Canada's Nuclear Regulator

Cyber Security and the Protection of Digital Information

Discussion Paper DIS-21-03

July 2021

Canadian Nuclear Safety Commission
Commission canadienne de sûreté nucléaire

Canada

Cyber Security and the Protection of Digital Information
Discussion paper DIS-21-03

Également publié en français sous le titre :
Cybersécurité et protection des renseignements numériques

Document availability
This document can be viewed on the CNSC website. To request a copy of the document in English or French, please contact:

Canadian Nuclear Safety Commission
280 Slater Street
P.O. Box 1046, Station B
Ottawa, Ontario K1P 5S9
CANADA

Tel.: 613-995-5894 or 1-800-668-5284 (in Canada only)
Facsimile: 613-995-5086
Email: cnsc.info.ccsn@cnsc-ccsn.gc.ca
Website: nuclearsafety.gc.ca
Facebook: facebook.com/CanadianNuclearSafetyCommission
YouTube: youtube.com/cnscccsn
Twitter: @CNSC_CCSN
LinkedIn: linkedin.com/company/cnsc-ccsn

Publishing history
July 2021 Version 1

Preface

Discussion papers play an important role in the selection and development of the regulatory framework and regulatory program of the Canadian Nuclear Safety Commission (CNSC). They are used to solicit early public feedback on CNSC policies or approaches.

The use of discussion papers early in the regulatory process underlines the CNSC's commitment to a transparent consultation process. The CNSC analyzes and considers preliminary feedback when determining the type and nature of requirements and guidance to issue.

Discussion papers are made available for public comment for a specified period of time. At the end of the first comment period, CNSC staff review all public input, which is then posted for feedback on the CNSC website for a second round of consultation.

The CNSC considers all feedback received from this consultation process in determining its regulatory approach.

Table of Contents

Executive Summary

The CNSC regulates the use of nuclear energy and materials to protect the health, safety and security of Canadians and the environment, and to implement Canada's international commitments on the peaceful use of nuclear energy. As part of accomplishing this mandate, the CNSC regulates nuclear security via the *General Nuclear Safety and Control Regulations* and the *Nuclear Security Regulations* (NSR).

The CNSC is proposing amendments to the NSR, including in areas pertaining to cyber security, specifically, the protection of prescribed information and computer-based systems and components that perform or impact nuclear safety, nuclear security, emergency preparedness and management, and safeguards functions. The CNSC issued a discussion paper, *Proposals to Amend the Nuclear Security Regulations*, DIS-21-02, which discusses the NSR changes at a high level. The purpose of this discussion paper is to provide details regarding the proposed changes to the requirements and guidance for cyber security and the protection of digital information. This discussion paper also proposes expanding cyber security and information protection requirements to other licensees not governed by the NSR.

In addition, the CNSC is proposing to add a requirement requiring all licensees subject to the regulations to assess their vulnerability to cyber threats and that cyber threat be included in the licensee's threat and risk assessment (TRA). The objective of this requirement is to ensure that licensees are able to detect and respond to cyber attacks targeting prescribed information and systems performing functions important to nuclear safety, security, emergency preparedness and safeguards. Affected licensees will be required, as part of their overall security program, to develop a cyber security program and measures to manage the risks identified in their TRAs. Affected licensees will also be required to report cyber security incidents in a similar manner to other security incidents. This activity is already being undertaken by high-security sites (HSS).

The CNSC's expectations for cyber security at HSS are set out in the CSA Group standard CSA N290.7, *Cyber Security for Nuclear Power Plants and Small Reactor Facilities* (N290.7) [1]. CSA N290.7 is currently undergoing revision and the CNSC is involved in the revision process. If required, the CNSC may also consider adding cyber security elements to its regulatory framework to supplement N290.7, within the REGDOC-2.12 series. This discussion paper does not propose any additional cyber security requirements for assets providing safety, security, emergency preparedness and safeguard functions for licensees that are already required to comply with N290.7.

In 2015, the International Atomic Energy Agency conducted an International Physical Protection Advisory Service (IPPAS) [2] mission to Canada to review its nuclear security regime and regulatory framework. In its mission report, the IPPAS recommended that the CNSC consider extending cyber security requirements to other at-risk licensed activities beyond nuclear power plants, such as nuclear fuel facilities and nuclear substance processing facilities. In response to this recommendation, the CNSC reviewed the risks to these licensees and is proposing potential requirements and guidance for cyber security to certain at-risk licensees who are not subject to the NSR. Lessons learned from the implementation of N290.7 at nuclear power plants were used to develop potential improvements in the regulation of cyber security.

The CNSC is considering expanding cyber security requirements to licensees who are not covered by the NSR, such as Category 1 and 2 sealed sources licensees. There is currently very little Canadian or international experience with the regulation of cyber security applied to nuclear substances, consequently, this paper is primarily aimed at gaining information that can be used as the basis for developing regulatory requirements and guidance in this area.

This paper also proposes an approach for protecting prescribed digital information and sensitive information managed digitally by licensees. The approach is similar to that employed for managing classified and sensitive information managed by the Government of Canada.

The proposed regulatory approach and proposed requirements and guidance are set out in this discussion paper for consideration by licensees, proponents, the Canadian public, civil society organization, Indigenous peoples, other government departments and agencies, and other stakeholders.

This paper is designed to initiate discussions with CNSC stakeholders. The CNSC may engage in additional consultations with interested parties to further the discussion and to gather relevant information. All feedback received during the consultation phase of this project will inform the CNSC's approach.

Cyber Security and the Protection of Digital Information

1. Information

Computer-based systems play an increasing role in the nuclear industry, and are used to provide for the safe and secure operations of facilities and activities that use, store and transport nuclear substances. Adversaries may use cyber attacks to target computer-based systems to facilitate malicious acts (e.g., sabotage or theft of nuclear substances). Cyber attacks may be used in conjunction with other conventional means such as physical actions and the involvement of insiders.

Cyber attacks targeting computer-based systems potentially allow adversaries to compromise the function and performance of nuclear safety systems, security systems, emergency preparedness systems, and safeguard systems, and auxiliary systems that support these systems. Cyber attacks against nuclear safety systems, for example, may potentially result in injury or increase the likelihood of injury to workers and/or the public, or may result in harmful releases to the environment. Cyber attacks may also degrade the performance or function of physical protection systems, which could facilitate the sabotage of a nuclear facility or the theft or sabotage of nuclear substances.

Cyber attacks could also allow adversaries to gain unauthorized access to sensitive information that is stored, processed and transmitted on computer-based systems such as information technology systems and corporate networks. Cyber attacks targeting sensitive information could allow adversaries to deny access to or falsify sensitive information required for safe and secure operation. It could also allow unauthorized disclosure of prescribed and sensitive information, such as details of security arrangements or information regarding shipments of material, which could facilitate theft of nuclear substances or acts of sabotage during transport.

The CSA Group has developed a national standard, N290.7 [1], for cyber security at nuclear power plants and small reactor facilities. This standard was developed with the involvement of licensees, the CNSC and other stakeholders. N290.7 contains requirements and guidance for a risk-informed cyber security program to protect from cyber attack the systems performing functions important to nuclear safety, nuclear security, emergency preparedness and safeguards (SSEPS). N290.7 also defines cyber security measures which may be applied to facilities other than nuclear power plants and small reactor facilities using a graded approach as defined in REGDOC 3.5.3, *Regulatory Fundamentals* [3].

Where specific cyber security requirements do not exist, it is difficult for the CNSC to verify that digital information and nuclear substances are adequately protected from threats using cyber attack to facilitate theft and sabotage. The following are areas where additional cyber security and information protection requirements may be needed:

- The CNSC proposes developing specific cyber security requirements for protection of SSEPS functions at the facilities and activities listed in tables 2 and 3.
- CNSC regulatory document REGDOC-2.12.3, *Security of Nuclear Substances: Sealed Sources and Category I, II and III Nuclear Material* [4], specifies that "This information should not be stored on open or shared computer networks without proper protection" but provides no specific requirements or guidance for protection of these networks. The CNSC proposes developing specific information security requirements to protect computer based systems and networks that prepare, use, store, and transmit sensitive information, including prescribed information.

The status of cyber security requirements for licensees affected by the proposed requirements are summarized in table 1.

This paper seeks to initiate the discussion for developing regulatory requirements and guidance for licensees. Further discussions will be held in consultation meetings later this year to continue the conversation.

The feedback from this paper and future consultation meetings will inform the CNSC's regulatory approach as it relates to cyber security and the protection of digital information. It will also complement existing requirements and guidance that apply to SSEPS.

