L'organisme de réglementation nucléaire du Canada

Cybersécurité et protection des informations numériques

Document de travail DIS-21-03

Juillet 2021

Commission canadienne de sûreté nucléaire
Canadian Nuclear Safety Commission
Canada

Cybersécurité et protection des informations numériques
Document de travail DIS-21-03

Also available in English under the title: Cyber Security and the Protection of Digital Information

Disponibilité du document
Les personnes intéressées peuvent consulter le document sur le site Web de la CCSN ou l'obtenir, en français ou en anglais, en communiquant avec la :

Commission canadienne de sûreté nucléaire
280, rue Slater
C.P. 1046, succursale B
Ottawa (Ontario) K1P 5S9
CANADA

Téléphone : 613-995-5894 ou 1-800-668-5284 (au Canada seulement)
Télécopieur : 613-995-5086
Courriel : cnsc.info.ccsn@cnsc-ccsn.gc.ca
Site Web : suretenucleaire.gc.ca
Facebook : facebook.com/Commissioncanadiennedesuretenucleaire
YouTube : youtube.com/ccsncnsc
Twitter : @CCSN_CNSC
LinkedIn : linkedin.com/company/cnsc-ccsn

Historique de publication
juillet Version 1

Préface

Les documents de travail jouent un rôle important dans la sélection et l'élaboration du cadre et du programme de réglementation de la Commission canadienne de sûreté nucléaire (CCSN). Ils visent à obtenir, tôt dans le processus, la rétroaction du public sur les politiques et approches de la CCSN.

L'utilisation de documents de travail au début du processus de réglementation souligne l'engagement de la CCSN à l'égard d'un processus de consultation transparent. La CCSN analyse les rétroactions préliminaires et en tient compte lorsqu'elle détermine le type et la nature des exigences et orientations à établir.

Les documents de travail sont rendus publics aux fins de commentaires pour une période déterminée. À la fin de la première période de commentaires, le personnel de la CCSN examine toutes les observations formulées par le public. Les commentaires reçus sont ensuite affichés aux fins de rétroaction sur le site Web de la CCSN pour une deuxième période de consultation.

La CCSN tient compte de toute la rétroaction obtenue dans le cadre de ce processus de consultation lorsqu'elle établit son approche de réglementation

Table des matières

Sommaire

La CCSN réglemente l'utilisation de l'énergie et des matières nucléaires afin de préserver la santé, la sûreté et la sécurité des Canadiens, de protéger l'environnement et de respecter les engagements internationaux du Canada à l'égard de l'utilisation pacifique de l'énergie nucléaire. Dans le cadre de son mandat, la CCSN réglemente la sûreté nucléaire par le biais du *Règlement général sur la sûreté et la réglementation nucléaires* (RGSRN) et du *Règlement sur la sécurité nucléaire* (RSN).

La CCSN propose d'apporter des modifications au RSN dans les domaines touchant la cybersécurité, notamment la protection des renseignements réglementés et des systèmes et composants informatiques qui remplissent des fonctions de sûreté nucléaire, de sécurité nucléaire, de préparation et de gestion des urgences et des garanties ou qui ont une incidence sur ces fonctions. La CCSN a publié un document de travail, *Modifications proposées au Règlement sur la sécurité nucléaire*, DIS-21-02, qui traite des modifications du RSN à un niveau élevé. L'objectif de ce document de travail est de fournir des détails sur les changements proposés aux exigences et aux directives en matière de cybersécurité et de protection de l'information numérique. Ce document de travail propose également d'étendre les exigences en matière de cybersécurité et de protection des informations à d'autres titulaires de permis non régis par le RSN.

De plus, la CCSN propose d'ajouter une exigence selon laquelle tous les titulaires de permis assujettis au règlement devront évaluer leur vulnérabilité aux cybermenaces, et que celles-ci soient incluses dans l'évaluation des menaces et des risques (EMR) du titulaire de permis. L'objectif de cette exigence est de s'assurer que les titulaires de permis sont en mesure de détecter et de contrer les cyberattaques ciblant les renseignements réglementés et les systèmes qui remplissent des fonctions importantes pour la sûreté nucléaire, la sécurité, la préparation aux situations d'urgence et les garanties. En raison de cette proposition, les titulaires de permis concernés devront, dans le cadre de leur programme de sécurité, élaborer un programme et des mesures de cybersécurité pour gérer les risques relevés dans leurs EMR. Les titulaires de permis concernés seront également tenus de signaler les incidents de cybersécurité de la même manière que les autres incidents de sécurité. Cette activité est déjà mise en œuvre par les sites à sécurité élevée (SSE).

Les attentes de la CCSN en matière de cybersécurité aux SSE sont énoncées dans la norme CSA N290.7, *Cybersécurité pour les centrales nucléaires et les installations dotées de petits réacteurs* (N290.7) [1]. La norme CSA N290.7 est en cours de révision et la CCSN participe à ce processus. Au besoin, la CCSN peut également envisager d'ajouter des éléments de cybersécurité à son cadre de réglementation, dans la série de REGDOC-2.12, pour compléter la norme N290.7. Le présent document ne propose pas d'exigences supplémentaires en matière de cybersécurité pour les biens assurant des fonctions de sûreté, de sécurité, de préparation aux situations d'urgence et de garantie pour les titulaires de permis qui sont déjà tenus de se conformer à la norme N290.7.

En 2015, l'Agence internationale de l'énergie atomique a mené une mission du Service consultatif international sur la protection physique (SCIPP) [2] au Canada pour examiner le régime de sécurité nucléaire et le cadre de réglementation du Canada. Dans son rapport de mission, le SCIPP a recommandé que la CCSN envisage d'étendre les exigences en matière de cybersécurité à d'autres activités autorisées de nature délicate dans des installations autres que les centrales nucléaires, notamment les installations de combustible nucléaire et les installations de traitement des substances nucléaires. En réponse à cette recommandation, la CCSN s'est engagée à examiner les risques pour ses titulaires de permis et à mettre en œuvre de telles exigences, le cas échéant. Les leçons apprises durant la mise en application de la norme N290.7 dans les centrales nucléaires ont été utilisés pour développer les améliorations potentielles à la réglementation de la cyber sécurité.

La CCSN envisage d'étendre les exigences de cybersécurité aux titulaires de permis qui ne sont pas couverts par le RSN, comme les titulaires de permis de sources scellées de catégories 1 et 2. À l'heure actuelle, il existe très peu d'expérience canadienne ou internationale en matière de réglementation de la cybersécurité appliquée aux substances nucléaires. Par conséquent, le présent document vise principalement à obtenir des renseignements qui pourront servir de base à l'élaboration d'exigences réglementaires et de directives dans ce domaine.

Le présent document propose également une approche pour protéger les renseignements réglementés numériques et les renseignements de nature délicate gérés numériquement par les titulaires de permis. L'approche est similaire à celle qui est utilisée pour la gestion des renseignements classifiés et de nature délicate gérés par le gouvernement du Canada.

