Canada's Nuclear Regulator

Proposals to Amend the REGDOC 2.12 Nuclear Security Series

Discussion Paper DIS-22-02

November 2022

Canadian Nuclear Safety Commission
Commission canadienne de sûreté nucléaire

Canada

Proposals to Amend REGDOC 2.12 Nuclear Security Series
Discussion paper DIS-22-02

Également publié en français sous le titre : DIS-22-02 Propositions de modification de la série de REGDOC 2.12

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 St
PO Box 1046 Stn B
Ottawa ON K1P 5S9

Tel.: 613-995-5894 or 1-800-668-5284 (in Canada only)
Fax: 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
November 2022

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 highlights 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 under the *General Nuclear Safety and Control Regulations* and the *Nuclear Security Regulations* (NSR).

The CNSC is revising the nuclear security regulatory documents (REGDOC 2.12 Nuclear Security Series) to align with the proposed changes to the *Nuclear Security Regulations* (NSR).

The purpose of this discussion paper is to gather feedback from licensees, proponents, the Canadian public, Indigenous peoples and other stakeholders on the proposed changes to the REGDOC 2.12 Nuclear Security Series. The feedback received during this consultation will inform the CNSC's approach to revising the REGDOC 2.12 Nuclear Security Series.

1. Introduction

The *General Nuclear Safety and Controls Regulations* and the NSR define the nuclear security requirements (i.e., protecting prescribed information, preventing unauthorized removal of nuclear substances and the sabotage of nuclear facilities and nuclear substances) for nuclear facilities that produce, process, use, store and/or transport Category I, II and/or III nuclear material and for the nuclear facilities listed in Schedule 2 of the *Nuclear Security Regulations* (NSR).

The NSR are currently supported by the following four nuclear security REGDOCs:

a) REGDOC-2.12.1, *High Security Facilities, Volume I: Nuclear Response Force, Version 2* (2018) (Classified)
b) REGDOC-2.12.1, *High-Security Facilities, Volume II: Criteria for Nuclear Security Systems and Devices* (2018) (Classified)
c) REGDOC-2.12.2, *Site Access Security Clearance* (2013)
d) REGDOC-2.12.3, *Security of Nuclear Substances: Sealed Sources and Category I, II and III Nuclear Material, Version 2.1* (2020)

The CNSC has yet to publish a REGDOC relating to cyber security or the protection of information. The CNSC intends to develop a standalone REGDOC within the REGDOC 2.12 Nuclear Security Series to provide guidance and expectations relating to cyber security; however, it is undecided whether expectations and guidance relating to information protection would be best suited within this REGDOC or elsewhere in the REGDOC 2.12 Nuclear Security Series. Nonetheless, Section 2.5 of this paper will outline the projected contents of the new cyber security REGDOC and the CNSC's projected expectations surrounding the protection of information.

Please note that the CNSC will also explore declassifying REGDOCs 2.12.1, Volumes I and II and realigning content throughout the entire REGDOC 2.12 Nuclear Security Series to promote clarity, reduce duplication of information and to ensure that the series remains fit for purpose.

Interested parties will be able to review and comment on the proposed changes to the REGDOC 2.12 Nuclear Security Series, including the new cyber security/protection of information document, during the normal consultation period.

1.1 Scope

This paper will outline the anticipated changes to the REGDOC 2.12 Nuclear Security Series in order to complement the proposed amendments to the NSR. The projected changes were derived from the comments received from the following two discussion papers as well as those received during the consultation sessions held with stakeholders throughout 2021:

- DIS-21-02, *Proposals to Amend the Nuclear Security Regulations,* which outlines the proposed amendments to the NSR.
- DIS-21-03, *Cyber Security and the Protection of Digital Information,* which provides details regarding the proposed changes to the requirements and guidance for cyber security and the protection of digital information.

2. Updates and additions to existing REGDOC 2.12 Nuclear Security Series

2.1 REGDOC-2.12.1, *High Security Facilities, Volume I: Nuclear Response Force, Version 2*

2.1.1 Updates to and enhancements of existing content

The CNSC intends to enhance and update REGDOC-2.12.1, Volume I to clarify:

- the minimum qualifications and equipment required for all on-site security personnel, including contractors
- the requirements surrounding the use of various combinations of response forces (on and off site) to respond to acts of sabotage and unauthorized removal of nuclear material
- the roles, responsibilities, equipment and training required for the off-site response forces expected to make and/or support an effective on-site intervention
- that secure and constant communication must be maintained between the licensee and the off-site response force
- how to plan, conduct, evaluate drills and exercises

2.1.2 Introduction of new elements

The current NSR requires that high-security sites (HSS) have an on-site armed nuclear response force that can execute an effective intervention to prevent theft and sabotage against the Design Basis Threat (DBT).