Table 1: Current cyber security requirements

Licence types or activities	Current requirements for cyber security for nuclear safety, nuclear security, emergency preparedness and safeguards
High-security sites	
Nuclear power reactor operating licences Nuclear research and test establishment operating licences and decommissioning licences	As per each License Condition Handbook (LCH), licensing basis publications are as follows: • REGDOC 2.12.3 [4]section 6.2 requires a cyber security program in accordance with CSA N290.7 [1] • N290.7 [1] is identified as a licensing basis document in the LCH
Waste facility operating licences	As per each LCH: • Require a cyber security program that includes a defined list of program elements • N290.7 [1] is included as a guidance document in the LCH
Facilities with Category III nuclear material (including research reactors) and Class IB research accelerators	
Research Reactors	As per each LCH, the licensee is required to implement cyber security measures to protect cyber critical assets for SSEPS functions
Class IB facilities (table 2)	No specific cyber security requirements
Category 1 and 2 sealed source licensees	
All category 1 and 2 sealed source licensees Representative activities involving these sources are listed in table 3	No specific cyber security requirements

Licence types or activities	Current requirements for cyber security for nuclear safety, nuclear security, emergency preparedness and safeguards
Entities who transport or arrange the transport of Category I, II or III nuclear material or Category 1 or 2 sealed sources	
Transport of Category I, II and III nuclear material Transport of sealed sources requiring transport security plans (Category 1 and 2 sealed sources)	No specific cyber security requirements

1.1 Scope

For licensees with nuclear power reactor operating licences, nuclear research and test establishment operating licences, or nuclear research and test establishment decommissioning licences, the scope of this document is to propose guidance and requirements for information protection. The scope of this document does not include cyber security to protect SSEPS functions, since these licensees are required to implement cyber security programs following N290.7 [1].

For licensees listed in table 2 (facilities, including research reactors, with Category III nuclear material; and Class IB licensees) this document provides potential requirements and guidance for information protection and for cyber security to protect SSEPS functions.

For activities involving Category 1 and 2 sealed sources listed in table 3, this document provides potential requirements and guidance for information protection. It also contains questions designed to obtain information that could be used as the basis for developing requirements and guidance for cyber security to protect SSEPS functions.

For licensees who transport, or arrange the transport of Category I, II or III nuclear material or Category 1 or 2 sealed sources, cyber security requirements applicable to transport are provided. The scope of the document also includes provisions for information security and cyber security principles that underpin the potential requirements and guidance.

Table 2: Licensees (including research reactors) with Category III nuclear material, and Class IB accelerators

Facility type
Waste management facilities that are not HSS
Uranium conversion facilities
Reactors under decommissioning
Nuclear substance processing facilities
Fuel manufacturing and refineries
Prototype waste facilities
Research reactors
Class IB research accelerator facilities

Table 3: Representative activities involving Category 1 and 2 sealed sources

Activity
Irradiators: pool type, sterilization and food preservation
Irradiators: self-shielded
Irradiators: blood/tissue
Processing/manufacturing
Multi-source teletherapy (gamma knife)
Teletherapy (source-based)
Industrial radiography
Well logging

1.2 Pre-consultation activities to date

The CNSC had previously consulted stakeholders on plans to modernize the CNSC's regulations, including the NSR, via the discussion paper DIS-14-02, *Modernizing the CNSC's Regulations* [5]. A summary of the comments received from stakeholders, as well as the CNSC's responses to those comments, was published in What We Heard Report – DIS-14-02 [6].

The CNSC organized three workshops with stakeholders in 2016 and 2017 to research potential regulatory amendments that might be made to the NSR based on operational experience and new technologies potentially impacting the security of nuclear facilities already in place or possible in the foreseeable future. The attendees were those directly responsible for implementing security measures at nuclear facilities and those responsible for the security of nuclear and/or radioactive material, prescribed equipment and prescribed information, as well as the designers of future reactor technologies.

The attendees provided comments on the areas of the NSR where the CNSC was considering amendments; suggested additional areas to consider amendments; and, provided preliminary information on the impact of those potential amendments. CNSC published the results of these workshops in the *Stakeholder Workshop Report: Periodic Review of the Nuclear Security Regulations* [7].

The CNSC intends to conduct additional consultation meetings in the summer and fall of 2021. These consultation meetings, based on the proposals outlined in this paper, will provide an opportunity to discuss the proposed changes and their potential impacts and challenges, in greater detail, with licensees, proponents, the Canadian public, civil society organizations, Indigenous peoples, other government departments and agencies, and other stakeholders. More details on these events will be provided in the coming months.

1.3 Document organization

The remainder of this document is organized as follows:

- The first part of this paper outlines the proposed regulatory guidance to protect digital information from cyber attacks throughout its lifecycle.

  - Section 2 describes the requirement to protect prescribed information.
  - Section 3 provides an overview of information protection principles and contains questions to solicit input for the development of regulatory guidance.

- The second part of this paper outlines potential guidance for cyber security of systems and networks used to implement SSEPS functions.

  - Section 4 identifies licensed activities possibly requiring cyber security programs and/or measures.
  - Section 5 provides an overview of a cyber security program, cyber security measures, a risk-informed graded approach and defence in depth.
  - Section 6 provides potential cyber security requirements and guidance for the protection of high-security sites.
  - Section 7 provides potential cyber security requirements and guidance for the protection of licensees with Category III nuclear material, including research reactors and Class IB research accelerators.
  - Section 8 provides potential cyber security requirements and guidance for the protection of selected nuclear substance licensees.
  - Section 9 provides potential cyber security requirements for entities who transport or arrange the transport of Category I, II or III nuclear material or nuclear substances

2. Information Protection for CNSC-Licensed Activities

An objective of the *Nuclear Safety and Control Act* (NSCA) [8] is to limit the risks to national security, the health and safety of persons and the environment that are associated with the production, possession and use of information prescribed under the act. The NSCA provides for the creation of regulations related to prescribed information.

The CNSC regulates nuclear security pursuant to:

- The NSR which apply to nuclear facilities that produce, process, use, store and/or transport Category I, II and/or III nuclear material and nuclear facilities listed under Schedule 2 of the NSR.
- The *General Nuclear Safety and Control Regulations* (GNSCR)[9] which apply to activities described in paragraphs 26 (a) to (f) of the NSCA. These activities include the possession, transfer, import, export, use or abandonment of prescribed information.

Together, the NSR and GNSCR ensure that Canada continues to fulfill its domestic and international obligations for the security of nuclear facilities, nuclear and radioactive materials, prescribed equipment and prescribed information as required by the NSCA. They are currently supported by four nuclear security regulatory documents that provide guidance on how applicants and licensees may meet the nuclear security regulatory requirements. These regulatory documents are as follows:

- REGDOC-2.12.1, *High-Security Facilities, Volume I: Nuclear Response Force* (2018) (Classified) [10]
- REGDOC-2.12.1, *High-Security Facilities, Volume II: Criteria for Nuclear Security Systems and Devices* (2018) (Classified) [11]
- REGDOC-2.12.2, *Site Access Security Clearance* (2013) [12]
- REGDOC-2.12.3, *Security of Nuclear Substances, Sealed Sources and Category I, II and III Nuclear Material* (2020) [4]

There currently is no CNSC regulatory document that provides guidance for the protection of prescribed information in digital form, or for the protection of computer-based systems, networks and media that are used to create, store, process, and transmit prescribed information.

The following section describes information security principles. They also contain questions for licensees regarding how these principles might be applied to the protection of digital information and computer-based systems, networks and media.

3. Principles of Information Protection

3.1 Definition of prescribed information

Section 21 of the GNSCR defines prescribed information as information (including a record of that information) that concerns:

a) "a nuclear substance that is required for the design, production, use, operation or maintenance of a nuclear weapon or nuclear explosive device, including the properties of the nuclear substance;
b) the design, production, use, operation or maintenance of a nuclear weapon or nuclear explosive device;
c) the security arrangements, security equipment, security systems and security procedures established by a licensee in accordance with the Act, the regulations made under the Act or the licence, and any incident relating to security; and
d) the route or schedule for the transport of Category I, II or III nuclear material, as defined in section 1 of the *Nuclear Security Regulations*."

Prescribed information must be protected throughout its lifecycle, regardless of its format (e.g., digital or hard copy). The licensee is responsible for implementing security measures (physical and cyber) commensurate with the sensitivity level of the information being managed. Sensitivity in this context refers to the level of impact that the unauthorized release could have on the safe and secure operation of the facility or activity.

The "national interest" is the defence and maintenance of the social, political, and economic stability of Canada. An example of prescribed information in the national interest would be the transportation details of nuclear material in Canada.

