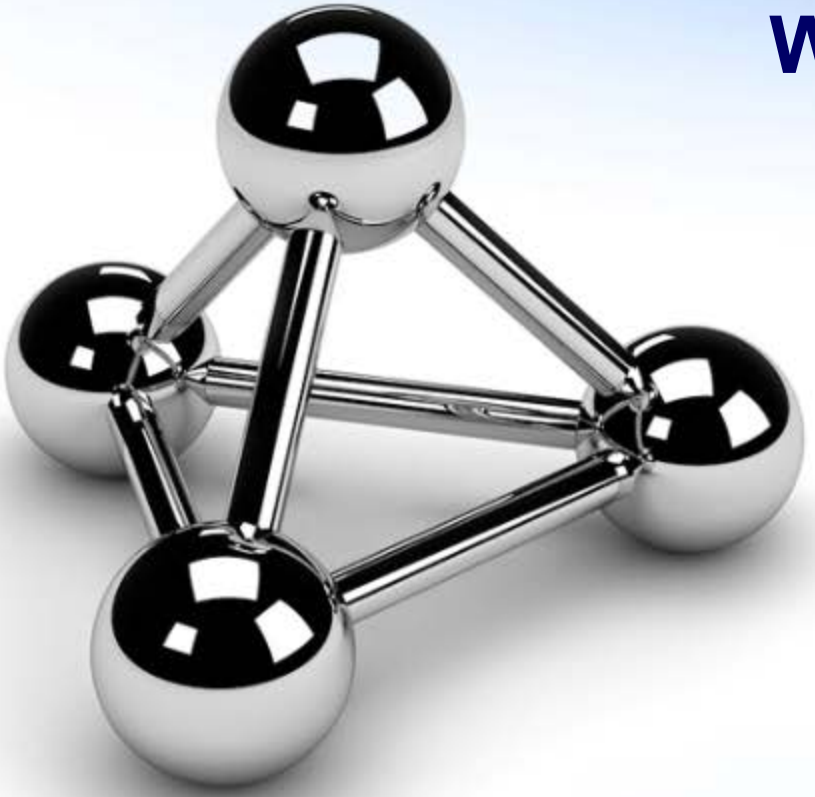
Canadian Nuclear Safety Commission
Commission canadienne de sûreté nucléaire



Workshop on Proposed Amendments to the *Nuclear Security Regulations*

Michael Beaudette
Director
Nuclear Security Division

October 12, 2016
e-Doc: 5054938

Canada

nuclearsafety.gc.ca

Focus of Today's Workshop

- Licensees currently listed in Schedule 2 of the *Nuclear Security Regulations*
  - Cameco, GE-Hitachi, Nordion, SRB Technologies
- Licensees who process, use and store Category III nuclear material
  - examples include Slowpoke Reactors, McMaster Nuclear Reactor
- Licensees and stakeholders who transport or arrange for the transport of nuclear material
  - examples include RSB Logistic, TAM International, Laurentide Forwarders Inc.

Today's Goals

- Provide an overview of several proposed amendments that CNSC staff is considering making to the *Nuclear Security Regulations* (NSR) and receive preliminary feedback from stakeholders