In the proposed amendments to the NSR, the CNSC proposed to revise the definition of "effective intervention" to allow for "…nuclear security measures, including detection, delay or response, or any combination thereof that are timely and powerful enough to prevent a sabotage event or the unauthorized removal of nuclear material or nuclear substances." By implementing this change, licensees will have greater flexibility as to how they produce an effective intervention.

Applicants and licensees will be required to test and demonstrate to the CNSC that the combination of measures they have proposed and implemented in their nuclear security system (i.e., systems, structures and/or components for security by design) will prevent a sabotage event or the unauthorized removal of nuclear material or nuclear substances.

2.2 REGDOC-2.12.1, *High-Security Facilities, Volume II: Criteria for Nuclear Security Systems and Devices*

2.2.1 Updates and enhancements to existing content

The CNSC intends to update the content of REGDOC-2.12.1, Volume II to align with the performance-based requirements set out in the proposed NSR. The updated content will maintain the current baseline criteria to measure and evaluate the performance objectives for each security measure deployed at HSS and use more technology-neutral requirements, where applicable.

The following examples illustrate the proposed changes:

Example 1: Barriers enclosing the Protected Area
Specific fence heights and robustness characteristics will be removed. This will allow applicants and licensees to propose alternative measures, designs, etc., to deter and delay potential intruders until such time that an intervention can be made and to maintain overall defence in depth for the site. Applicants/licensees will be required to demonstrate the effectiveness of their design and how it satisfies the performance objectives.

Example 2: Nuclear security measures in the Central Alarm Stations (CAS)
In the current iteration of REGDOC-2.12.1, Volume II, Security Monitoring Rooms must be located in the protected area and staffed with a Nuclear Security Officer. REGDOC-2.12.1, Volume II will be amended to permit applicants and licensees to use trained and qualified security personnel as CAS operators; and the CAS itself can be located outside the protected area if the applicant or licensee meets certain conditions and requirements.

In addition to the above, the CNSC intends to reinforce the current requirement that on-site security measures be actively managed in accordance with the preventative maintenance concepts established in REGDOC-2.6.2, *Maintenance Programs for Nuclear Power Plants*.

2.2.2 Introduction of new elements

The CNSC intends to introduce the following guidance and expectations in REGDOC-2.12.1, Volume II regarding the new regulatory requirements for the CAS:

- securing two-way communication between the CAS and on- and off-site response forces
- recording communications between the CAS and on- and off-site response forces
- staffing of the CAS, specifically how to meet the new two-person rule and establish that the licensee may propose equally effective alternatives that would achieve the same objective
- considering cyber-attacks in threat and risk assessments (TRA) for the CAS

In addition to the above, the CNSC plans to enhance REGDOC-2.12.1, Volume II to:

- clarify the importance of using security principles early in the design phase and promote recognized security-by-design approaches to protect nuclear material and nuclear substances
- clarify how to adequately identify and protect vital areas at HSS. Licensees will be responsible for outlining in their security program how they define the boundary of vital areas and how they intend to protect (i.e., security measures and tactical deployment plans) each vital area against threats identified in the DBT
- expanding the section on key controls to include other access control measures that are used at HSS (e.g., access card, proximity devices, biometric devices)

2.3 REGDOC-2.12.2, *Site Access Security Clearance*

2.3.1 Updates to existing guidance

REGDOC-2.12.2, *Site Access Security Clearance* will be updated to provide guidance for all nuclear facilities subject to the NSR that are required to implement Site Access Security Clearance (NSR section 17) or a facility access security clearance (NSR section 42).

2.3.2 Introduction of new elements

The CNSC will include new guidance to expand on the tiered model suggested in the Standard on Security Screening (SSS) sections Site Access Status, Site Access Clearance and Enhanced Site Access Clearance (see table below). Licensees will be responsible for assigning the appropriate level to their employees, workers, contractors, etc. and conducting the appropriate checks.