L'approche réglementaire proposée ainsi que les exigences et les directives proposées sont présentées dans ce document de travail afin d'être examinées par les titulaires de permis, les promoteurs, le public canadien, les organisations de la société civile, les peuples autochtones, les autres ministères et organismes gouvernementaux et les autres intervenants.

Le présent document vise à initier les discussions avec les parties prenantes de la CCSN. Cette dernière pourra entreprendre d'autres consultations avec les parties intéressées pour faire avancer les discussions et recueillir d'autres renseignements pertinents. Tous les commentaires reçus au cours de la phase de consultation de ce projet guideront l'approche de la CCSN.

Cybersécurité et protection des informations numériques

1. Introduction

Les systèmes informatiques jouent un rôle croissant dans l'industrie nucléaire et sont utilisés pour assurer la sûreté et la sécurité des installations et des activités lors de l'utilisation, de l'entreposage et du transport des substances nucléaires. Les adversaires peuvent recourir à des cyberattaques pour cibler les systèmes informatiques afin de faciliter leurs actes malveillants (p. ex., le sabotage ou le vol de substances nucléaires). Les cyberattaques peuvent être utilisées conjointement avec d'autres moyens conventionnels notamment des actions physiques ou des actes commis par des initiés.

Les cyberattaques visant les systèmes informatiques pourraient permettre aux adversaires de compromettre le fonctionnement et le rendement de divers systèmes touchant la sûreté nucléaire, la sécurité, la préparation aux situations d'urgence et les garanties, ainsi que les systèmes auxiliaires qui soutiennent ces systèmes. Les cyberattaques contre les systèmes de sûreté nucléaire peuvent, par exemple, causer des blessures aux travailleurs et au public, ou entraîner des rejets nocifs dans l'environnement. Les cyberattaques peuvent également dégrader le rendement ou la fonction des systèmes de protection physique, ce qui peut faciliter le sabotage d'une installation nucléaire ou encore le vol ou le sabotage de substances nucléaires.

En outre, les cyberattaques pourraient permettre à des adversaires d'obtenir un accès non autorisé à des renseignements de nature délicate qui sont stockés, traités et transmis sur des systèmes informatiques et des réseaux corporatifs. Les cyberattaques visant des renseignements de nature délicate pourraient permettre à des adversaires d'empêcher l'accès aux renseignements de nature délicate nécessaires à la sûreté et à la sécurité des opérations, ou de les falsifier. Elles pourraient également permettre la divulgation non autorisée de renseignements réglementés et de nature délicate, par exemple des détails sur les mesures de sécurité ou encore des informations concernant les expéditions de matières, ce qui pourrait faciliter le vol de substances nucléaires ou les actes de sabotage.

Le Groupe CSA a élaboré une norme nationale portant le numéro N290.7 [1]. Cette norme a été élaborée avec la participation des titulaires de permis, de la CCSN et d'autres parties prenantes. La norme N290.7 contient des exigences et des orientations concernant l'établissement d'un programme de cybersécurité fondé sur le risque, afin de protéger contre les cyberattaques les systèmes qui remplissent des fonctions importantes pour la sûreté nucléaire, la sécurité nucléaire, la préparation aux situations d'urgence et les garanties (SSPUG). La norme N290.7 définit également des mesures de cybersécurité qui peuvent être appliquées aux installations autres que les centrales nucléaires et les installations à petits réacteurs en utilisant une approche graduelle telle que définie dans le REGDOC 3.5.3, *Principes fondamentaux de réglementation* [3].

En l'absence d'exigences spécifiques en matière de cybersécurité, il est difficile pour la CCSN de vérifier que les informations numériques et les substances nucléaires sont protégées de manière adéquate contre les menaces utilisant la cyberattaque pour faciliter le vol et le sabotage. Voici des domaines où des exigences supplémentaires en matière de cybersécurité et de protection de l'information pourraient être nécessaires :

- La CCSN propose de développer des exigences spécifiques pour les cyber sécurité pour la protection des systèmes qui remplissent des fonctions de SSPUG et les activités énumérées dans les tableaux 2 et 3.

- Le document d'application de la réglementation de la CCSN REGDOC-2.12.3, *La sécurité des substances nucléaires : Sources scellées et matières nucléaires de catégories I, II et III* [4], précise que « ces renseignements ne devraient pas être conservés sur un réseau ouvert ou partagé sans protection adéquate », mais ne présente aucune exigence ni orientation particulière pour la protection de ces réseaux. La CCSN propose de développer des exigences ou des orientations spécifiques sur la sécurité de l'information pour protéger les systèmes et réseaux informatiques qui préparent, utilisent, stockent et transmettent des renseignements de nature délicate, y compris les renseignements réglementés.

Le tableau 1 présente un résumé de l'état des exigences proposées en matière de cybersécurité pour les titulaires de permis qui seraient touchés par de telles exigences.

Le présent document vise à initier la discussion sur l'élaboration d'exigences réglementaires et d'orientations pour les titulaires de permis. D'autres discussions auront lieu lors de réunions de consultation plus tard dans l'année, afin de poursuivre la conversation.

Les commentaires recueillis grâce au présent document et durant les futures réunions de consultation informeront l'approche réglementaire de la CCSN en ce qui concerne la cybersécurité et la protection des informations numériques. Elle complétera également les exigences et les orientations existantes qui s'appliquent aux SSPUG.

Tableau 1 : Exigences actuelles en matière de cybersécurité

Types de permis ou d'activités	Exigences actuelles en matière de cybersécurité pour la sûreté nucléaire, la sécurité nucléaire, la préparation aux situations d'urgence et les garanties
Sites à sécurité élevée	
Permis d'exploitation d'un réacteur de puissance Permis d'exploitation et de déclassement d'un établissement de recherche et d'essais nucléaires	Selon chaque manuel des conditions de permis (MCP), les publications du fondement d'autorisation sont les suivantes : • La section 6.2 du REGDOC 2.12.3 [4] exige un programme de cybersécurité conforme à la norme CSA N290.7 [1]. • La norme N290.7 [1] est incluse comme document du fondement d'autorisation dans le MCP.
Permis d'exploitation d'une installation de gestion des déchets	Selon chaque MCP : • L'installation est tenue d'avoir un programme de cybersécurité comprenant une liste définie d'éléments du programme. • La norme N290.7 [1] est incluse comme document d'orientation dans le MCP.
Installations ayant des matières nucléaires de catégorie III (y compris les réacteurs de recherche) et les accélérateurs de recherche de catégorie IB	
Réacteurs de recherche	Selon chaque MCP, le titulaire de permis est tenu de mettre en œuvre des mesures de cybersécurité pour

Types de permis ou d'activités	Exigences actuelles en matière de cybersécurité pour la sûreté nucléaire, la sécurité nucléaire, la préparation aux situations d'urgence et les garanties
	protéger les biens qui ont une importance élevé pour les fonctions de SSPUG.
Installations de catégorie IB (tableau 2)	Aucune exigence particulière en matière de cybersécurité.
Titulaires de permis de sources scellées de catégories 1 et 2	
Tous les titulaires de permis de sources scellées de catégories 1 et 2 Des activités représentatives utilisant ces sources sont présentées dans le tableau 3.	Aucune exigence particulière en matière de cybersécurité.
Entités qui transportent ou font transporter des matières nucléaires de catégories I, II ou III ou des sources scellées de catégories 1 ou 2	
Transport de matières nucléaires de catégories I, II ou III Transport de sources scellées nécessitant des plans de sécurité du transport (sources scellées de catégories 1 et 2)	Aucune exigence particulière en matière de cybersécurité.

