Canada's Nuclear Regulator

Proposals to Amend the Nuclear Security Regulations

Discussion Paper DIS-21-02

April 2021

Canadian Nuclear Safety Commission
Commission canadienne de sûreté nucléaire

Canada

Proposals to Amend the *Nuclear Security Regulations*
Discussion paper DIS-21-02

Également publié en français sous le titre : Modifications proposées au Règlement sur la sécurité nucléaire

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@canada.ca
Website: nuclearsafety.gc.ca
Facebook: facebook.com/CanadianNuclearSafetyCommission
YouTube: youtube.com/cnscccsn
Twitter: @CNSC_CCSN
LinkedIn: linkedin.com/company/cnsc-ccsn

Publishing history
April 2021 Draft Version 1.0

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 is proposing amendments to the *Nuclear Security Regulations* (NSR). The proposed changes to the NSR will take a performance objectives-based approach to regulating nuclear security by affording licensees greater flexibility in the measures and approaches they can use to meet the nuclear security regulatory requirements. Accordingly, the CNSC is also taking this opportunity to revise and align the nuclear security regulatory documents (REGDOC-2.12 series) to provide clear guidance on how nuclear security regulatory requirements can be met.

The purpose of this discussion paper is to gather feedback from licensees, proponents, the Canadian public, Indigenous peoples, and other stakeholders on the proposed amendments. All feedback received during this consultation will inform the CNSC's approach. Stakeholders will have additional opportunities to comment during the *Canada Gazette,* Part I, pre-publication process and when the regulatory documents are posted for public consultation.

Proposals to Modernize the Regulation of Nuclear Security

1. Introduction

The Canadian Nuclear Safety Commission (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.

The CNSC regulates nuclear security pursuant to the *Nuclear Security Regulations* (NSR) and the *General Nuclear Safety and Control Regulations* (GNSCR).

The NSR and GNSCR:

(a) Apply to nuclear facilities that produce, process, use, store and/or transport Category I, II and/or III nuclear material[1] and to nuclear facilities listed in Schedule 2 of the NSR.; and

(b) 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.

The NSR are currently supported by four nuclear security regulatory documents (REGDOCs) which provide guidance on how applicants and licensees may meet nuclear security regulatory requirements. The nuclear security REGDOCs are:

(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); and

(d) REGDOC-2.12.3, Security of Nuclear Substances: Sealed Sources and Category I, II and III Nuclear Material, Version 2.1 (2020).

2. Scope

The proposed amendments to the NSR described in this discussion paper will only apply to licensees and proponents who produce, process, use, store and/or transport Category I, II and/or III nuclear material as well as nuclear processing facilities that are listed in Schedule 2 of the current NSR. Licensees who produce, process, use, store and/or transport Categories 1 to 5 radioactive sources[2] are not in scope of the proposed amendments to the NSR and should reference REGDOC-2.12.3, *Security of Nuclear Substances: Sealed Sources and*

[1] Category I, II and III nuclear materials are currently defined in Schedule 1 of the NSR.
[2] Sealed sources categories are defined in REGDOC-2.12.3.

Category I, II and III Nuclear Material. No amendments to the GNSCR will be proposed as part of this project.

3. Pre-consultation activities to date

The CNSC had previously consulted stakeholders on plans to modernize the CNSC's regulations, including the NSR, via a 2014 discussion paper, DIS-14-02, Modernizing the CNSC's Regulations. 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.

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 security of nuclear facilities already in place or possible in the foreseeable future. Attendees were those directly responsible for implementing security measures at nuclear facilities and/or responsible for the security of nuclear and/or radioactive material, prescribed equipment and prescribed information, as well as designers of future reactor technologies.

Attendees provided comments on areas of the NSR where the CNSC was considering amendments, suggested additional areas where amendments could be considered, and, provided preliminary information on the impact of those potential amendments. CNSC published the results of the workshops in the *Stakeholder Workshop Report: Periodic Review of the Nuclear Security Regulations*.

The CNSC intends to conduct additional workshops in the spring of 2021 based on the proposals outlined in this paper. They 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 workshops will be provided in the coming months.