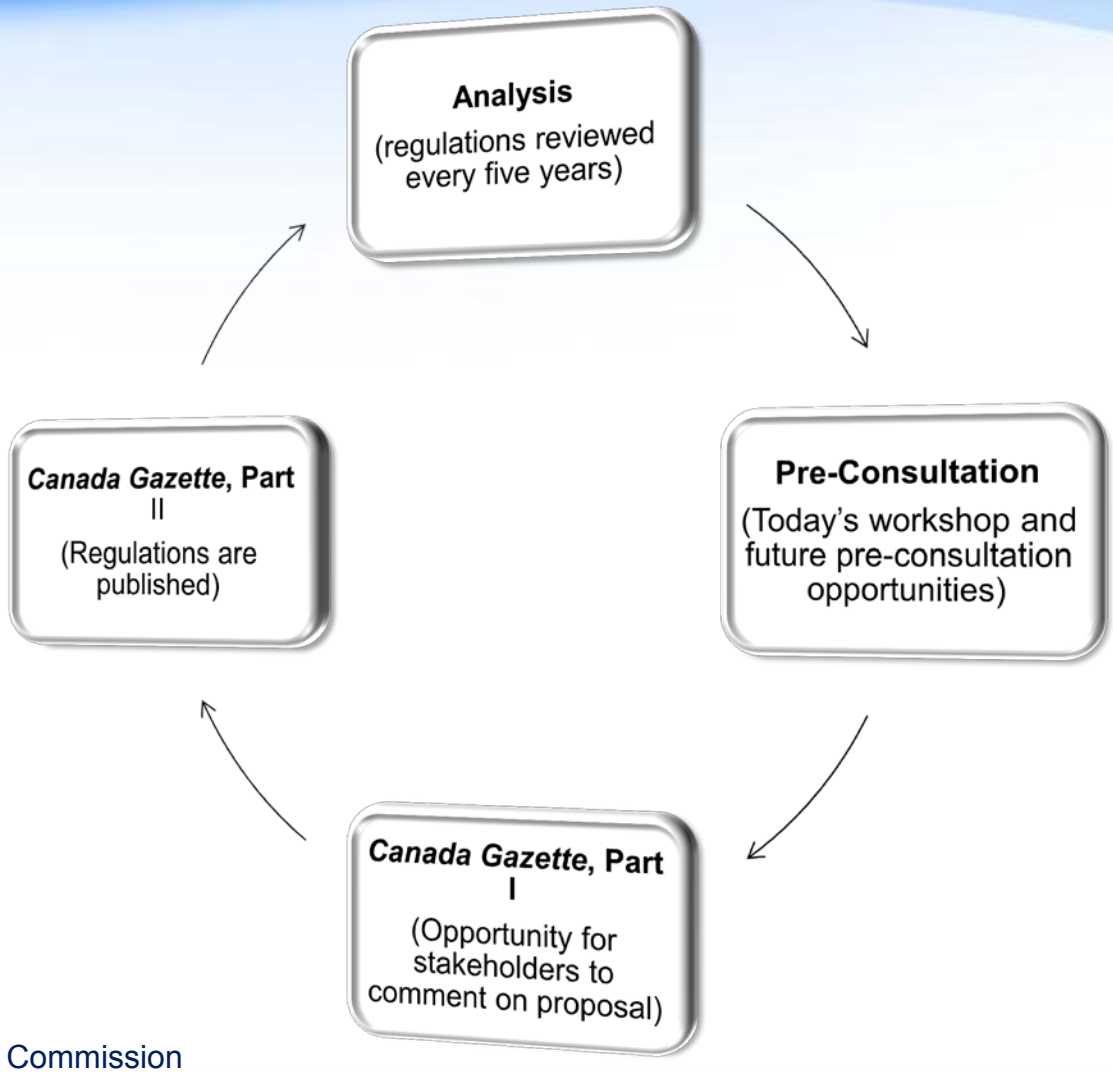
- Provide an opportunity for stakeholders to suggest additional areas for potential amendments to the NSR

Please note that this is a CNSC staff assessment for prompting early discussion

Objectives of Amendments

- Ensure that the regulations continue to fulfill their role in effectively addressing Canada's nuclear security
- Ensure that Canada continues to fulfill its international obligations for the security of nuclear and radioactive materials

Overview of the Regulatory Amendment process



Context: Changes Since Last Amendments

- Last major amendments to NSR published in 2006
- Operational experience
  - opportunity to amend regulations based on industry and CNSC operational experience gained in the past 10 years
- Evolving security environment
  - security threats continue to emerge, change and evolve (e.g., cyber, insider)

Context: Changes Since Last Amendments (Cont'd)

- Technology advancements
  - NSR should allow new security technology to be implemented in a timely manner by licensees when appropriate (e.g., digital fingerprints, body scanners)
- New international recommendations, guidance and best practices
  - amendment to the *Convention on the Physical Protection of Nuclear Material*
  - publication of new International Atomic Energy Agency (IAEA) Nuclear Security Series recommendations
  - potential lessons learned and recommendations/suggestions from 2015 International Physical Protection Advisory Service mission report

Overview of Proposed Changes and Amendments

1. Simplified layout of the NSR
2. Performance-based approach to the NSR
3. Replace the list of facilities in Schedule 2 with a common definition
4. Cyber security program
5. Protection of nuclear security information
6. Nuclear security culture
7. Nuclear security plan

Other Items for Update, Discussion and Feedback

8. Facility access security clearance – information update
9. Potential changes for slowpoke operators
10. Transportation security plans
11. Security officer duties and responsibilities
12. Suggestions for amendments, updates, etc.