3.2 Sensitive information and sensitive information asset definitions

The CNSC proposes the following definition for sensitive information: "any information, including prescribed or classified information, in whatever form, including software, for which the unauthorized disclosure, modification, alteration, destruction, or denial of use could compromise nuclear security". The CNSC proposes the following definition for sensitive information asset: "any equipment or components, including digital assets, that are used to store, process, control, or transmit sensitive information".

3.3 Information protection objectives

The pillars of information protection are the assurance of the confidentiality, integrity and availability of information. During the pre-consultation activities, and as summarized in section 3.6 of *Stakeholder Workshop Report: Periodic Review of the Nuclear Security Regulations* [7], some NPP licensee participants were of the view that the above information protection objectives should be defined in a flexible manner to allow their existing information protection mechanisms

to be credited with meeting the regulatory requirements. Other participants were of the view that it would be challenging to achieve consistency with a performance-based approach and that a degree of prescriptiveness would be required.

3.4 Information protection scope

This discussion paper focuses on the protection of sensitive information, including prescribed information, in digital form. This involves protection against cyber attacks which target:

- digital media and portable devices on which digital information is stored
- the computer-based systems that are used to create, store, process and transmit digital information
- the communications networks over which digital information is transmitted

Many licensees already have existing information protection programs or information security measures that protect their digital information. Using performance-based requirements could allow these existing programs to be credited whereas using prescriptive requirements may require significant changes to existing programs.

3.5 Proposed lifecycle for information and specific considerations

Figure 1 describes the CNSC's proposed lifecycle for the management of digital information. Subsequent content in this section outlines the possible activities that licensees may be requested to perform to manage digital information. The phases of the information lifecycle are described in greater detail in subsequent sections.

Figure 1: Proposed lifecycle for digital information

3.5.1 Create phase

In the Create phase, the licensee creates information. This information can be in any form, including paper, thought or electronic record. The information may be sensitive or not.

3.5.2 Identifying sensitive information

In this phase, licensees could be expected to:

- conduct a review to determine if the licensee creates, uses, stores, transmits or disposes of sensitive digital information including prescribed information
- identify sensitive information assets, including computer systems and networks which create, store, process, and transmit prescribed digital information

If the licensee determines that it does not manage sensitive digital information, then it may be reasonable to expect that licensees would not be required to implement any of the security measures applicable to information protection outlined in this document; however, it could implement them as a best-practice.

3.5.3 Classifying and marking sensitive information

If the licensee determines that they manage sensitive information, including prescribed information, they would be expected to ascertain its sensitivity level to determine the appropriate levels of protection for their information.

Sensitivity levels vary based on the exact contents of the document in question and the potential impacts on the national and non-national interest should the information be compromised. Table 4 outlines the various sensitivity levels which can be assigned to information and the respective potential level of injury for each level.

In addition, appendix A was created as a reference guide to determine the potential sensitivity level of information typically held by a licensee. The list of documents was derived from International Atomic Energy Agency (IAEA) Nuclear Security Series (NSS) 23-G, *Security of Nuclear Information* [13], which describes the documents and the information it contains. Appendix A recommends a mapping between the documents/information and the government of Canada information sensitivity levels in Table 4.

Sensitive information, regardless of its form, should be marked with its sensitivity level so that it can be managed appropriately. CNSC staff can assist licensees to determine the most appropriate sensitivity level upon their request; however, the responsibility for the assignment of sensitivity always will remain with the creator of the document.

Table 4: Information sensitivity levels and comparative injury

Level	Description	Comparative injury
Top secret	Applies to information or assets that, if compromised could cause exceptionally grave injury to the national interest	Release could result in an extreme event that could impact a large portion of the population: • Widespread loss of life • Widespread psychological trauma • Potential civil unrest
Secret	Applies to information or assets that, if compromised could cause serious injury to the national interest.	Release could have significantly negative impacts on individuals or the nation: • Potential loss of life or disability for some • Serious illness or injury for many • Alienation of large groups
Confidential	Applies to information or assets that, if compromised could cause injury to the national interest	Release could have serious impacts on the nation: • Moderate damages to national opinion / international relations

Some licensees already have established information classification schemes which use different terminology and criteria for classification. They suggested during consultation that, by using broad definitions for nuclear security information, new classification systems would not be required. The CNSC proposes that, as a government entity, it would make use of the classification scheme described in table 4 in any regulatory guidance. Licensees having existing schemes could

map the classification scheme described in table 4 to their existing classification schemes to avoid creating a new classification system.

The CNSC would like to know:

Q1. Do you agree with the proposed model for managing prescribed information electronically?

Q2. Could this model be used to manage all sensitive information generated by your organization?

Q3. Do you agree with the proposed manner for the identification, classification and marking of sensitive information (including prescribed information) that you manage? Why? Why not?

Q4. Please identify any impacts that would arise if the CNSC would make the suggested practices mandatory.

3.5.4 Using sensitive information

Licensees are prohibited from transmitting prescribed information with the exceptions listed in subsection 23 (1) of the GNSCR. The CNSC proposes that when sensitive information (including prescribed information) is transmitted or transferred it must be protected with security measures commensurate with the sensitivity of the information and only to those with a need-to-know[1] and appropriate security clearance or trustworthiness verification. Licensees are encouraged to use the RCMP's Guide G1-009, *Transport and Transmittal of Protected and Classified Information* [14], for transmitting sensitive information.

All systems used to process sensitive information, including prescribed information, should be protected against cyber attack to assure the confidentiality, integrity and availability of the information.

The following documents can be leveraged to manage information protection and to implement cyber security measures to protect sensitive information. These measures may be implemented using a graded approach:

- Communications Security Establishment: ITSG-33, *IT Security Risk Management: A Life Cycle Approach*, and its catalogue of security controls [15]
- National Institute of Standards and Technology: SP 800-53, *Security and Privacy Controls for Information Systems and Organizations* [16]
- International Organization for Standardization: ISO/IEC 27001, *Information Security Management* [17]

To ensure that digital prescribed information and other sensitive information is protected, the licensee should implement appropriate measures. Possible measures include:

- limiting access to the digital files to those with a need-to-know and appropriate security clearance or trustworthiness verification
- detecting unauthorized access to files by those without a need-to-know
- Encrypting files in storage using cryptographic algorithms certified by a national technical authority

[1] Need-to-know: demonstrable operational requirement to access information.

- creating and verifying cryptographic checksums of electronic records to detect tampering (e.g., digital signatures, message digests)
- Ensuring that protection is extended to backup copies of the documents (e.g., copies used for business continuity or disaster recovery)

The CNSC proposes that licensees manage information security risk as part of their nuclear security program and that measures are implemented to protect information using a graded approach.

The CNSC would like to know:

Q5. What specific standards or guidance have you implemented to protect the prescribed information and other sensitive information on your information systems?

Q6. Are there additional sources of guidance for protecting your information systems that would be suitable to you?

Q7. Would your organization be able to implement the example measures listed above?

3.5.5 Storing and disposing of sensitive information

Pursuant to subsection 28 (1) of the GNSCR [9], every licensee must retain prescribed information for the period specified in the regulations applicable to their respective licensed activity. If no period is specified, then the licensee must retain the prescribed information for one year after the expiry of their licence. This applies regardless of the form of information (i.e., electronic or hard copies).

Prescribed information must be safeguarded while in storage. Section 3.5.4 provides examples of measures that may be employed to safeguard digital prescribed information in use, and many of these can also be applied to information in storage. Physical and cyber security measures should be considered to detect attempts to steal and/or falsify or destroy digital prescribed information and these measures should be hardened against cyber attack. The documents listed in section 3.5.4 provide guidance for security measures applicable to the storage of digital information.

Examples of guidance relating to disposal include:

- Canadian Centre for Cyber Security: *Sanitization and Disposal of Electronic Devices* (ITSAP.40.006) [18]
- Information and Privacy Commissioner: *Disposing of Your Electronic Media Technology Fact Sheet* [19]
- Cornell University: *Best Practices for Media Destruction* [20]

To dispose of electronic prescribed information, the licensee could:

- Securely erase or destroy the media based on its type
- Sanitize systems before removal

The CNSC would like to know:

Q8. What specific measures have you implemented to protect the prescribed information you are managing while not in use?

Q9. What are your thoughts concerning the examples of guidance provided?

Q10. Are there additional sources of guidance for disposal that would be suitable to reference?

3.6 Incident response and reporting

Licensees are responsible for notifying the CNSC as to the unauthorized access and/or disclosure of prescribed information immediately upon discovering the compromise. The expected timelines for a detailed event report describing what transpired, the actions taken, etc., are provided in REGDOC-3.1.1, *Reporting Requirements for Nuclear Power Plants*, Version 2 [21], REGDOC-3.1.2, *Reporting Requirements, Volume I: Non-Power Reactor Class I Facilities and Uranium Mines and Mills* [22] or REGDOC-3.1.3, *Reporting Requirements for Waste Nuclear Substance Licensees, Class II Nuclear Facilities and Users of Prescribed Equipment, Nuclear Substances and Radiation Devices* [23] depending upon the licensee type.