4. Desired outcome of the proposed amendments

In Canada, the licensee has the primary responsibility for safety and security. In our role as a nuclear regulator, the CNSC uses both *prescriptive* and *performance-based* regulatory approaches, taking into account the potential risks of the proposed activity or technology. Prescriptive regulations contain very specific provisions, provide little flexibility and are generally easier to monitor and enforce. However, prescriptive regulations may delay the implementation of improvements in safety due to their specific approach and limited recognition of alternatives.

Performance-based regulatory approaches are meant to provide flexibility for licensees to introduce new technologies, processes and procedures and, at the same time, allow the CNSC to adjust its requirements to improvements in science, technology, and safety. In addition, the direction from the Government of Canada's *Cabinet Directive on Regulation* and the Treasury Board of Canada's *Policy on Regulatory Development* is for regulators to consider performance-based regulations. In a performance-based approach, safety and security are never compromised. The proposed means of achieving a performance-based requirement *must* be approved by the CNSC and will require applicants and licensees to focus on achieving specific and measurable objectives or outcomes.

The current NSR utilizes both prescriptive and performance-based regulatory requirements. The evolution towards a more performance-based regulatory approach will continue under the proposed NSR. To that effect, the CNSC will continue to maintain clear nuclear security performance objectives for nuclear facilities where Category I, II and/or III nuclear materials are produced, processed, used, stored and/or transported and in other nuclear facilities currently listed in Schedule 2 of the NSR. In addition, the CNSC intends to introduce proposed amendments to the NSR that will remove, where practicable, prescriptive requirements for how and by what means nuclear security regulatory requirements must be met and implement performance-based requirements in their stead. Overall, the CNSC is seeking to recognize and respond to both new and evolving security threats and new technologies, systems and processes to address these threats, by allowing licensees flexibility to deal with these challenges *without compromising security objectives and maintaining the same, or higher, level of security*.

In order to implement this performance objective-based approach, definitions, terms and/or references in the NSR will be revised, added and/or removed as appropriate. Furthermore, the REGDOC-2.12 series will be updated to include technical requirements and additional guidance on how to meet the performance objectives.

During the licensing process, every applicant or licensee will still need to demonstrate that its approach continues to meet the nuclear security performance objectives through ongoing compliance verification activities during the licence period.

Specifically, it is proposed that:

(a) The current requirements prevent the unauthorized removal (i.e., theft) of Category I, II and III nuclear material and other radioactive materials remain in place. Furthermore, the prevention of unauthorized removal of Category I and II material from high-security sites will continue to be based on adversaries described in the Design Basis Threat Analysis (DBTA).

(b) The current requirement to prevent sabotage (as defined in the current NSR) by way of an effective intervention (as defined in the current NSR) will be revised. The proposed revised requirement will be to prevent radiological consequences stemming from the sabotage[3] of nuclear facilities or Category I, II or III nuclear material in use, transport or storage. For high-security sites and Category I and II nuclear material, this requirement will be subject to an adversary characterized by the DBTA.

(c) Prescriptive requirements related to the components of a nuclear security system, including prescriptive requirements for on-site and off-site armed response force arrangements, will be amended to allow for greater flexibility in the design of the overall nuclear security system in all aspects of deterrence, detection, delay and defence, or any combination thereof, in order to prevent radiological consequences from DBTA sabotage event(s). This will also include the possibility of relying entirely on engineered safety and security-by-design protection and containment systems when it can be demonstrated that those systems will

[3] The proposed revised definition of sabotage to be included in the NSR will be consistent with IAEA Nuclear Security Series No. 13 (INFCIRC/225/Revision 5): "Any deliberate act directed against a nuclear facility or nuclear material in use, storage or transport which could directly or indirectly endanger the health and safety of personnel, the public or the environment by exposure to radiation or release of radioactive substances."

ensure no radiological consequences will occur from a DBTA sabotage event(s) until such time an appropriate off-site response (if necessary) can effectively intervene.

(d) Licensees and proponents will be required to demonstrate to the CNSC that the combination of measures implemented in their nuclear security system to meet the requirements in (a) and (b) listed above are met and maintained through technical submissions.