1.1 Portée

Le présent document propose des orientations et des exigences pour la protection des informations et s'adresse aux titulaires de permis d'exploitation de réacteurs nucléaire, d'établissements de recherche et d'essais nucléaires ou de permis de déclassement d'établissements de recherche et d'essais nucléaires. La portée de ce document ne comprend pas la cybersécurité visant à protéger les fonctions de SSPUG, car ces titulaires de permis sont tenus de mettre en œuvre des programmes de cybersécurité conformément à la norme N290.7 [1].

En ce qui concerne les titulaires de permis figurant dans le tableau 2 (installations, y compris les réacteurs de recherche, ayant des matières nucléaires de catégorie III, et les titulaires de permis de catégorie IB) et les titulaires de permis de sources scellées de catégories 1 et 2 (voir le tableau 3), le présent document propose des exigences et des orientations potentielles pour la protection des informations et pour la cybersécurité afin de protéger les fonctions de SSPUG.

Le présent document fournit des exigences en matière de cybersécurité applicables au transport et s'adresse aux titulaires de permis qui transportent ou font transporter des matières nucléaires de catégories I, II ou III ou des sources scellées de catégories 1 ou 2. Le document comporte également des dispositions relatives à la sécurité des renseignements et aux principes de cybersécurité qui sous-tendent les exigences et les orientations potentielles.

Tableau 2 : Titulaires de permis (y compris les réacteurs de recherche) ayant des matières nucléaires de catégorie III, et accélérateurs de catégorie IB

Type d'installation
Installations de gestion des déchets radioactifs qui ne sont pas des SSE
Installations de conversion de l'uranium
Réacteurs en état d'arrêt et déclassés
Installations de traitement des substances nucléaires
Installations de fabrication de combustible et raffineries
Installations prototypes de gestion des déchets
Réacteurs de recherche
Installations d'accélérateurs de recherche de catégorie IB

Tableau 3 : Activités représentatives utilisant des sources scellées de catégories 1 et 2

Activité
Irradiateurs : type piscine, stérilisation et préservation des aliments
Irradiateurs : autoblindés
Irradiateurs : sang/tissu
Industrie de la transformation/fabrication
Téléthérapie à faisceaux multiples (scalpel gamma)
Téléthérapie (avec sources radioactives)
Gammagraphie industrielle
Diagraphie de puits

1.2 Activités préalables à la consultation réalisées à ce jour

La CCSN a déjà consulté les parties intéressées au sujet de ses plans de modernisation de la réglementation, y compris le RSN, par le biais du document de travail DIS-14-02, *Moderniser les règlements de la CCSN* [5]. Un résumé des commentaires reçus des parties intéressées ainsi que les réponses de la CCSN à ces commentaires ont été publiés dans le *Rapport sur ce que nous avons entendu* – DIS-14-02 [6].

La CCSN a organisé trois ateliers avec les parties intéressées en 2016 et en 2017 afin d'examiner les éventuelles modifications réglementaires au RSN en fonction des exigences opérationnelles et des nouvelles technologies qui pourraient avoir un impact sur la sécurité des installations nucléaires existantes ou envisageables dans un avenir prévisible. Y ont participé des responsables de la mise en œuvre des mesures de sécurité dans les installations nucléaires, des responsables de la sécurité des matières nucléaires ou radioactives, de l'équipement réglementé et des renseignements réglementés, ainsi que les concepteurs de futures technologies des réacteurs.

Les participants ont formulé des commentaires sur les aspects du RSN que la CCSN envisage de modifier. De plus, ils ont suggéré d'autres aspects à modifier et ont présenté des données préliminaires sur l'impact de ces éventuelles modifications. La CCSN a publié les résultats de ces ateliers dans le *Rapport sur les ateliers avec les parties intéressées : Examen périodique du Règlement sur la sécurité nucléaire* [7].

La CCSN a l'intention de tenir d'autres réunions de consultation à l'été et à l'automne 2021. Ces réunions de consultation, s'appuyant sur les propositions décrites dans le présent document, seront l'occasion de discuter plus en détail des changements proposés et de leurs impacts et défis potentiels avec les titulaires de permis, les promoteurs, le public canadien, les organisations de la société civile, les peuples autochtones, les autres ministères et organismes gouvernementaux et les autres parties intéressées. De plus amples détails sur ces événements seront fournis dans les mois à venir.

1.3 Organisation du document

Le reste du présent document est organisé comme suit :

- La première partie présente les orientations réglementaires proposées pour protéger les informations numériques contre les cyberattaques tout au long de leur cycle de vie.
    - La section 2 décrit l'obligation de protéger les renseignements réglementés.
    - La section 3 présente un aperçu des principes de protection des informations. De plus, elle présente des questions auxquelles pourraient contribuer les parties intéressées en vue de l'élaboration d'orientations réglementaires.
- La deuxième partie du document présente des orientations potentielles en matière de cybersécurité des systèmes et des réseaux utilisés pour mettre en œuvre les fonctions de SSPUG.
    - La section 4 présente les activités autorisées pouvant nécessiter des programmes ou des mesures de cybersécurité.
    - La section 5 donne une vue d'ensemble d'un programme de cybersécurité, des mesures de cybersécurité, d'une approche graduelle fondée sur le risque et la défense en profondeur.
    - La section 6 présente des exigences et des orientations potentielles en matière de cybersécurité afin d'assurer la protection des sites à sécurité élevée.
    - La section 7 présente des exigences et des orientations potentielles en matière de cybersécurité pour la protection des titulaires de permis détenant des matières nucléaires de catégorie III, y compris les réacteurs de recherche et les accélérateurs de recherche de catégorie IB.
    - La section 8 présente des exigences et des orientations potentielles en matière de cybersécurité pour la protection de titulaires de permis sélectionnés de substances nucléaires.
    - La section 9 présente des exigences potentielles en matière de cybersécurité pour les entités qui transportent ou font transporter des matières nucléaires ou des substances nucléaires de catégories I, II ou III.

2. Protection des informations concernant les activités autorisées par la CCSN

L'un des objectifs de la *Loi sur la sûreté et la réglementation nucléaires* (LSRN) [8] est de limiter les risques pour la sécurité nationale, la santé et la sécurité des personnes et l'environnement qui sont associés à la production, la possession et l'utilisation des renseignements réglementés en vertu de la loi. La LSRN contient des provisions pour la création de règlements concernant les renseignements réglementés.