1. Simplified Layout of the NSR

- **Proposed amendment**
  - propose to layout the NSR in modular format
    - e.g., in the case of high-security sites all requirements that apply to these types of facilities will be listed concurrently
- **Why is this under consideration?**
  - current layout makes it challenging to find out what regulatory requirements apply to what facility
    - e.g., requirements that apply to Category III nuclear material are found in both Parts 1 and 2
- **Potential impacts**
  - no anticipated cost impacts
  - improved clarity

2. Performance-Based Approach

- **Proposed amendment**
  - considering a performance-based approach to the regulations where it makes sense to do so
  - regulations to set high-level security requirements
  - technical requirements and guidance to be moved to regulatory documents
  - examples
    - subsection 46 (3) of the NSR provides an example of performance-based language
    - example – Regulatory guide G-208, *Transportation Security Plans for Category I, II or III Nuclear Material*

2. Performance-Based Approach (Cont'd)

- **Why is this under consideration?**
  - provides flexibility for licence holders or applicants to propose an acceptable approach to meeting requirements

- **Potential impacts**
  - no anticipated cost impact

3. Replace the List of Facilities in Schedule 2 With a Definition

- **Proposed amendment**
  - remove Schedule 2 and replace with a definition
  - new definition, “medium-security site”, would replace the list of facilities in Schedule 2
  - definition could be expanded to include all non-power research reactors that use, process or store Category III nuclear material such as SLOWPOKE reactors

- **Why is this under consideration?**
  - current listing in Schedule 2 is out of date
  - future licensee applicants would be able to determine if medium-security site requirements would apply to them based on facility type

3. Replace the List of Facilities in Schedule 2 with a Definition (Cont'd)

- **Why is this under consideration? (cont'd)**
  - expanding requirements to SLOWPOKE reactors wouldminimize insider threat security risk
  - would preclude the need to update the schedule each time a facility is added or removed from the list

- **Potential impacts**
  - SLOWPOKE reactor licensees would be impacted
    - these facilities would be required to have a facility access security clearance for staff with unescorted access to reactors, as well as a supervisory awareness program to assess potential security risk indicators to reactor operation (additional information is provided on future slides)

4. Cyber Security Program

- **Proposed amendment**
  - licensees who fall under the new definition of medium-security sites would be required to establish a cyber security program for critical nuclear security and safety systems
  - medium-security sites would be required to
    - identify critical cyber assets
    - consider cyber threats – assessing potential security risk to operation
    - protect nuclear security and safety systems against cyber attacks using a graded approach

4. Cyber Security Program (Cont'd)

- **Why is this under consideration?**
  - cyber security is one of the fastest-growing threats to critical infrastructure in Canada

- **Potential impact**
  - medium impact for current Schedule 2 facilities
  - potential impact on SLOWPOKE reactors would require further discussion
  - could be phased in over a period of time, with a graded approach

5. Protection of Nuclear Security Information

- **Proposed amendment**
  - licensees who fall under the new definition of medium-security sites would be required to:
    - appropriately protect critical and/or sensitive nuclear security information by setting out high-level requirements for the protection and classification of information, the unauthorized disclosure of which could compromise or place at risk the security of nuclear material and/or facilities at medium-security sites
      - includes cyber media for the processing, storing and transmitting of nuclear security information
- **Why is this under consideration?**
  - without requirements, there is considerable risk and a likelihood that nuclear security information will be disclosed to unauthorized parties

5. Protection of Nuclear Security Information (Cont'd)

- **Why is this under consideration? (cont'd)**
  - licensees use a mix of terms, labels, and approaches to protecting information
  - assist in implementing consistent protection approaches within the nuclear industry
  - protection of sensitive, prescribed, and classified information to protect national security
  - to meet international fundamentals (NSS 20)
- **Potential impacts**
  - depends on the licensee as some have already implemented programs for the protection of nuclear security information
  - could be phased in over a period of time, using a graded approach

6. Nuclear Security Culture

- **Proposed amendment**
  - licensees who fall under the new definition of medium-security sites would be required to implement a nuclear security culture program
- **Why is this under consideration?**
  - Fundamental principle F, “Security Culture” – Amended Convention on the Physical Protection of Nuclear Material
  - the IAEA has identified the need for licensees, regulators, and states to establish an effective nuclear security culture with the goal of providing greater assurance that nuclear security activities will maintain and improve the following: preventing, detecting, delaying and responding to theft, sabotage, unauthorized access, illegal transfer, or other malicious acts involving radioactive material in use, storage, or transport