To meet these regulatory requirements, licensees should develop and implement:

- systems to identify unauthorized attempts at accessing prescribed information
- systems to signal actual incidents of compromise
- response procedures to manage events
- reporting mechanisms

Guidance for planning and handling computer security incidents is provided in the following documents:

- National Institute of Standards and Technology (NIST): SP 800-61 Rev 2, *Computer Security Incident Handling Guide* [24]
- IAEA: TLD-005, *Computer Security Incident Response Planning for Nuclear Facilities* [25]
- Public Safety Canada: *Developing an Operational Technology and Information Technology Incident Response Plan* [26]

The CNSC would like to know:

Q11. In terms of incident response and reporting, what measures do you currently have in place to monitor for and address security incidents?

Q12. What impacts and challenges do you foresee implementing the suggested measures?

Q13. Are there any other measures that you believe should be included?

3.7 Evaluating effectiveness and continuous improvement

Security measures, including programs, policies, plans, etc. must always evolve to meet threats. As the risk environment can change over time, the CNSC suggests that licensees generating and managing sensitive information implement mechanisms to periodically review and update all security measures to mitigate threats and risks.

Review timeframes should be defined and respected. The licensee should also initiate ad hoc reviews following key events such as an incident at the facility or elsewhere in industry, or as a result in changes to a policy, threat or regulation. The review should apply at all levels with nuclear security responsibilities. Reports should be generated documenting any gaps or areas that require intervention.

Change management plans should be developed to improve existing measures or implement additional security measures to protect sensitive information. These plans (where possible) should

include specific time frames for implementation and any associated performance metrics to demonstrate efficacy.

Changes to security measures should be communicated to the licensee's employees where practicable.

The CNSC would like to know:

Q14. The CNSC outlined possible steps that should be taken to evaluate the effectiveness of security measures. Do you agree with these steps? What impacts would these activities pose to your organization if made mandatory?

4. Cyber Security for CNSC-Licensed Activities

The CNSC regulates thousands of licensees; each operating in different environments with unique characteristics and risks. As mentioned, one risk includes the disruption of the safe and secure operation of licensed activities through cyber attacks.

Licensees with power reactor operating licences, nuclear research and test establishment operating licences, or nuclear research and test establishment decommissioning licences, are required to implement and maintain cyber security programs as part of their nuclear security programs. One element of their cyber security programs is to implement cyber security measures to protect systems and functions to prevent compromise. Currently, as shown in table 1, the implementation of a cyber security program is not a requirement for certain other licensed activities. At the suggestion of the IAEA's 2015 International Physical Protection Advisory Service (IPPAS) mission [2], CNSC subject matter experts evaluated the cyber security risks associated with all licensed nuclear facilities and activities by identifying the licensees that could be at higher risk and identifying possible security measures to reduce those risks to acceptable levels.

4.1 Identifying other possible at-risk licensed activities

CNSC staff conducted an internal review and identified all licensed nuclear facilities and nuclear substance licensees for which cyber security programs or measures are warranted. The CNSC proposes that licensed activities and licensees listed in tables 2 and 3 of section 1.1 be required to establish a cyber security program or cyber security measures commensurate with the risk of compromise.

4.2 Proposed way forward for other possible at-risk licensees

The CNSC's proposed way forward for the cyber security requirements and guidance for the possible at-risk licenses is, using a risk-informed graded approach, to separate the licensees into the groups listed in table 1.

The sections of this paper that provide the potential requirements and guidance for these groups of licensees is shown in table 5. To provide additional background and context for the potential requirements and guidance, section 5 provides an overview of cyber security principles.

Table 5: Way forward for cyber security of SSEPS systems and functions

Licensee or activity type	Way forward
High-security sites	Section 6
Facilities, including research reactors, with Category III nuclear material	Section 7
Selected nuclear substance licensees (table 3)	Section 8
Entities who transport or arrange the transport of Category I, II or III nuclear material or nuclear substances	Section 9

5. Principles: Cyber Security Program, Cyber Security Measures, Graded Approach, Defence in Depth

This section describes some key cyber security principles that may be used as the basis for establishing cyber security. This is provided for information only. The requirements and guidance for specific groups of licensees are described in sections 6 through 9.

5.1 Cyber security program

A cyber security program defines the roles, responsibilities and procedures used by a facility to meet their cyber security objectives. The CNSC expects that, when cyber security programs are required, they are implemented and maintained to ensure that computer-based systems that perform or support SSEPS functions are protected against cyber attack.

IAEA NSS 17, *Computer Security at Nuclear Facilities* [27], provides a recommended framework for nuclear facilities, which includes the following major elements:

1. Organization and responsibilities
2. Asset management
3. Risk, vulnerability, and compliance assessment
4. System security design and configuration management
5. Operational security procedures
6. Personnel management

NSS 17 provides additional details on these elements. CSA N290.7 [1] also provides cyber security program elements.

5.2 Cyber security measures

Nuclear security measures prevent an adversary from completing malicious acts against nuclear material, radiological material, associated facilities or associated activities. Nuclear security measures also detect and respond to such events[2]. These measures:

- prevent, delay, detect, and respond to malicious and unauthorized acts
- mitigate the consequence of these acts

[2] IAEA, Objective and Essential Elements of a State's Nuclear Security Regime, Nuclear Security Fundamentals, IAEA Nuclear Security Series No. 20, IAEA, Vienna (2013)

- recover from the consequences of these acts

Cyber security measures are an element of nuclear security that protect computer based systems that perform or support SSEPS functions against cyber attack. These measures:

- make computer-based systems less susceptible to malicious acts
- prevent unintentional/non-malicious acts from degrading cyber security
- reduce the consequence of malicious acts (e.g., measures that respond to cyber attacks to prevent them from propagating)

Cyber security measures can be physical, technical or administrative in nature, and are supported by other measures such as physical protection, personnel security and information security.

The Treasury Board Secretariat's *Directive on Security Management* [28]defines practices that are crucial for safeguarding Government of Canada IT security systems. In addition, Public Services and Procurement Canada's *Contract Security Manual* [29] outlines the procedures to be applied by contractors for the safeguarding of government information and assets. The contents of these two documents may be adapted to secure sensitive information including prescribed information developed and managed by licensees.

In addition, the following sources have identified components of a security plan to protect information and computer-based systems. These sources also includes recommendation and guidance information on protection of operating technologies used to provide safety, security, emergency preparedness, and safeguard functions:

- N290.7-14, *Cyber Security for Nuclear Power Plants and Small Reactor Facilities* [1]
- IAEA Nuclear Security Series No. 23-G, *Security of Nuclear Information* [13]
- IAEA Nuclear Security Series No. 17, *Computer Security at Nuclear Facilities* [27]
- IAEA Nuclear Security Series No. 33-T, *Computer Security of Instrumentation and Control Systems at Nuclear Facilities* [30]

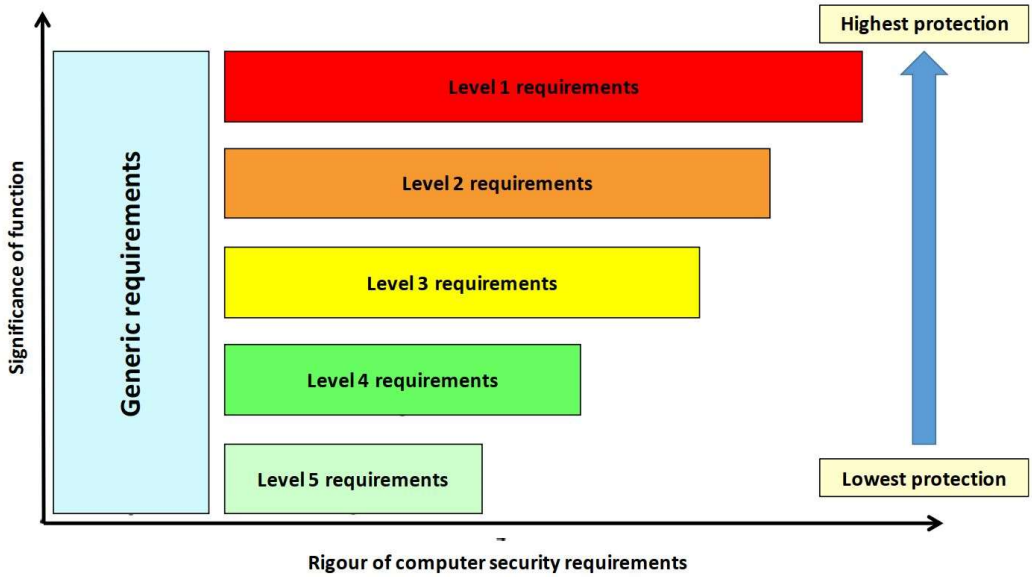
5.3 Risk-informed graded approach

A risk-informed graded approach is a fundamental element of nuclear security in which the rigour of the security requirements are proportionate to the consequence arising from a malicious act. Applied to cyber security, the strength of measures that should be applied is commensurate with the consequence that would arise from a cyber attack that compromised an SSEPS function performed by that system.