La CCSN réglemente la sécurité nucléaire en vertu du :

- RSN, qui s'applique aux installations nucléaires qui produisent, traitent, utilisent, entreposent ou transportent des matières nucléaires de catégories I, II ou III, et aux installations nucléaires figurant à l'annexe 2 du RSN.
- *Règlement général sur la sûreté et la réglementation nucléaires* (RGSRN) [9], qui s'applique aux activités décrites aux alinéas 26 (a) à (f) de la LSRN. Ces activités comprennent la possession, le transfert, l'importation, l'exportation, l'utilisation ou l'abandon de renseignements réglementés.

Ensemble, le RSN et le RGSRN permettent au Canada de continuer à remplir ses obligations nationales et internationales en matière de sécurité des installations nucléaires, des matières nucléaires et radioactives, de l'équipement réglementé et des renseignements réglementés, comme l'exige la LSRN. Ils sont actuellement appuyés par quatre documents d'application de la réglementation (REGDOC) portant sur la sécurité nucléaire, qui fournissent des orientations sur la façon dont les demandeurs et les titulaires de permis peuvent satisfaire aux exigences réglementaires en matière de sécurité nucléaire. Ces REGDOC sont les suivants :

- REGDOC-2.12.1, *Sites à sécurité élevée, tome I : Force d'intervention pour la sécurité nucléaire* (2018) (document classifié) [10]
- REGDOC-2.12.1, *Sites à sécurité élevée, tome II : Critères pour les systèmes et dispositifs de sécurité nucléaire* (2018) (document classifié) [11]
- REGDOC-2.12.2, *Cote de sécurité donnant accès au site* (2013) [12]
- REGDOC-2.12.3, *Sécurité des substances nucléaires : Sources scellées et matières nucléaires de catégories I, II et III* (2020) [4]

À l'heure actuelle, aucun REGDOC de la CCSN ne fournit d'orientation concernant la protection des renseignements réglementés sous forme numérique, ou sur la protection des systèmes, réseaux et supports informatiques utilisés pour créer, stocker, traiter et transmettre des renseignements réglementés.

La section suivante décrit les principes de sécurité de l'information. Elle présente également les aspects dont doivent tenir compte les titulaires de permis pour ce qui est de l'application de ces principes à la protection des informations numériques, des systèmes informatiques, des réseaux et des médias.

3. Principes de protection des informations

3.1 Définition des renseignements réglementés

L'article 21 du RGSRN définit comme suit les renseignements réglementés (y compris les documents sur ces renseignements) :

a) « les substances nucléaires, y compris leurs propriétés, qui sont nécessaires à la conception, la production, l'utilisation, le fonctionnement ou l'entretien des armes nucléaires ou des engins explosifs nucléaires;
b) la conception, la production, l'utilisation, le fonctionnement ou l'entretien des armes nucléaires ou des engins explosifs nucléaires;
c) les arrangements, l'équipement, les systèmes et les procédures en matière de sécurité que le titulaire de permis a mis en place conformément à la Loi, à ses règlements ou au permis, y compris tout incident relatif à la sécurité;
d) l'itinéraire ou le calendrier de transport des matières nucléaires de catégorie I, II ou III au sens de l'article 1 du *Règlement sur la sécurité nucléaire*. »

Les renseignements réglementés doivent être protégés tout au long de leur cycle de vie, quel que soit leur format (p. ex., numérique ou papier). Le titulaire de permis est responsable de la mise en œuvre de mesures de sécurité (mesures physiques et cybersécurité) proportionnelles au niveau de sensibilité des renseignements gérés. Dans ce contexte, la sensibilité fait référence au niveau d'impact qu'une diffusion non autorisée pourrait avoir sur le fonctionnement sûr et sécuritaire de l'installation ou de l'activité.

L'« intérêt national » désigne la défense et le maintien de la stabilité sociopolitique et économique du Canada. Un exemple de renseignements réglementés dans l'intérêt national serait les détails concernant le transport de matières nucléaires au Canada.

3.2 Définitions des termes « renseignements de nature délicate » et « biens relatifs aux renseignements de nature délicate »

La CCSN propose la définition suivante pour les renseignements de nature délicate : « tout renseignement, y compris les renseignements réglementés ou classifiés, peu importe leur format, y compris les logiciels, dont la divulgation non autorisée, la modification, l'altération, la destruction ou le refus d'utilisation pourrait mettre en péril la sécurité nucléaire ». La CCSN propose la définition suivante pour les biens relatifs à des renseignements de nature délicate : « tout équipement ou composant, y compris les biens numériques, qui servent à stocker, traiter, contrôler ou transmettre des renseignements de nature délicate ».

3.3 Objectifs de la protection des renseignements

Les piliers de la protection des renseignements sont l'assurance de la confidentialité, de l'intégrité et de la disponibilité des renseignements. Au cours des activités de consultation préalable, et comme le résume la section 3.6 du *Rapport sur les ateliers avec les parties intéressées : Examen périodique du Règlement sur la sécurité nucléaire [7], certains* titulaires de permis de centrale nucléaire étaient d'avis que les objectifs de protection des renseignements susmentionnés devraient être définis de façon souple afin de permettre aux mécanismes existants de protection des renseignements de satisfaire aux exigences réglementaires. D'autres participants étaient plutôt d'avis qu'il serait difficile d'assurer la cohérence avec une approche axée sur le rendement, et qu'un certain degré de mesures normatives serait requis.

3.4 Portée de la protection des renseignements

Le présent document de travail traite de la protection des renseignements de nature délicate, y compris les renseignements réglementés, sous forme numérique. Cela implique une protection contre les cyberattaques qui visent :

- les supports numériques et les dispositifs portables sur lesquels sont stockés des renseignements numériques
- les systèmes informatiques utilisés pour créer, stocker, traiter et transmettre des renseignements numériques
- les réseaux de communication sur lesquels les renseignements numériques sont transmis

De nombreux titulaires de permis disposent déjà de programmes ou de mesures de sécurité qui protègent leurs renseignements numériques. Le recours à des exigences axées sur le rendement permettrait de créditer ces programmes existants, alors que des exigences normatives pourraient nécessiter des changements importants aux programmes existants.

3.5 Cycle de vie proposé pour les renseignements et considérations particulières

La Figure 1 décrit le cycle de vie proposé par la CCSN pour la gestion des informations numériques. Par la suite, cette section décrit les activités possibles que les titulaires de permis peuvent être tenus de réaliser pour gérer les informations numériques. Les phases du cycle de vie des informations sont décrites plus en détail dans les sections subséquentes.

Figure 1 : Cycle de vie proposé pour les informations numériques

3.5.1 Phase de création

Dans la phase de création, le titulaire de permis crée des informations. Ces informations peuvent se présenter sous diverses formes : documents papier, réflexions ou enregistrements électroniques. Les informations peuvent être de nature délicate ou non.