6. Nuclear Security Culture (Cont'd)

- **Why is this under consideration? (cont'd)**
  - IAEA definition of nuclear security culture: The assembly of characteristics, attitudes and behaviors of individuals, organizations and institutions which serves as a means to support, enhance and sustain nuclear security
- **Potential impact**
  - requires further discussion to assess impact on licensees, likely limited impact as this can be accomplished through a "corporate culture" that embraces security and safety culture in one program or as a stand-alone program that is equivalent to the safety culture programs

7. Nuclear Security Plan

- **Proposed amendment**
  - licensees who fall under the new definition of medium-security sites would be required to document all essential security-related information in a nuclear security plan (NSP)
  - this information is currently described in a document called “site security report or plan”
  - the NSP will continue to have to be reviewed and updated as required
- **Why is this under consideration?**
  - reflect IAEA recommendations for nuclear security
  - mix of terms used now including security report, site security report, site security plan, etc.
- **Potential impact**
  - minimal, no increase in cost to what is currently being done

8. Facility Access Security Clearance – Information Update

- **Proposed amendment**
  - licensees who fall under the new definition of medium-security site will be subject to a new criminal record name check (CRNC) process for vetting candidates for a facility-access security clearance
    - currently projected that by late 2017, criminal record name CRNCs will only be processed by digital fingerprint scanning by the RCMP
    - this will impact every police service in Canada that currently provides CRNCs
    - also impacts licensees who require CRNC information when vetting candidates for a facility access security clearance
      - we want to ensure that affected licensees are aware of this change

8. Facility Access Security Clearance – Information Update (Cont'd)

- **Why is this under consideration?**
  - CRNC process is moving to digital scanning technology
  - updated digital fingerprint scanning technology will result in a faster response time
  - more secure system, addresses privacy concerns
  - addresses gaps in current criminal record name check system
- **Potential impacts**
  - licensees will have to send facility-access security clearance applicants or renewal candidates to an RCMP-approved contractor/vendor for fingerprint scans in support of CRNCs
  - we are not sure of what additional costs might be at this point in time
  - the CNSC is considering accepting alternatives to a CRNC, such as Nexus card

9. Proposed Changes for SLOWPOKE Operators

- **Proposed amendment**
  - SLOWPOKE licensees will be defined as medium-security sites so the previous proposed requirements would apply to them
  - all persons with unescorted access to the SLOWPOKE reactor area will require a facility access security clearance
  - Supervisory Awareness Program to minimize insider risk
  - vehicles that enter the reactor area must be screened for explosives, weapons and unauthorized persons

9. Proposed Changes for SLOWPOKE Operators (Cont'd)

- **Why is this under consideration?**
  - minimize the insider risk
- **Potential impact**
  - some SLOWPOKE operators already conduct CRNCs
  - some SLOWPOKE operators conduct screening of vehicles entering reactor area
  - welcome feedback on impacts from SLOWPOKE licensees at today's workshop

10. Transportation Security Plans

- Section 5 of the NSR provides the high-level requirements for a transportation security plan
  - in addition, Regulatory guide G-208, *Transportation Security Plans for Category I, II or III Nuclear Material,* provides detailed guidance for licensees
- No amendments are currently being considered to section 5
  - the CNSC's view is that section 5 provides the necessary requirements given the current threat environment
  - depending on stakeholder feedback, current plan is only to update the content of G-208 in consultation with the licensees and the public
- As part of this workshop, we would request licensee feedback on how they feel this section is working

11. Security Officer Duties and Responsibilities

- Should the CNSC consider adding language to the amended NSR similar to section 30 that would outline the duties of security officers deployed at medium-security sites?
- Is there a need to screen persons for nuclear material when they are exiting the areas where such material is used, stored or processed, and how is that currently being handled?
- Do onsite security staff have the tools they need to protect a medium-security site, its operation or staff?

12. Suggestions for Additional Amendments, Updates

- Additional suggestions for potential amendments or improvements to the NSR are welcome

Group Work Sessions

- Now that we have provided some of our proposed amendments for the NSR we would appreciate your feedback on them
- At your table please discuss your feedback
- CNSC staff at your table will guide conversations at your table and will record feedback on the laptop provided
  - this feedback will be posted on the CNSC's website
  - prescribed information may be discussed during the course of the workshop and will be handled in accordance with regulatory requirements
- Designate one person at the table to present a summary of the feedback from your table to the workshop

nuclearsafety.gc.ca