A standard means of implementing a graded approach for cyber security is to define a set of cyber security levels each with a different level of security protection, and to assign computer systems to those levels based upon the consequence of compromise of the SSEPS functions performed by those computer systems. An example from IAEA NSS 17 [27] showing 5 levels of protection is provided in figure 2. In this example, generic security requirements apply to all functions then, as the significance (e.g., the safety or security significance) of a function increases, the rigour of the security requirements increase, such that assets having the most significance are protected to the highest level.

By making use of multiple levels of security, overprotection of assets may be reduced thereby decreasing the level of effort required to secure the facility or activity. An example using 3 levels (high, moderate, low) is provided in CSA N290.7 [1].

Figure 2: Illustration of the graded approach using the security level concept (adapted from [16])



5.4 Defence in depth

Defence in depth in cyber security requires successive layers of cyber security measures that have to be overcome or bypassed by an adversary in order to compromise systems performing SSEPS functions [30]. It also requires diverse and independent measures in terms of type (e.g., physical, administrative and technical) and function (e.g., detect, delay, respond, and recover).

IAEA NSS 17 [27] provides an approach for implementing defense in depth by defining and establishing a defensive cyber security architecture and deploying cyber security measures within that architecture. In the approach of NSS 17 [27], cyber security zones are used as the basis for creating defense in depth.

A zone is a logical and physical grouping of assets that have similar requirements for protection that is established for the purposes of simplifying the application and management of cyber security measures. The degree of protection required for each zone is based upon the most significant nuclear security consequence arising from compromise of systems within that zone. The arrangement of zones within the defensive cyber security architecture can establish defense in depth by requiring an adversary to traverse multiple protected zone boundaries to target systems performing SSEPS functions.

The practical approach, recommended in IAEA NSS 17 [27], involves:

- arranging computer systems into zones (based upon common security requirements, such as their security level as described in section 5.3)
- establishing physical and logical zone boundaries
- specifying rules for information flow between zones
- using cyber security measures at zone boundaries to enforce these rules and detect security policy violations
- deploying measures within zones

Following the above approach can result in an arrangement of zones that help to establish defense in depth.

The CNSC would like to know:

Q15. What are your thoughts in relation to the application of the graded approach and defence in depth for cyber security for your licensed activity?

6. Potential Cyber Security Requirements for High-Security Sites

The following section applies to all HSS. The proposed changes to the NSR would require that these sites assess their vulnerability to cyber threats and that cyber threats be included in licensees' TRAS. The objective of this proposed requirement is to ensure that licensees are able to detect and respond to cyber attacks targeting sensitive information, including prescribed information, and systems performing functions important to nuclear safety, security, emergency preparedness and safeguards. As a result of this proposed change, affected licensees will be required, as part of their overall security program, to develop a cyber security program and measures to manage the risks identified in their TRAs. For each high security site LCH that does not currently list N290.7 [1] as a licensing basis publication for compliance verification, the CNSC proposes that N290.7 [1] be established as a licensing basis publication in the compliance verification criteria section of the facility's LCH. This will make implementation of an N290.7-compliant cyber security program mandatory.

The CNSC would like to know:

Q16. For HSS licensees affected by the proposed requirement to implement an N290.7-compliant cyber security program at your facility, would this requirement be appropriate? If not, what cyber security requirements would be appropriate and why?

7. Potential Cyber Security Requirements and Guidance for Protection of Facilities (Including Research Reactors) Having Category III Nuclear Material, and Class IB Accelerators

The following section applies to licensees listed in table 2. The proposed changes to the NSR would require that these sites assess their vulnerability to cyber threats and that cyber threat be included in licensees' TRAs. The objective of this proposed requirement is to ensure that licensees are able to detect and respond to cyber attacks targeting sensitive information, including prescribed information, and systems performing functions important to nuclear safety, security, emergency preparedness and safeguards. As a result of this proposed change, affected licensees will be required, as part of their overall security program, to develop a cyber security program and measures to manage the risks identified in their TRAs.

CNSC staff and representatives from the Canadian industry co-authored the N290.7 [1] which addresses "cyber security at nuclear power plants and small reactor facilities for the following computer systems and components:

(a) systems important to nuclear safety;
(b) nuclear security;
(c) emergency preparedness;
(d) production reliability;
(e) safeguards; and

(f) auxiliary assets or systems, which, if compromised, exploited, or failed, could adversely impact item (a), (b), (c), (d) or (e)"

N290.7 [1] is based upon the cyber security principles described in section 5, and given the scope of the standard, the CNSC considers it reasonable that the standard could be applied using a graded approach for the licensees listed in table 2.

The CNSC would like to know:

Q17. Would the elements set out in the standard be suitable for the licensees listed in table 2 in section 1.1, such as small nuclear reactor facilities, fuel processing facilities, fuel conversion facilities and Class IB accelerators if it is applied using a graded approach and licensees can propose alternative methods, approaches, security measures, etc.? If not, what would be suitable?

Q18. Do you agree with the proposed requirement of the implementation of a cyber security program for all licensees who conduct activities with Category III nuclear material? If not, why?

8. Potential Cyber Security Requirements and Guidance for Nuclear Substance Licensees

This section applies to category 1 and 2 sealed sources including the representative activities in table 3.

8.1 Potential cyber security requirements and guidance for the protection of physical protection systems

Licensees are responsible for implementing physical security measures to prevent the unauthorized removal of sealed sources and/or nuclear material and to prevent sabotage of licensed activities.

Physical security measures (e.g., digital cameras, alarms, motion detectors, forced entry detection, communication systems, etc.) are no longer exclusively hardwired, standalone devices; they are often digital devices and are increasingly connected by computer networks. They may be monitored remotely to allow for the timely assessment of potential incidents and the dispatch of on-site and off-site security responders such as security guards and police officers. Telephone systems are also increasingly relying upon digital technologies as copper landlines are being replaced by voice-over internet protocol telephones.

Adversaries can potentially use cyber attacks to compromise digital technologies to alter their function or performance. Where these technologies are used in physical protection systems, they provide an adversary with additional possibility when planning a malicious act targeting radiological material. For instance, in a blended attack, an adversary might perform a cyber attack to degrade a physical protection system in order to increase the chance of successfully stealing a sealed source or radiological material or to gain unauthorized access to the facility.

For example, an adversary might use cyber attack to:

- access an entry control system to obtain PIN codes for keyless locks
- transmit an old video stream from a digital camera to the central and remote monitoring stations or freeze the image sent from the camera

- modify an intrusion detection system to disable alarms to prevent them from being sent to the central and remote alarm stations

Based on these possibilities, the CNSC considers it reasonable to expect that licensees required to implement physical protection systems verify if their physical security measures, including their monitoring station(s), are vulnerable to cyber attack and to expect that these licensees will protect their physical protection systems. Given that vulnerabilities can vary among licensees and systems, it would be difficult for the CNSC to provide prescriptive requirements for each licensee to accomplish this objective. Therefore, the CNSC would prefer to apply a performance-based approach to mitigate the adverse effects of cyber attacks. The performance based requirements would be defined in additional guidance provided in the REGDOC-2.12 series.

The CNSC may require that licensees be responsible for demonstrating how they have achieved this objective to the best of their abilities by providing the CNSC with evidence that supports their claims. All evidence supporting their security case would be required to be from reputable sources that the CNSC could verify. In circumstances where experimental or novel approaches are used, the evidence provided should be replicable.

The CNSC may also require that the licensees implement industry best practices for cyber security to protect their physical protection systems against cyber attack. An example of good practices for radioactive source users is provided in the National Nuclear Security Administration's (NNSA) Office of Radiological Security *Cybersecurity Best Practices for Users of Radioactive Sources* [31].

The following documents may serve as potential expectations and/or guidance for the protection of physical protection systems

- N290.7, *Cyber Security for Nuclear Power Plants and Small Reactor Facilities* [1]
- NNSA Office of Radiological Security, *Cybersecurity Best Practices for Users of Radioactive Sources* [31]
- NNSA Office of Radiological Security, *Cybersecurity Procurement Requirements for ORS-Provided Security Systems* [32].