3.5.2 Détermination des renseignements de nature délicate

Au cours de cette phase, on s'attend à ce que le titulaire de permis :

- effectue un examen pour déterminer s'il crée, utilise, stocke, transmet ou élimine des informations numériques de nature sensible, y compris des renseignements de nature délicates ou des renseignements réglementés
- répertorie les biens relatifs aux renseignements de nature délicate, y compris les systèmes et réseaux informatiques qui créent, stockent, traitent et transmettent des renseignements réglementés numériques

Si le titulaire de permis détermine qu'il ne gère pas de renseignements numériques de nature délicate, il peut être raisonnable de penser qu'il n'est pas tenu de mettre en œuvre l'une des mesures de sécurité applicables à la protection des renseignements décrites dans le présent document. Il pourra toutefois les mettre en œuvre à titre de pratiques exemplaires.

3.5.3 Classification et marquage des renseignements de nature délicate

Si le titulaire de permis détermine qu'il gère des renseignements de nature délicate, y compris des renseignements réglementés, on s'attend à ce qu'il en évalue le niveau de sensibilité afin de déterminer le degré approprié de protection de ses renseignements.

Les niveaux de sensibilité varient en fonction du contenu exact des documents et des impacts potentiels sur l'intérêt national et les autres intérêts advenant la compromission des renseignements. Le Tableau 4 présente les différents niveaux de sensibilité qui peuvent être attribués aux renseignements, et le niveau de préjudice potentiel respectif pour chaque niveau.

En outre, l'annexe A est présentée à titre de référence pour déterminer le niveau de sensibilité potentielle des renseignements généralement détenus par un titulaire de permis. La liste de documents est tirée du document de la Collection Sécurité nucléaire de l'AIEA no 23-G, Sécurité de l'information nucléaire [13], qui décrit les documents et les renseignements qu'ils contiennent. L'annexe A recommande une correspondance entre les documents/renseignements et les niveaux de sensibilité des renseignements du gouvernement du Canada dans le Tableau 4.

Les renseignements de nature délicate, quelle que soit leur forme, devraient être accompagnés de leur degré de sensibilité, afin d'en faciliter la gestion appropriée. Le personnel de la CCSN peut aider les titulaires de permis à déterminer le niveau de sensibilité convenant le mieux, sur demande. Toutefois, il incombera toujours au créateur du document de lui assigner un niveau de sensibilité.

Tableau 4 : Niveaux de sensibilité des renseignements et préjudices comparatifs

Niveau	Description	Préjudice comparatif
Très secret	S'applique aux renseignements ou aux biens dont la compromission pourraient causer un préjudice exceptionnellement grave à l'intérêt national.	Leur diffusion pourrait entraîner un événement extrême susceptible d'affecter une grande partie de la population : • Pertes humaines élevées • Traumatisme psychologique important • Troubles civils potentiels
Secret	S'applique aux renseignements ou aux biens dont la compromission pourraient causer un préjudice grave à l'intérêt national.	Leur diffusion pourrait avoir des répercussions négatives importantes sur les individus ou la nation : • Perte potentielle de vie ou d'invalidité pour certains • Maladie ou blessure grave pour de nombreuses personnes • Aliénation de grands groupes
Confidentiel	S'applique aux renseignements ou aux biens dont la compromission pourraient causer un préjudice limité ou modéré à l'intérêt national.	Leur diffusion pourrait avoir de graves répercussions sur la nation : • Dommages modérés à l'opinion nationale / aux relations internationales

Certains titulaires de permis ont déjà établi des systèmes de classification des renseignements qui utilisent une terminologie et des critères de classification différents. Ils ont suggéré, lors des consultations, que s'ils utilisaient les définitions générales pour les renseignements sur la sécurité nucléaire, de nouveaux systèmes de classification ne seraient pas nécessaires. La CCSN propose qu'en tant qu'entité gouvernementale, d'utiliser le système de classification décrit dans le tableau 4 pour établir l'orientation réglementaire. Les titulaires de permis ayant des systèmes existants pourraient assurer la correspondance entre le système de classification décrit dans le tableau 4 et leur propre système de classification existant, afin d'éviter de créer un nouveau système de classification.

La CCSN aimerait savoir ce qui suit :

Q1. Êtes-vous d'accord avec le modèle proposé pour la gestion électronique des renseignements réglementés?

Q2. Ce modèle pourrait-il être utilisé pour gérer tous les renseignements de nature délicate générés par votre organisation?

Q3. Êtes-vous d'accord avec la méthode proposée pour la détermination, la classification et le marquage des renseignements de nature délicate (y compris les renseignements réglementés) que vous gérez? Pourquoi? Dans la négative, pourquoi?

Q4. Veuillez indiquer tout impact susceptible de se produire si la CCSN rendait les pratiques suggérées obligatoires.

3.5.4 Utilisation des renseignements de nature délicate

Il est interdit aux titulaires de permis de transmettre des renseignements réglementés, sauf pour les exceptions énumérées au paragraphe 23(1) du RGSRN. La CCSN propose que lorsque des renseignements de nature délicate (y compris des renseignements réglementés) sont transmis ou transférés, ils soient protégés par des mesures de sécurité proportionnelles à leur sensibilité et ne soient communiqués qu'aux seules personnes qui ont un besoin de savoir[1] et qui détiennent une autorisation de sécurité ou une vérification de fiabilité appropriée. Les titulaires de permis sont encouragés à utiliser le Guide G1-009, *Transport et transmission de renseignements protégés ou classifiés* [14] de la Gendarmerie royale du Canada (GRC), pour la transmission de renseignements de nature délicate.

Tous les systèmes utilisés pour traiter des renseignements de nature délicate, y compris les renseignements réglementés, doivent être protégés contre les cyberattaques afin de garantir la confidentialité, l'intégrité et la disponibilité des renseignements.

On peut utiliser les documents suivants pour gérer la protection des renseignements et mettre en œuvre des mesures de cybersécurité pour protéger les renseignements de nature délicate. Ces mesures peuvent être mises en œuvre selon une approche graduelle :

- Centre de la sécurité des télécommunications du Canada, *La gestion des risques liés à la sécurité des TI : Une méthode axée sur le cycle de vie (ITSG-33)*, et ses guides [15]

[1] Besoin de savoir : besoin opérationnel démontrable d'accéder aux renseignements.

- National Institute of Standards and Technology, SP 800-53, *Security and Privacy Controls for Information Systems and Organizations* [16]
- Organisation internationale de normalisation : ISO/IEC 27001, *Management de la sécurité de l'information* [17]

Pour s'assurer que les renseignements réglementés numériques sont protégés, le titulaire de permis devrait mettre en œuvre les mesures appropriées. Les mesures possibles comprennent ce qui suit :

- limiter l'accès aux fichiers numériques aux seules personnes ayant un besoin de savoir et disposant d'une habilitation de sécurité appropriée ou d'une vérification de la fiabilité
- détecter les accès non autorisés aux fichiers par des personnes qui n'ont pas un besoin de savoir
- chiffrer les fichiers stockés en utilisant des algorithmes de cryptographie certifiés par une autorité technique nationale
- créer et vérifier les totaux des contrôles cryptographiques des documents électroniques afin de détecter toute falsification (p. ex., signatures numériques, condensés de message)
- s'assurer que la protection est étendue aux copies de sauvegarde des documents (p. ex., les copies utilisées pour assurer la continuité des activités ou la reprise après sinistre)

La CCSN propose que les titulaires de permis gèrent le risque lié à la sécurité des renseignements dans le cadre de leur programme de sécurité nucléaire et qu'ils mettent en œuvre des mesures pour protéger les renseignements selon une approche graduelle.