Proposed Tiered Model to be Inserted into REGDOC-2.12.2, Version 2			
Screening Type	**Site Access Status** *(Previous NSR S.42 facility access security clearance)*	**Site Access Security Clearance** *(Previous NSR S17)*	**Enhanced Site Access Clearance** *(Previous NSR S18.1)*
Applicable facilities	**Nuclear facility** subject to the NSR	**HSS**	**HSS**
Access provided	Unescorted access to nuclear facility	Unescorted access to **protected area**	Access to **vital areas** or **inner areas** and security personnel[1]
Verification of background information, education history, professional qualifications, employment history and character references	5-year background information	5-year background information	10-year background information
Validity period	up to 10 years	up to 10 years	5 years
Verification of identity	Mandatory		
Law enforcement inquiry (criminal record check) or fingerprinting	Mandatory Note: Fingerprinting is mandatory under SSS		
Government of Canada Security Assessment	N/A	Mandatory	
Financial inquiry (credit check)	Recommended Note: mandatory under SSS		Mandatory

In addition to the above, the CNSC intends to incorporate and provide new guidance on the following elements of the SSS:

- using open-source information during security screening and aftercare activities
- conducting aftercare activities as defined in Appendix F of the SSS (i.e., conducting security briefings and awareness sessions, security training, etc.)

[1] "Security personnel" will include nuclear security officers, nuclear security support persons, central alarm station operators and their supervisors. This term also includes personnel who have access to prescribed information, who maintain and repair nuclear security systems or devices and who perform security clearance, intelligence, firearms maintenance or security training work.

2.4 REGDOC-2.12.3, *Security of Nuclear Substances: Sealed Sources and Category I, II and III Nuclear Material, Version 2.1*

2.4.1 Updates to existing requirements and guidance

The CNSC intends to update Part A of REGDOC-2.12.3:

- to clarify the aggregation concept– specifically regarding how to aggregate multiple and different radioactive sources for the purpose of identifying the appropriate security level and assignment of security measures
- to clarify security expectations and provide examples of good practices for sealed sources that are used and stored at HSS
- to note that applicants and licensees are required to notify the CNSC of final transportation plans 48 hours before the shipment will be removed

The CNSC intends to update Part B of REGDOC-2.12.3:

- to include new cyber security and information protection requirements/guidance for nuclear facilities subject to the NSR. See section 2.5 for more guidance
- to clarify the requirements for escorts and security arrangements to ensure that shipments are appropriately protected at all times and that an effective intervention can be provided to ensure the prevention of theft and sabotage during transport

2.4.2 Introduction of new elements

The CNSC intends to update Part A of REGDOC-2.12.3 with new guidance:

- regarding the use of security zones to protect sealed sources
- recommending the hardening of security measures deployed by the licensee to ensure they remain effective
- referring to the new REGDOC on cyber security and provisions relating to the protection of sensitive information, which will allow licensees to protect their site security plan and to implement cyber security best practices

The CNSC intends to update Part B of REGDOC-2.12.3 with the following new guidance:

- how to conduct a TRA for a nuclear facility
- how to implement an effective safety and security interface
- how to implement an effective interface between nuclear material accountancy and security measures
- how to support and promote security culture measures
- how to conduct and evaluate security exercises for nuclear facilities subject to the NSR, which will also include guidance for carriers and freight forwarders that transport category I, II and III nuclear material

In addition to the above, the CNSC intends to include provisions:

- requiring licensees to use armed response forces and escorts for the transport of Category I and II nuclear material or to make appropriate arrangements with local police forces that have jurisdiction and/or other armed response capabilities in circumstances where armed response forces and escorts cannot be made available by licensees
- providing licensees the opportunity to develop and present transport security plans that make use of alternative technologies and features that offer security by design in all aspects of deterrence, detection, delay, denial and response
- establishing cyber security and information protection requirements and guidance for all applicable licensees (As previously stated, all cyber-security related content is expected to be located within the new standalone cyber security REGDOC; however, the CNSC is currently analyzing the entire REGDOC 2.12 Nuclear Security Series to determine the appropriate location for information protection expectations.)

2.5 Cyber security and protection of sensitive information

As previously mentioned, the CNSC plans to detail its requirements and guidance for cyber security and the protection of information in a new REGDOC. This document will be available for consultation in 2023 alongside the redrafted REGDOC 2.12 Nuclear Security Series.

The sections below outline the CNSC's proposed approach to cyber security and the protection of information.