Note: Licensees may subcontract the design and installation of their security systems, measures, and response to third-party vendors. For these situations, the CNSC may consider it reasonable to require that licensees would be able to demonstrate that the contractor has implemented means to prevent cyber-intrusion and can maintain the continuous functionality of the security measures it has installed on the licensees' behalf.

The CNSC would like to know:

Q19. What measures have you implemented to protect your physical security measures from cyber attack?

Q20. Can you identify any impacts that would result should the CNSC require you to implement measures to protect your physical security measures (including the central monitoring station) from cyber attack?

8.2 Potential cyber security requirements and guidance for safety, emergency preparedness and safeguards

A graded approach is an important component of security risk management. The stringency of the security measures should be commensurate with the risk of compromise of computer-based systems performing or supporting safety, emergency preparedness and safeguards functions.

With that in mind, the CNSC is determining regulatory requirements and guidance that would be appropriate for the representative activities identified in table 3. The CNSC intends to put requirements and guidance for the application of cyber security measures for safety, emergency preparedness and safeguards systems. These requirements would be defined in additional guidance provided in the REGDOC-2.12 series.

The proposed steps to establish and maintain the cyber security measures are:

1) Review and identify all systems, functions, auxiliary systems, or devices that, if compromised by cyber attack, would result in adverse consequences. Adverse consequences include any release that could affect the health of workers or the public, or that could damage the environment. Patient safety, as regulated by Health Canada, is considered out of scope as an adverse consequence.
2) Identify all threats to the systems, devices or functions identified in the previous step. Sources of threats are available publicly and privately, and include the Canadian *National Cyber Threat Assessment* [33] produced by the Canadian Centre for Cyber Security.
3) Quantify the threats to the greatest extent possible by assessing the likelihood of the threat occurring, and quantifying the impacts. All impacts (both radiological and non-radiological) should be identified. In this step, licensees should also identify any vulnerabilities associated with the systems it has in place as well as any existing security measures.
4) Implement corrective actions to remove vulnerabilities or implement cyber security measures to address the risks and vulnerabilities identified in the previous step.
5) Develop an incident response capability to detect cyber-attacks, respond to them, develop lessons learned, implement corrective actions, and provide reports to the CNSC. The requirements for incident response will be similar to those provided for information security in section 3.5.
6) Regularly review the effectiveness of cyber security measures, implement changes, and document and communicate changes as required.

Operational technologies (OT) are hardware and software that monitor, communicate or control the physical world (i.e., industrial process systems and equipment). These technologies may be used to provide for functions important to nuclear safety, nuclear security, emergency preparedness and safeguards. Compromise of OT may result in damage to systems or equipment, failure to detect an unsafe condition, or otherwise affect the designed functions. The methods and measures used to provide for cyber security of OT are different from those used in information technology (IT).

The following documents may serve as potential expectations and/or guidance for the protection of OT systems:

- N290.7, *Cyber Security for Nuclear Power Plants and Small Reactor Facilities* [1]
- NIST: SP 800-82, *Guide to Industrial Control Systems Security*

Additional security measures may be required based on the unique operations, threats and risks faced by each licensee.

The CNSC would like to know:

Q21. Do you believe that the Baseline Cyber Security Controls for Small and Medium Organizations IT systems by the Canadian Centre for Cyber Security is appropriate for your organization's licensed activities? Why or why not?

Q22. Do you agree with the steps to establish and maintain the cyber security measures suggested in section 8.2? Why or why not? What method do you currently use (or recommend be used) to establish cyber security measures?

Q23. What impacts would these potential requirements and guidance have on your licensed activities?

Q24: Which cyber security standard do you use (or recommend be used) for your OT systems that support safety, emergency preparedness and safeguards?

Q25: For activities involving patient safety, do other regulatory bodies specify cyber security requirements and, if so, what requirements do they specify?

9. Potential Cyber Security Requirements and Guidance for Entities Who Transport or Arrange the Transport of Nuclear Material or Sealed Sources

This applies to entities who transport or arrange the transport of:

1) Category I, II and III nuclear material
2) Category 1 and 2 sealed sources.

The U.S. Department of Homeland Security, Customs and Trade Partnership against Terrorism has published guidance on its website for security various modes of transport. This guidance includes cyber security guidance. For example, section 4 of *Minimum Security Criteria – Highway Carriers* [35], contains possible cyber security measures applicable to highway carriers.

9.1 Potential cyber security requirements and guidance for entities who transport or arrange the transport of Category I, II and III Nuclear Materials

For Category I and II nuclear materials, the transport security plan (TSP) defines requirements for security measures and communications. Where these requirements are met using digital technology, the TSP should include cyber security measures. Where communications involves transmittal of information in digital form, information security should be applied to assure the confidentiality, integrity and availability of the digital information.

Licensees arranging the shipment of Category I, II and III materials have requirements for cyber security and information protection programs defined in previous sections of this discussion paper. The CNSC proposes that these programs should be applied to manage the cybersecurity and information protection measures within the TSP. The CNSC proposes that these programs include elements that address situations where the transportation is procured as a service from a third-party.

The CNSC would like to know:

Q26. Do you think that the cyber security measures contained in the referenced CPAT guidance would be appropriate for your organization? If not, why not? What additional or alternate measures would you recommend?

Q27. Do you agree with the CNSC's proposal that licensees should manage cyber security for transport within their cyber security and information security programs? If not, how do you suggest cyber security and information security for transport be managed?

9.2 Potential cyber security requirements and guidance for entities who transport or arrange the transport of Category 1 and 2 Sealed Sources

For Category 1 and 2 sealed sources, a transport security plan (TSP) defines the requirements for security measures and communications. For Category 2 sealed sources, a generic TSP is used.

The CNSC proposes that TSPs should include measures to:

1) Protect physical security measures that rely upon digital technology (if any) against cyber attack,
2) Protect the confidentiality, integrity and availability of prescribed information and other sensitive information,
3) Protect the confidentiality, integrity and availability of digital communications channels.

The CNSC proposes that the procurement process should include elements that address situations where the transportation is procured from a third-party.

The CNSC would like to know:

Q28. Do you think that the cyber security measured contained in the referenced CPAT guidance would be appropriate for your organization? If not, why not? What additional or alternate measures would you recommend?

Q29. Do you agree with the CNSC proposal that the TSP should include measures to protect prescribed information and other sensitive information, digital communications and physical security measures which rely upon digital technology?

Appendix A: Examples of Nuclear Information and Recommended Classification Level

Adapted from: IAEA Nuclear Security Series No. 23-G, Appendix II

Category	Document type	Description	Sensitivity	Recommended Classification
Plans	Facility security plan	They typically contain detailed descriptions of the security measures in place at a site and precise detail of where within the site material is stored. For nuclear facilities, the plans also contain details of other areas essential to the operation of the site. For high-security sites these are classified as secret.	Sensitive	Confidential up to Secret
Security Reports	Reports from security surveys, inspections and assessments and other reports on the physical protection or technical security measures employed at a site or facility	Access to these reports may provide adversaries with detail on the location of material, the measures taken to protect it and any assessed vulnerabilities there may be, thus assisting them to avoid security measures and controls.	Sensitive	Secret
	Reports describing critical features and/or highlighting requirements for security improvements, including at vital areas (if applicable)	Information of this nature could be of use to adversaries wishing to avoid security arrangements and could assist the targeting of a facility	Sensitive	Secret
	Results of security investigations at a site or facility, including those into leaks and losses of sensitive information	Information of this nature could be of use to adversaries wishing to avoid security arrangements and could assist the targeting of a facility.	Sensitive	Secret
	Reports describing vulnerabilities of the security management system and consequences of failure	Information of this nature could be of use to adversaries wishing to bypass security arrangements.	Sensitive	Secret
Construction Details	Details of construction and layout of locations where material may be stored or processed, including drawings or plans held on any media, showing features of physical protection relevant to the prevention of malicious acts	Official maps, chart or plans of sites may be released at the discretion of site management, provided they contain no description of the details of a building's functions, the materials stored within, and the location of internal security fences and the other security measures employed at the building. Classification depends upon the category/activity levels of materials in storage.	Sensitive	Up to Secret