La CCSN aimerait savoir ce qui suit :

Q5. Quelles normes ou orientations spécifiques avez-vous mises en application pour protéger les renseignements réglementés et autres renseignements de nature délicate sur vos systèmes d'information?

Q6. Existe-t-il d'autres sources d'orientation pour la protection de vos systèmes d'information qui vous conviendraient?

Q7. Votre organisation serait-elle en mesure de mettre en œuvre les exemples de mesures énumérés ci-dessus?

3.5.5 Stockage et élimination des renseignements de nature délicate

En vertu du paragraphe 28(1) du RGSRN, chaque titulaire de permis doit conserver les renseignements réglementés pendant la période précisée dans la règlementation et applicable à son activité autorisée. Si aucune période n'est précisée, le titulaire de permis doit conserver les renseignements réglementés pendant un an après l'expiration de son permis. Cela s'applique, quelle que soit la forme des renseignements (c.-à-d. documents électroniques ou papier).

Les renseignements réglementés doivent être protégés lorsqu'ils sont stockés. La section 3.5.4 donne des exemples de mesures qui peuvent être employées pour protéger les renseignements réglementés numériques lors de leur utilisation, et nombre d'entre elles peuvent également être appliquées aux informations stockés. Des mesures de sécurité physique et de cybersécurité devraient être envisagées pour détecter les tentatives de vol, de falsification ou de destruction des renseignements réglementés numériques, et ces mesures devraient être renforcées contre les cyberattaques. Les documents énumérés à la section 3.5.4 fournissent des orientations sur les mesures de sécurité applicables au stockage des informations numériques.

Voici quelques exemples d'orientations concernant l'élimination des renseignements :

- Centre canadien pour la cybersécurité, *Nettoyage et élimination d'appareils électroniques* (ITSAP.40.006) et *Nettoyage des supports de TI (ITSP.40.006)* [18]
- Commissaire à l'information et à la protection de la vie privée de l'Ontario, Feuille-info : *Comment se débarrasser des supports électroniques* [19]
- Cornell University : *Best Practices for Media Destruction* [20]

Pour éliminer les renseignements réglementés électroniques, le titulaire de permis pourrait :

- Effacer ou détruire le support en toute sécurité, en fonction de son type
- Assainir les systèmes avant de les éliminer

La CCSN aimerait savoir ce qui suit :

Q8. Quelles mesures précises avez-vous mises en œuvre pour protéger les renseignements réglementés que vous gérez lorsqu'ils ne sont pas utilisés?

Q9. Que pensez-vous des exemples d'orientations fournis?

Q10. Existe-t-il d'autres sources d'orientation en matière d'élimination qu'il conviendrait de mentionner?

3.6 Réponse aux incidents et rapports

Les titulaires de permis sont tenus d'aviser la CCSN de l'accès non autorisé aux renseignements réglementés et de leur divulgation dès qu'ils découvrent qu'ils ont été compromis. Les délais prévus pour la présentation d'un rapport d'événement détaillé décrivant ce qui s'est passé, les mesures prises, etc., sont indiqués dans les documents REGDOC-3.1.1, *Rapports à soumettre par les exploitants de centrales nucléaires* [21], REGDOC-3.1.2 : Exigences relatives à la production de rapports, tome 1 : Installations nucléaires de catégorie I non productrices de puissance et mines et usines de concentration d'uranium [22], et REGDOC-3.1.3, Exigences relatives à la production de rapports pour les titulaires de permis de déchets de substances nucléaires, les installations nucléaires de catégorie II et les utilisateurs d'équipement réglementé, de substances nucléaires et d'appareils à rayonnement [23], selon le type de titulaire de permis.

Pour répondre à ces exigences réglementaires, les titulaires de permis doivent élaborer et mettre en œuvre ce qui suit :

- systèmes pour déterminer les tentatives non autorisées d'accès aux renseignements réglementés
- systèmes pour signaler les incidents réels de compromission
- procédures d'intervention pour gérer les événements
- mécanismes de déclaration

Des orientations concernant la planification et le traitement des incidents de sécurité informatique sont présentées dans les documents suivants :

- National Institute of Standards and Technology (NIST) : SP 800-61 Rev 2, *Computer Security Incident Handling Guide* [24]
- AIEA : TLD-005, *Computer Security Incident Response Planning for Nuclear Facilities* [25]

- Sécurité publique Canada, *Élaboration d'un plan d'intervention en cas d'incident de la technologie opérationnelle et de la technologie de l'information* [26]

La CCSN aimerait savoir ce qui suit :

Q11. En termes d'intervention et de déclaration des incidents, quelles mesures avez-vous actuellement en place pour surveiller et traiter les incidents de sécurité?

Q12. Quels impacts et défis prévoyez-vous pour la mise en œuvre des mesures suggérées?

Q13. Y a-t-il d'autres mesures qui, selon vous, devraient être incluses?

3.7 Évaluation de l'efficacité et amélioration continue

Les mesures de sécurité, y compris les programmes, les politiques, les plans, etc., doivent toujours évoluer pour répondre aux menaces. Comme le contexte des risques change avec le temps, la CCSN suggère aux titulaires de permis qui produisent ou gèrent des renseignements réglementés de mettre en place des mécanismes pour réviser et mettre à jour périodiquement toutes les mesures de sécurité afin d'atténuer les menaces et les risques.

La fréquence des revues et des mises à jours devrait être définie et respectée Le titulaire de permis devrait également entreprendre des examens spéciaux à la suite d'événements majeurs, par exemple un incident survenu dans l'installation ou ailleurs dans l'industrie, ou à la suite de modifications apportées à une politique, une menace ou un règlement. L'examen devrait s'appliquer à tous les niveaux ayant des responsabilités en matière de sécurité nucléaire. Des rapports devraient être produits pour documenter toute lacune ou tout domaine nécessitant une intervention.

Des plans de gestion du changement devraient être élaborés pour améliorer les mesures existantes ou mettre en œuvre des mesures de sécurité supplémentaires afin de protéger les renseignements réglementés. Ces plans devrait inclure, autant que possible, des délais précis pour la mise en œuvre et toute mesure de rendement associée afin d'en démontrer l'efficacité.

Les modifications apportées aux mesures de sécurité devraient être communiquées aux employés du titulaire de permis lorsque cela est possible.

La CCSN aimerait savoir ce qui suit :

Q14. La CCSN a décrit les étapes possibles à suivre pour évaluer l'efficacité des mesures de sécurité. Êtes-vous d'accord avec ces étapes? Quels impacts ces activités auraient-elles sur votre organisation si elles étaient rendues obligatoires?