2.5.1 Introduction of new elements

2.5.1.1 Cyber security for HSS

The CNSC intends to include the following elements for HSS licensees:

- cyber security information in the licensee's TRAs regarding all computer-based systems and components that uphold or impact nuclear safety, nuclear security, emergency preparedness and safeguards
- guidance for conducting a cyber security TRA
- requirement to design, implement and maintain a cyber security program in accordance with the CSA Group standard CSA N290.7 (entitled "Cyber security for nuclear power plants and small reactor facilities" in the 2014 version of the standard, CSA N290.7-14, and "Cyber security for nuclear facilities" in the 2021 version, CSA N290.7:21)

2.5.1.2 Cyber security for non-HSS licensed activities subject to the NSR

The CNSC intends to include the following elements for research reactors and class IB nuclear facilities subject to the NSR:

- cyber security information in the licensee's TRAs regarding all computer-based systems and components that uphold or impact nuclear safety, nuclear security, emergency preparedness and safeguards
- guidance for conducting a cyber security TRA
- requirement to design, implement and maintain a cyber security program using a risk-informed, graded approach

2.5.1.3 Cyber security for entities that transport or arrange the transport of Category I, II, or III nuclear material

The CNSC intends to include the following elements for licensees and entities that transport category I, II or III nuclear material:

- cyber security information in the TRA that forms the basis for the transport security plan, including information regarding any computer-based systems and components that are relied upon to uphold or that impact nuclear safety, nuclear security, emergency preparedness and safeguards during transport
- guidance on the cyber security aspects to be included in a transport security plan, including industry best practices

2.5.1.4 Cyber security for category 1 and 2 nuclear substance licensees that are not subject to the NSR

For licensees that are not subject to the NSR and that hold licences to possess, use and store category 1 and 2 nuclear substances, the CNSC plans to include in the REGDOC 2.12 Nuclear Security Series risk-informed requirements and guidance for the cyber security measures to be implemented by licensees, based on industry best practices.

2.5.1.5 Cyber security for entities that transport or arrange the transport of category 1 or 2 nuclear substances

For licensees and entities that transport category 1 and 2 nuclear substances, the CNSC plans to include the following elements in the REGDOC 2.12 Nuclear Security Series:

- a requirement that licensees and entities include in their transport security plans cyber security and all computer-based systems and components that uphold or impact nuclear safety, nuclear security, emergency preparedness and safeguarding functions
- guidance on the cyber security aspects to be included in a transport security plan, including industry best practices

2.5.2 Protection of sensitive information

As communicated in its pre-consultation activities, the CNSC plans to include in its proposed amendments to the NSR the following elements:

- a definition of sensitive information, similar to that provided in DIS-21-03: "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"

- a requirement in the NSR for licensees to protect the confidentiality, integrity and availability of sensitive information against threats identified in their threat and risk assessment (TRA)

Based on these proposed requirements, the CNSC intends to expand the content of the REGDOC 2.12 Nuclear Security Series to state the following:

- access to sensitive information shall be restricted to those with a need-to-know (i.e., a demonstrable need to access the information to be able to perform their duties)
- TRAs must include threats that could lead to unauthorized disclosure, modification, destruction and/or denial of use of sensitive information
- The Nuclear Security Program must reference a program or process that ensures that sensitive information is protected throughout its lifecycle. This program or process must detail the measures the licensee has put in place to adequately protect, create, identify, classify, store, use, transmit and dispose of sensitive information. Security measures should be implemented using a graded approach based on the classification of the information. The program or process shall be integrated into the licensee's management system.

The planned additional content will also include the following elements:

- links to REGDOC-2.12.2, specifically ensuring that people with access to sensitive information have the appropriate site access status, site access clearance or enhanced security clearance
- references to the International Atomic Energy Agency, Government of Canada and American Society for Industrial Security resources to assist licensees to identify and protect sensitive information
- examples of nuclear information and recommended classification levels, similar to Appendix A, as set out in DIS-21-03, *Cyber Security and the Protection of Digital Information*

3. Future public consultations and how to provide feedback

Future public consultations with the nuclear industry, government departments and members of civil society may be held regarding the development of the REGDOC 2.12 Nuclear Security Series. Notification of these opportunities will be posted on the CNSC's online consultation platform at Let's Talk Nuclear Safety.

Interested parties will have the opportunity to comment on this paper either on Let's Talk Nuclear Safety or via email. In addition, interested parties will also have the ability to comment on the draft changes to the REGDOC 2.12 Nuclear Security Series through the normal REGDOC development process.