Category	Document type	Description	Sensitivity	Recommended Classification
	Details of construction of vital areas at nuclear power plants and other nuclear facilities	Information of this nature can help adversaries to avoid security arrangements and could possibly assist the targeting for sabotage purposes.	Sensitive	Secret
Protection Systems	Details of any physical protection measures in use, for example alarms, surveillance cameras, access controls, security personnel, etc.		Sensitive	Secret
	The types and locations of intrusion detection system sensors and the associated surveillance cameras, including circuit diagrams, location of critical power supplies, cable runs, the maintenance and testing programmes for this equipment		Sensitive	Secret
	Details of automated access control systems, including the location of computer servers and backup servers and their power supplies	Any details of this nature would be of use to any adversary who wished to defeat the security systems at a facility.	Sensitive	Secret
	Stores: Security procedures for the issue, receipt and control of material stock; names of authorized key holders; arrangements for monitoring and guarding	Of potential use to adversaries planning malicious acts	Sensitive	Secret
	General maps showing the position and limits of a facility but without detail of what is contained within	Freely available Internet mapping applications show such information clearly.	Not Sensitive	Unclassified
	Other physical protection associated matters, e.g. location, set-up, manning and equipment at the central alarm station; location of the secondary alarm station; type of inner area barrier	Any details of this nature would be of great use to any adversary who wished to defeat the security systems at nuclear facilities.	Sensitive	Secret
Information Relating to Quantity and Form of Material	Information about the quantity, type and form of nuclear material, including sources, received or held in specified locations on all categories of site and nuclear power plant, including the exact locations where spent fuel is held	The type of information could be of use to adversaries choosing targets while planning attacks.	Sensitive	Secret

Category	Document type	Description	Sensitivity	Recommended Classification
	Throughput — nominal capacity, actual throughput and historical data on throughput of a facility under IAEA safeguards	Such high level information, especially for nuclear power plants, is released to the IAEA.	Not Sensitive	Unclassified
	Inventories, either national or local, of other radioactive material (including disused material), including the quantity, type, form and exact location	This type of information could be of use to adversaries choosing targets while planning attacks in order to steal radioactive material. Consideration should be given on which information is already publicly available with regard to such inventories. All such information may not be considered sensitive. Risk informed processes will help determine whether something should be designated as sensitive.	Sensitive	Unclassified
Material in Transit	Information on Category I, II, III movements of nuclear material	Such information could aid in choosing targets while planning malicious acts involving nuclear material in transit.	Sensitive	Secret
	High-security vehicles (HSVs): Visual access to interior of cab and cargo compartment; physical security features of vehicle design and construction; design and function of alarms, immobilization devices and key designs for special locks; load compartment keys, spare keys and combination lock settings, where used; vehicle tracking system if fitted to the HSV; system performance and communications	HSVs are vehicles specially designed to transport nuclear material securely. HSVs carry nuclear material and any information of the type listed in this section could be of use to an adversary planning an attempt to steal or sabotage nuclear material in transit.	Sensitive	Secret
	Nuclear material transit containers: Level of resistance of transport containers to attack by various means, Information on the design of specific containers (specially protected containers)	Useful to an adversary planning a sabotage attack with the aim of releasing nuclear material or planning the theft of the material during transport / Useful to an adversary planning a sabotage attack with the aim of releasing nuclear material or planning the theft of the material during transport.	Sensitive	Unclassified
	Specifications and design data on container	Information on the design of such containers without identification of construction details is often available on the Internet.	Not Sensitive	Unclassified

Category	Document type	Description	Sensitivity	Recommended Classification
	Transport packages: Information on the design of transport packages	Useful to an adversary planning a sabotage attack with the aim of releasing nuclear material or planning the theft of the material during transport	Sensitive	Unclassified
	Information on movements of other radioactive material	This type of information, particularly if concerned with the transport of powerful radiation sources, could be of use in planning a theft.	Sensitive	Unclassified
IT Systems and Computer Systems Important to Security and Safety	Details of IT systems storing and processing sensitive information, including the systems used for security purposes, system architecture, details of computer security measures employed and location of backup media	Information useful to an adversary planning a malicious act at a facility.	Sensitive	Secret
	Details of access control, intrusion detection systems, alarm monitoring systems, assessment and surveillance systems and other security functions and devices; and information on the location of backup hardware and software	Information useful to an adversary planning a malicious act at a facility.	Sensitive	Secret
	Details of safety-related IT systems or computer systems important to safety, including the locations, functions, upgrade routes, power supply and backup	Such systems have control and operational monitoring functions. Successful compromise of these systems could enable an adversary, at the least, to disrupt the operation of a facility, and in the worst case disruption could lead to a radioactive release.	Sensitive	Unclassified
Guard and Response Forces	Guard force at a facility: Overall establishment and the current capabilities of the force	Publicizing the existence of a force can reassure the public and potentially act as a deterrent. Note: Existence of a force not sensitive but capabilities of the force is sensitive and classified.	Sensitive	Secret
	Guard force at a facility: Establishment and current capabilities at particular sites	Information of this nature could be of use to any adversary in planning an incursion into a nuclear site for the purpose.	Sensitive	Secret
	Guard force at a facility: Numbers on any shift at a site		Sensitive	Secret
	Weapons and other special equipment available to the guard force and the number of trained users of firearms in the guard force individual sites	Any information that could help an adversary to estimate in advance the scale of response and the capabilities available in	Sensitive	Secret

Category	Document type	Description	Sensitivity	Recommended Classification
	Response force location, capabilities, weapons, special response vehicles and timings at a site	a tactical operational unit should be secured against disclosure.		Secret
	Deployment plans			Secret
	Escorts for nuclear material movements: Deployment and capabilities of the escort / Radio frequencies in use to enable communication with a response force or local police forces	Information could be of use to an adversary planning to attack a convoy.	Sensitive	Secret
Nuclear Material Accounting	Description: Statements of general material accounting principles	General principles of this type exist in the public domain.	Not Sensitive	Unclassified
	Description: Design information questionnaire and description, and location of material balance areas (MBAs) and key measurement points (KMPs)	Such detailed information on the location and quantities of nuclear material could be of use to an adversary planning a malicious act.	Sensitive	Unclassified
	Description: Physical and chemical form of material measurement at KMP		Sensitive	Unclassified
	Measurements and instrumentation data: Precision and accuracy of standard laboratory techniques	This information is often in the public domain.	Not Sensitive	Unclassified
	Measurements and instrumentation Data: Data which reveal the sensitivity of measurement or the alarm limits for material unaccounted for (MUF) at a particular plant	Precision and accuracy data relating to actual or typical measurements at sites, whether aggregated or disaggregated, could be of use to an adversary planning theft of material.	Sensitive	Unclassified
	Nuclear material flow and inventory data held on IT systems, in hard copy or on any form of storage medium	Information could reveal exact details of the location and movements of nuclear material.	Sensitive	Unclassified
	Material unaccounted for: Annual MUF figures for a site which does not reveal the MBA concerned	In many States, aggregated annual MUF figures are, or can be, published in the public domain.	Not Sensitive	Not applicable
	Material unaccounted for: MUF in MBAs or KMP		Sensitive	Unclassified
	Material unaccounted for: Details of investigations into particular MUF unless formally approved for release	However, detailed MUF figures or investigation results could be of use to an adversary in targeting a specific facility and therefore should be considered sensitive.	Sensitive	Unclassified May be higher depending on the specific nature of the source

Category	Document type	Description	Sensitivity	Recommended Classification
	Material unaccounted for: Limit of error for MUF or other specific indications of the uncertainty of MUF figures		Sensitive	Unclassified May be higher depending on the specific nature of the source
Licensing and Permissions Process Applications	Licensing and permissions process applications without detailed information on security measures; type, form and quantity of material	Content of such an application will vary depending on the legal and regulatory framework and the specific end use. If applications contain sensitive information that could be of potential use to an adversary, the application should also be treated as sensitive information.	Not Sensitive	Unclassified
	Licensing and permissions process applications containing detailed information on; e.g., security measures, and type, form and quantity of material	Content of such an application will vary depending on the legal and regulatory framework and the specific end use. If applications contain sensitive information that could be of potential use to an adversary, the application should also be treated as sensitive information.	Sensitive	Secret
Safety Cases, Engineering Documents and other Safety or Environmental Information	Safety cases of all classes: Details of the potential hazards or other information that could be used as a surrogate for evaluating the impact of a release, or details on the impacts of releases	While most information with regard to safety cases may be made public for transparency, some information may be considered sensitive with regard to nuclear security. Note: If any information does have nuclear security implications, it should be evaluated and marked on a case-by-case basis.	Sensitive	Unclassified
	Safety Cases of all classes: Details of strengths and weaknesses of processes, structures and protection systems designed to contain, control or secure nuclear material or other radioactive material	The type of detailed information contained in safety cases could be of use to an adversary for choosing targets and planning an operation.	Sensitive	Unclassified
	Safety Cases of all classes: Details of access to the production process, both physical access control and the removal of material from the process for control and monitoring purposes		Sensitive	Unclassified
	Contingency and response: Existence of a contingency and response plan	Publicizing the existence of plans can reassure the public and potentially act as a deterrent.	Not Sensitive	Unclassified