4. Cybersécurité pour les activités autorisées par la CCSN

La CCSN réglemente des milliers de titulaires de permis, chacun exerçant ses activités dans des environnements différents qui présentent des caractéristiques et des risques uniques. Comme nous l'avons mentionné, l'un de ces risques est la perturbation de l'exploitation sûre et sécuritaire des activités autorisées par des cyberattaques.

Les titulaires d'un permis d'exploitation d'un réacteur de puissance, d'un permis d'exploitation d'un établissement et d'essais de recherches nucléaires ou d'un permis de déclassement d'un

établissement et d'essais de recherches nucléaires, sont tenus de mettre en œuvre et de tenir à jour des programmes de cybersécurité dans le cadre de leurs programmes de sécurité nucléaire. Un élément de leurs programmes de cybersécurité consiste à mettre en œuvre des mesures de cybersécurité pour protéger les systèmes et les fonctions afin d'éviter toute compromission. À l'heure actuelle, comme le montre le tableau 1, la mise en œuvre d'un programme de cybersécurité n'est pas une exigence pour certaines autres activités autorisées. À la suggestion du Service consultatif international sur la protection physique (SCIPP) de l'AIEA [2] lors de sa mission de 2015, les experts de la CCSN ont évalué les risques cybernétiques associés à toutes les installations et activités nucléaires autorisées en répertoriant les titulaires de permis qui pourraient être les plus à risque et en déterminant les mesures de sécurité possibles pour réduire ces risques à des niveaux acceptables.

4.1 Détermination des autres activités autorisées pouvant être à risque

Le personnel de la CCSN a effectué un examen interne et a répertorié toutes les installations nucléaires autorisées et les titulaires de permis de substances nucléaires pour lesquels des programmes ou des mesures de cybersécurité sont justifiés. La CCSN propose que les activités autorisées et les titulaires de permis énumérés dans les tableaux 2 et 3 de la section 1.1 soient tenus d'établir un programme ou des mesures de cybersécurité proportionnels au risque de compromission.

4.2 Marche à suivre proposée pour les autres titulaires de permis pouvant être à risque

La marche à suivre proposée par la CCSN en ce qui concerne les exigences et les orientations en matière de cybersécurité pour les titulaires de permis pouvant être à risque consiste à répartir les titulaires de permis dans les groupes énumérés dans le tableau 1, selon une approche graduelle fondée sur le risque.

Les sections du présent document qui décrivent les exigences et les orientations potentielles pour ces groupes de titulaires de permis sont présentées dans le tableau 5. La section 5 donne un aperçu des principes de cybersécurité, afin d'offrir des renseignements et un contexte supplémentaires pour les exigences et orientations potentielles.

Tableau 5 : Marche à suivre pour assurer la cybersécurité des systèmes et fonctions de SSPUG

Type de permis ou d'activité	Marche à suivre
Sites à sécurité élevée	Section 6
Installations, y compris les réacteurs de recherche, détenant des matières nucléaires de catégorie III	Section 7
Titulaires de permis sélectionnés de substances nucléaires (tableau 3)	Section 8
Entités qui transportent ou font transporter des matières nucléaires ou des substances nucléaires de catégories I, II ou III	Section 9

5. Principes : Programme de cybersécurité, mesures de cybersécurité, approche graduelle, défense en profondeur

Cette section décrit certains principes clés de la cybersécurité qui peuvent être utilisés comme base pour établir la cybersécurité. Elle est fournie à titre d'information uniquement. Les

exigences et les orientations destinés à des groupes spécifiques de titulaires de permis sont décrits dans les sections 6 à 9.

5.1 Programme de cybersécurité

Un programme de cybersécurité définit les rôles, les responsabilités et les procédures utilisés par une installation pour atteindre ses objectifs de cybersécurité. La CCSN s'attend à ce que des programmes de cybersécurité soient mis en œuvre et tenus à jour afin de garantir que les systèmes informatiques qui exécutent ou soutiennent les fonctions de SSPUG sont protégés contre les cyberattaques.

Le document de la Collection Sécurité nucléaire de l'AIEA NSS 17, *La sécurité informatique dans les installations nucléaires* [27], fournit un cadre recommandé pour les installations nucléaires, qui comprend les principaux éléments suivants :

1. Organisation et responsabilités
2. Gestion des biens
3. Évaluation des risques, des vulnérabilités et de la conformité
4. Conception de la sécurité du système de gestion et gestion de la configuration
5. Procédures de sécurité opérationnelles
6. Gestion du personnel

Le document NSS 17 [27] fournit des détails supplémentaires sur ces éléments. La norme CSA N290.7 [1] présente également des éléments d'un programme de cybersécurité.

5.2 Mesures de cybersécurité

Les mesures de sécurité nucléaire empêchent un adversaire de réaliser des actes malveillants touchant les matières nucléaires, les matières radioactives, les installations connexes ou les activités connexes. Les mesures de sécurité nucléaire permettent également de détecter de tels événements et d'y réagir[2]. Ces mesures servent à :

- prévenir, retarder et détecter les actes malveillants et non autorisés, et intervenir
- atténuer les conséquences de ces actes
- se remettre des conséquences de ces actes

Les mesures de cybersécurité sont un élément essentiel de la sécurité nucléaire protégeant les systèmes informatiques qui exécutent ou soutiennent les fonctions de SSPUG contre les cyberattaques. Ces mesures visent à :

- rendre les systèmes informatiques moins vulnérables aux actes malveillants
- empêcher les actes non intentionnels et/ou non malveillants de porter atteinte à la cybersécurité
- réduire les conséquences des actes malveillants (p. ex., grâce à des mesures qui répondent aux cyberattaques pour les empêcher de se propager)

[2] AIEA, *Objectif et éléments essentiels du régime de sécurité nucléaire d'un État*, Collection Sécurité nucléaire de l'AIEA nº 20, AIEA, Vienne (2013).

Les mesures de cybersécurité sont un élément de la sécurité nucléaire qui protège les systèmes informatiques qui exécutent ou soutiennent les fonctions SSEPS contre les cyberattaques. Ces mesures :

- rendent les systèmes informatiques moins sensibles aux actes malveillants
- empêchent les actes non intentionnels/non malveillants de dégrader la cybersécurité
- réduire les conséquences des actes malveillants (par exemple, mesures qui répondent aux cyberattaques pour les empêcher de se propager).

Les mesures de cybersécurité peuvent être de nature physique, technique ou administrative, et sont soutenues par d'autres mesures, notamment la protection physique, la sécurité du personnel et la sécurité d'information.

La *Directive sur la gestion de la sécurité* [28] du Secrétariat du Conseil du Trésor définit les pratiques essentielles à la protection des systèmes de sécurité informatique du gouvernement du Canada. De plus, le *Manuel de la sécurité des contrats* [29] de Services publics et Approvisionnement Canada décrit les procédures que doivent appliquer les entrepreneurs pour protéger l'information et les biens du gouvernement. Le contenu de ces deux documents peut être adapté pour sécuriser les renseignements réglementés élaborés et gérés par les titulaires de permis.

