plant digital systems for which compromise of their integrity or availability could:

- Degrade the management of an emergency situation, and/or
- Degrade the plant safety in normal operation, and/or
- Degrade the main nuclear process operation, and/or
- Degrade the physical protection of the plant.

II–7. The **security level 3** is assigned to plant digital systems for which compromise of their integrity or availability has no radiological consequences, nor on safety or physical protection, but could affect other major stakes, in particular computer-based systems assisting plant operation or maintenance, or systems which could lead to an effect on power generation within a given duration.

II–8. The **security level 4** is assigned to plant digital systems for which compromise of their integrity or availability has no short-term effect on the plant performance, but can have such an effect on a longer term.

II–9. The **security level 5** is assigned to plant digital systems for which compromise of their integrity or availability has no effect on the safety, on production availability or on the performance of the facility.

II–10. In addition to these high level criteria, the security levels definition can provide a list of typical functions or even directly types of systems which are considered as included, which ease the actual assignment of security levels to systems.

II–11. The security level classification has to focus on the potential related to computerized systems. In many cases, information acquired or calculated by a digital system can also be obtained with non-computerized tool or by a human being, which lowers the security level and leads to keep the categorization of the digital system in proportion.

II–12. When a high diversity of computer-based systems are used for the same function, a primary system supporting the function has to be chosen and categorized in a security level according to the consequences of its compromise. The other computer-based systems can be assigned to a less stringent security level.

REFERENCES FOR ANNEX III

[II–1] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Nuclear power plants - Instrumentation and control important to safety - General requirements for systems, IEC 61513:2011, IEC, Geneva (2011).

[II–2] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Nuclear power plants - Instrumentation and control systems - Requirements for security programmes for computer-based systems, IEC 62645:2014, IEC, Geneva (2014).

GLOSSARY

administrative control measures.: Policies, procedures and practices specifying permitted, necessary and forbidden actions to protect computer-based systems by providing instructions for actions of employees and of contractors, vendors and suppliers.

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

computer based systems. Technologies that create, provide access to, process, compute, communicate, store, or control services involving digital information. These systems may be tangible or virtual. These systems include but are not limited to desktops, laptops, tablets and other personal computers, smart phones, mainframes, servers, virtual computers, software applications, databases, removable media, digital I&C devices, programmable logic controllers, printers, network devices, and embedded components and devices.

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

defensive computer security architecture. The specification of design requirements, constraints and measures that are to be imposed during the lifecycle of a system, such that the identified functions having signficance to the safety and security of the facility and assigned to security levels on the facility level have the required level of protection..

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 level. The degree of security protection required for a facility function and consequently for the system that performs that function.

computer security measures: measures intended to protect computer-based systems against malicious acts perpetrated by individuals or organizations.

computer security programme. The implementation of the computer security policy in the form of organizational roles, responsibilities, and procedures. The plan specifies and details the means for achieving the computer security goals at the facility and is a part of (or linked to) the overall security plan.

computer security zone. A group of systems defined according to their security levels and, if necessary, additional subordinate criteria, to simplify the administration, communication and application of computer security measures.

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.

design basis threat. A comprehensive description of the motivation, intentions and capabilities of potential adversaries against which protection systems are designed and evaluated.

detection: A process in a physical protection system that begins with sensing a potentially malicious or otherwise unauthorized act and that is completed with the assessment of the cause of the alarm.

facility function. The collective effect of a coordinated set of actions, processes and operations that are needed to ensure the safety and security of a facility. Facility functions include but are not limited to functions that are important to nuclear safety, nuclear security, nuclear material accounting and control, or sensitive information.

information security. The preservation of the confidentiality, integrity and availability of information. In addition, other properties such as authenticity, accountability, non-repudiation and reliability can also be involved.

insider threat: A nuclear security threat who has authorized access to a nuclear facility. This insider can exploit their advantages of having authorized access, authority and knowledge to betray trust and bypass security measures.

nuclear security event. An event that has potential or actual implications for nuclear security that must be addressed.

nuclear security measures: Measures intended to prevent a nuclear security threat from completing criminal or intentional unauthorized acts involving or directed at nuclear material, other radioactive material, associated facilities, or associated activities or to detect or respond to nuclear security events.

nuclear security regime. A regime comprising:

— The legislative and regulatory framework and administrative systems and measures governing the nuclear security of nuclear material, other radioactive material, associated facilities and associated activities;

— The institutions and organizations within the State responsible for ensuring the implementation of the legislative and regulatory framework and administrative systems of nuclear security;

— Nuclear security systems and nuclear security measures for the prevention of, detection of and response to nuclear security events.

nuclear security system : An integrated set of nuclear security measures

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

physical control measures: Physical barriers that protect instruments, computer-based systems and supporting assets from physical damage and prevent unauthorized physical access.

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.

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

technical control measures. Hardware and/or software used to prevent, detect, mitigate the consequences of and recover from an intrusion or other malicious act.

threat assessment. An evaluation of the threats — based on available intelligence, law enforcement, and open source information — that describes the motivation, intentions, and capabilities of these threats.