5. Proposed changes to the regulations

5.1 Innovation and technological advances

Advancements and innovations in nuclear technology, as well as in technologies and methods for physical protection and cyber security, are expanding the range of measures and approaches through which licensees can design and operate their nuclear facilities in order to meet nuclear security regulatory requirements. Furthermore, these advancements and innovations offer opportunities for licensees and proponents to design nuclear facilities and/or implement concepts of operation that could potentially effectively eliminate vulnerabilities that licensees would otherwise have to consider in the design of the nuclear security systems of their respective facilities.

The proposed amendments will afford licensees and proponents greater flexibility in demonstrating how they can meet nuclear security regulatory requirements. This may include, but is not limited to, the application of traditional physical protection systems, including the use of on-site and/or off-site armed response forces, the use of alternative measures such as engineered systems and novel concepts of operation, safety and security-by-design containment systems, or any combination thereof.

For example, under the proposed changes to the NSR, licensees of high-security sites would be required to prevent the unauthorized removal of nuclear and other radioactive materials and ensure that there are no radiological consequences stemming from a DBTA sabotage event, but would no longer be required to implement prescribed components in their nuclear security systems, including the maintenance of an on-site nuclear response force (NRF).

Under the proposed NSR, the performance objective for sabotage will be that no radiological consequences can result from a DBTA sabotage event. This will expand the range of interventions that can be used by an operator, from the use of techniques, tactics and procedures and engineered systems for deterrence, delay, detection and/or response to protect against radiological releases from a DBTA sabotage event, or any combination of security measures thereof. To achieve this performance objective, applicants and licensees will be able to propose methods that employ novel technologies and concepts of operations, safety and security-by-design, the use of on-site armed response forces and/or arrangements with off-site armed response forces. Overall, and where practicable, the prescriptive requirements for how a nuclear system is to be designed will be removed and replaced with a performance-based requirement for a nuclear security system that will be required to ensure that no radiological consequences can result from a DBTA sabotage event.

The proposed amendments to the NSR would continue to ensure the appropriate level of security for all types of nuclear facilities, nuclear and radioactive materials, prescribed equipment and prescribed information that are subject to the requirements of the NSR in a manner that is consistent with Canada’s domestic laws and regulations and its international commitments. Furthermore, this would allow operators of existing nuclear facilities (including high-security

sites) to, where appropriate, modify their nuclear security systems to take advantage of alternative measures. At the same time, proponents and operators of new nuclear facilities (e.g., advanced reactors) will have greater flexibility to implement alternative measures and/or concepts of operation that could potentially eliminate vulnerabilities and therefore the need for certain measures in their respective nuclear security systems. This will allow for designers to take maximum advantage of the security-by-design concept.

5.2 Cyber security

The CNSC recognizes the novelty and complexity that cyber security considerations introduce into a nuclear security system, as both a threat vector and as an enabling solution to counter threats. Under the proposed amendments to the NSR, all licensees who produce, process, use, store and/or transport Category I, II and/or III nuclear material will be required to conduct a threat and risk assessment (TRA) that includes a cyber security component. Specifically, licensees will be required, as part of their overall nuclear security program, to develop a cyber security program to detect and respond to cyber attacks and/or cyber security compromises identified in their TRA. This would include compromises to the protection of prescribed information and the protection of operational technology that performs functions important to nuclear safety, security, safeguards and emergency preparedness.

Furthermore, and in alignment with the overall approach to nuclear security, licensees and proponents will be afforded flexibility in the design of their cyber security program in all aspects of deterrence, detection, delay and response, or any combination thereof, in order to meet the proposed performance objectives outlined in items 4 (a) to (d) of this discussion paper.

This activity is already being conducted at existing high-security sites and will be applied to other nuclear facilities, such as nuclear fuel facilities and nuclear substance processing facilities, using a graded approach. Additional information on the graded approach is found in REGDOC-3.5.3, *Regulatory Fundamentals*.