Category	Document type	Description	Sensitivity	Recommended Classification
Contingency and Response Plans and Exercises	Contingency and response: Detailed contents of a contingency and response plan	Details from the plan could indicate the capabilities, limitations and response times, and therefore be of use to an adversary in planning a deliberate attack.	Sensitive	Confidential
	Security contingency plans, including detailed information	Such documents contain information on the security measures in place, on the capabilities of the police or guard force contingents and on the likely response to a security incident.	Sensitive	Confidential
	Exercises: That an exercise is to take or has taken place	Publicizing the existence of exercises can reassure the public, provided that the level of detail would not assist an adversary, e.g. date/time/location of a future exercise.	Not Sensitive	Unclassified
	Exercises: Details of security exercises at a site including the scenario, which aspects of the security plan are being tested, whether a response force will be involved and the results of the exercise	Provides adversaries with information on the nature, size, capabilities and timing of response force reaction, detail of armed response force, nature of tactics employed and signal plan.	Sensitive	Confidential
	Exercises: Details of safety exercises	Safety exercises are often run in an open and transparent manner. They can typically be considered non-sensitive as long as they do not reveal detailed information on security measures.	Not Sensitive	Unclassified
Personal Information	Information from trustworthiness checks	Information of this nature could be used for blackmail or extortion. Most national privacy regulations will mandate the protection of this type of information.	Sensitive	Unclassified
	Information in personnel files			Unclassified
Radioactive Waste Inventory	General information about inventories that does not contain any information that could be exploited, e.g. the fact that waste is stored at a particular site, or aggregated quantities of waste without location	Such information is generally in the public domain and does not describe specifics of use to an adversary.	Not Sensitive	Unclassified
	Information that could be used in a malicious act or enables a specific building at a facility and the material held there to be identified	Such information provides targeting information for an adversary planning sabotage.	Sensitive	Unclassified Confidential when in combination with specific security details

Category	Document type	Description	Sensitivity	Recommended Classification
Decommissioning	Plans to decommission plant	Plans to decommission facilities are often publicly announced.	Not Sensitive	Unclassified
	Waste from decommissioning: That a store is to be built, and its location	This information is often in the public domain.	Not Sensitive	Unclassified
	Waste from decommissioning: Detail of the construction, security measures and quantity or type of material to be stored in new builds for the treatment and storage of waste and contaminated material arising from processing activities during decommissioning	This information can provide useful targeting information for an adversary planning sabotage attacks. Note: Security details and specifics on amount, type, and location of waste are confidential, the rest is likely unclassified.	Sensitive	Secret
Threat Assessments and Security Alerting Information	Threat assessments issued by the State, national security authorities or other competent authorities	Typically derived from national security material; e.g. national intelligence information. Note: If they actually contain detailed, sensitive information on national security, they may be rated higher, but derivative assessments should only refer to this material, not contain it.	Sensitive	Secret
	Details of the design basis threat	Typically derived from national security material, e.g. national intelligence information.	Sensitive	Secret
	Details of the vital area identification study	Could be of use to an adversary in identifying targets and carrying out an attack.	Sensitive	Secret
	Reasons for any security alert state in place and for any changes to it	Typically derived from national security material; e.g. national intelligence information.	Sensitive	Secret
Nuclear Technology	Detailed technical information about the production or processing of nuclear material (e.g. enriched uranium processing and reprocessing)	Information of this type could be of use to an adversary	Sensitive	Unclassified
	Designs or new technology submitted for licensing (e.g. advanced reactor technology, etc.)	Although details of these technologies may be made available to the public, it is possible that some detail of the design or technology could be of use to adversaries for planning purposes. Such information may be reviewed for sensitive information.	Sensitive	Unclassified

Category	Document type	Description	Sensitivity	Recommended Classification
	Detailed information that would assist in disassembly of devices to gain access to sources or would otherwise assist in defeating security measures	This information could be of use to an adversary attempting to remove radioactive material.	Sensitive	Unclassified
	Vulnerability studies of technology designs	Although academic studies may be publicly available, any detailed information exposing vulnerabilities that could be exploited by an adversary should be secured against unauthorized disclosure.	Sensitive	Unclassified
Historical Information	Historical information of current relevance and still sensitive, whether or not the information is classified	Information of this nature, although old, may still be of use to adversaries.	Sensitive	Unclassified

References

1. CSA N290.7 *Cyber security for nuclear power plants and small reactor facilities*
2. IAEA, *2015 IPPAS Mission Report to Canada*
3. CNSC, REGDOC 3.5.3: *Regulatory Fundamentals*
4. CNSC, REGDOC 2.12.3 : Security of Nuclear Substances: Sealed Sources and Category I, II and III Nuclear Material, Version 2
5. CNSC, *DIS-14-02, Modernizing the CNSC's Regulations and DIS-16-04, Small Modular Reactors: Regulatory Strategy, Approaches and Challenges*
6. CNSC, *What We Heard Report – DIS-14-02*
7. CNSC, *Stakeholder Workshop Report: Periodic Review of the Nuclear Security Regulations*
8. *Nuclear Safety and Control Act* (S.C. 1997, c. 9)
9. *General Nuclear Safety and Control Regulations* SOR/2000-202
10. CNSC, REGDOC-2.12.1, *High Security Facilities, Volume I: Nuclear Response Force, Version 2 (2018)* (Classified)
11. CNSC, REGDOC-2.12.1, *High-Security Facilities, Volume II: Criteria for Nuclear Security Systems and Devices (2018)* (Classified)
12. CNSC, REGDOC-2.12.2, *Site Access Security Clearance (2013)*
13. International Atomic Energy Agency (IAEA), NSS 23-G, *Security of Nuclear Information*
14. RCMP, Guide G1-009, *Transport and Transmittal of Projected and Classified Information*
15. Communications Security Establishment, *IT Security Risk Management: A Life cycle Approach* (ITSG-33) and its catalogue of security controls
16. National Institute of Standards and Technology (NIST), SP 800-53 Rev 5, *Security and Privacy Controls for Information Systems and Organizations*
17. International Organization for Standardization / International Electrotechnical Commission, ISO/IEC 27001, *Information Security Management*.
18. Canadian Centre for Cyber Security: *Sanitization and Disposal of Electronic Devices* (ITSAP.40.006)
19. Province of Ontario, *Information and Privacy Commissioner, Disposing of Your Electronic Media Technology Fact Sheet*
20. Cornell University, *Best Practices for Media Destruction* (webpage)
21. CNSC, REGDOC-3.1.1, *Reporting Requirements for Nuclear Power Plants*, Version 2
22. CNSC, REGDOC-3.1.2, *Reporting Requirements, Volume I: Non-Power Reactor Class I Facilities and Uranium Mines and Mills*
23. CNSC, REGDOC-3.1.3, *Reporting Requirements for Waste Nuclear Substance Licensees, Class II Nuclear Facilities and Users of Prescribed Equipment, Nuclear Substances and Radiation Devices*
24. NIST, SP 800-61, Rev 2, *Computer Security Incident Handling Guide*
25. IAEA, TDL-005, *Computer Security Incident Response Planning at Nuclear Facilities*
26. Public Safety Canada, *Developing an Operational Technology and Information Technology Incident Response Plan*
27. International Atomic Energy Agency (IAEA), NSS 17, *Computer Security at Nuclear Facilities*
28. Treasury Board Secretariat of Canada, *Directive on Security Management*

29. Public Services and Procurement Canada, *Contract Security Manual*

30. IAEA, NSS 33-T, *Computer Security of Instrumentation and Control Systems at Nuclear Facilities*

31. Office of Radiological Security, *Cybersecurity Best Practices for Users of Radioactive Sources*, January 2018. Retrieved from https://wins.org/wp-content/uploads/2020/09/ORS_Cybersecurity_Best_Practices_2019_digitalv2.pdf

32. Office of Radiological Security, *Cybersecurity Procurement Requirements for ORS-Provided Security Systems*, March 2018. Retrieved from: https://iiaglobal.com/wp-content/uploads/2019/09/ORS-Cybersecurity-Procurement-Requirements-030818.pdf

33. Canadian Centre for Cyber Security, *National cyber threat assessment 2020*

34. NIST, SP 800-82 Rev 2, *Guide to Industrial Control Systems Security*

35. U.S. Department of Homeland Security, Customs and Trade Partnership, *Minimum Security Criteria – Highway Carriers*

Additional Information

1. Treasury Board of Canada, *Standard on Security Screening*
2. NIST, *Glossary of Key Information Security Terms*