Lastly, in 2015, the IAEA conducted an International Physical Protection Advisory Service (IPPAS) 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 committed to reviewing the risks to its licensees and implementing requirements where necessary. The results of this review and the proposed way forward will be set out in a cybersecurity discussion paper, that will be issued in the near future. Interested parties will be able to comment on the discussion paper.

5.3 International obligations and alignment with good practices

Canada ratified the 2005 Amendment to the Convention on the Physical Protection of Nuclear Material (CPPNM/A) in December 2013. The CPPNMA contains 12 Fundamental Principles that are considered essential elements of a state's nuclear security regime. The proposed amendments to the NSRs to establish clear performance objectives while removing prescriptiveness in how said objectives can be met will maintain alignment with these principles.

In its 2015 mission report the IPPAS makes three recommendations and 30 suggestions to enhance Canada's nuclear security regime and framework. The CNSC considered the recommendations and suggestions and, on behalf of Canada, committed to:

(a) Enhancing the importance of nuclear security culture;

(b) Establishing a regulatory requirement for the conduct of transport security exercises at regular intervals;

(c) Implementing provisions for effective interfaces between nuclear security and nuclear material accountancy and control; and

(d) Extending cyber security requirements to other at-risk licensed activities.[4]

The proposed amendments to the NSR and associated REGDOC-2.12 series documents will consider these commitments.

6. Amendments to the *Nuclear Safety and Control Act* affecting nuclear security

The CNSC will develop and implement a revised regulatory framework to support proposed amendments to the *Nuclear Safety and Control Act* (NSCA) as a result of Bill C-21, which is currently under consideration by Parliament. These proposed amendments include:

(a) Expanded protections and authorities for NSOs (including NRF members) by granting them limited peace officer status. Their scope would be limited to the nuclear facility itself and to only those powers required to fulfill their duties and functions as defined by the NSR.

(b) Expansion of NSO duties to include the preservation and maintenance of the public peace at high-security sites.

(c) Permitting licensees who operate high-security sites to acquire, possess, transfer and dispose of prohibited and restricted firearms and special equipment used in the course of maintaining security at those sites. This will include the requirement to report inventories of prohibited and restricted firearms and special equipment to the Registrar of Firearms and to the CNSC.

(d) Establishment by the Commission of a framework for the designation of peace officers and for the suspension and revocation of peace officer designation.

(e) Establishment by the Commission of a framework for a complaints review process with respect to the conduct of NSOs and NRF members in the exercise of their powers or the performance of their duties and functions as peace officers.

The proposed amendments to the NSCA also provide an exemption to the proposed requirements listed above if the licensee is able to demonstrate, to the satisfaction of the Commission, that it does not require an on-site armed response based on the use of alternative security measures or security arrangements. This is consistent with the performance objectives being proposed in section 5.

[4] Refer to section 5.2 of this discussion paper for more information on the CNSC's cyber security proposals.

7. Conclusion

Licensees are responsible for operating in a manner that ensures there is no unreasonable risk to the health, safety and security of Canadians and the environment and for implementing Canada's international commitments on the peaceful use of nuclear energy. To that end, the CNSC is required to ensure that licensees make the necessary provisions for nuclear security. The proposed amendments to the NSR will ensure the continuity of Canada's robust nuclear security regime, while affording licensees and proponents greater flexibility in demonstrating how they can meet nuclear security regulatory requirements.

The CNSC intends to use the feedback received on this discussion paper to inform its approach to regulating nuclear security. Before incorporating any new requirements or guidance on nuclear security into its regulatory framework, the CNSC will provide stakeholders with further opportunities, including workshops, to provide additional feedback on any specific measures that might be proposed.

8. Questions

(a) What concerns or issues do you have with the overall proposed approach?

(b) What are your views, positive or negative, on our proposed transition, where practicable, from prescriptive to performance-based regulations?

(c) What are your views, positive or negative, on our proposed approach to cyber security?

(d) Do you see any unintended impacts on groups or individuals as a result of the proposed regulatory changes (e.g., unnecessary or restrictive requirements that could limit individual participation in a security system)?

(e) Are there key issues impacting nuclear security that you would like to propose for consideration that were not considered in this paper?