En outre, les documents suivants décrivent les composantes d'un plan de sécurité visant à protéger les renseignements et les systèmes informatiques. Ces documents comprennent également des orientations et des recommandations sur la protection des technologies opérationnelles utilisées pour assurer les fonctions de SSPUG :

- N290.7-14, *Cybersécurité pour les centrales nucléaires et les installations dotées de petits réacteurs* [1]
- AIEA, Collection Sécurité nucléaire n° 23-G, *Sécurité de l'information nucléaire* [13]
- AIEA, Collection Sécurité nucléaire n° 17, *La sécurité informatique dans les installations nucléaires* [27]
- AIEA, Collection Sécurité nucléaire n° 33-T, *Computer Security of Instrumentation and Control Systems at Nuclear Facilities* [30]

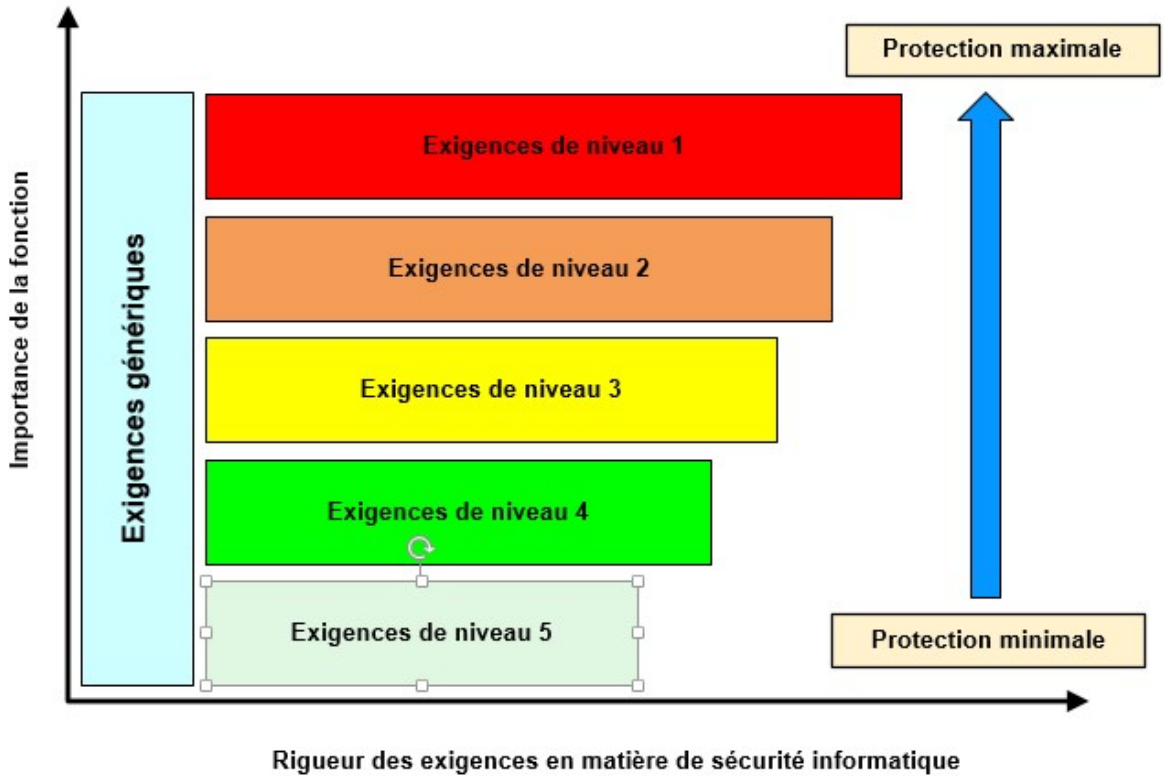
5.3 Approche graduelle fondée sur le risque

Une approche graduelle fondée sur le risque est un élément fondamental de la sécurité nucléaire, auquel la rigueur des exigences de sécurité étant proportionnelle aux conséquences d'un acte malveillant. Dans le contexte de la cybersécurité d'un système, la rigueur des mesures à appliquer devrait être proportionnelle aux conséquences d'une cyberattaque qui compromettrait une fonction de SSPUG exécutée par ce système.

Un moyen standard de mettre en œuvre une approche graduelle à la cybersécurité consiste à définir un ensemble de niveaux de cybersécurité, chacun ayant un niveau différent de protection de la sécurité, et à assigner des systèmes informatiques à ces niveaux en fonction des conséquences de la compromission des fonctions de SSPUG réalisées par ces systèmes informatiques. La figure 2 présente un exemple tiré du document NSS 17 de l'AIEA [27] présentant 5 niveaux de protection. Dans cet exemple, les exigences de sécurité génériques s'appliquent à toutes les fonctions, puis, à mesure que l'importance (p. ex., sur le plan de la sûreté ou de la sécurité) d'une fonction augmente, la rigueur des exigences de sécurité s'accroît, de sorte que les biens les plus importants sont protégés au niveau le plus élevé.

En utilisant plusieurs niveaux de sécurité, on peut réduire la surprotection des biens mais cela va de diminuer le niveau d'effort requis pour sécuriser l'installation ou l'activité. Un exemple utilisant 3 niveaux (élevé, modéré, faible) est présenté dans la norme CSA N290.7 [1].

Figure 2 : Illustration de l'approche graduelle utilisant le concept du niveau de sécurité (adapté de [27])



5.4 Défense en profondeur

La défense en profondeur en matière de cybersécurité nécessite des couches successives de mesures de cybersécurité qui doivent être surmontées ou contournées par un adversaire afin de compromettre les systèmes réalisant des fonctions de SSPUG [30]. Elle nécessite également des mesures diverses et indépendantes en termes de type (p. ex., physique, administratif et technique) et de fonction (p. ex., détecter, retarder, réagir et rétablir).

Le document NSS 17 de l'AIEA [27] propose une approche pour mettre en œuvre la défense en profondeur en définissant et en établissant une architecture de cybersécurité défensive et en déployant des mesures de cybersécurité au sein de cette architecture. Selon l'approche du document NSS 17 de l'AIEA [27], les zones de cybersécurité sont utilisées comme fondement pour créer une défense en profondeur.

Une zone est un regroupement logique et physique de biens ayant des exigences de protection similaires, établi dans le but de simplifier l'application et la gestion des mesures de cybersécurité.

Le degré de protection requis pour chaque zone est basé sur la conséquence la plus importante, sur le plan de la sécurité nucléaire, découlant de la compromission des systèmes dans cette zone. La disposition des zones au sein de l'architecture de cybersécurité défensive permet d'établir une défense en profondeur en obligeant un adversaire à franchir les limites de plusieurs zones protégées pour cibler des systèmes réalisant des fonctions de SSPUG.

L'approche pratique recommandée dans le document NSS 17 de l'AIEA [27] consiste à :

- répartir les systèmes informatiques en zones (d'après les exigences de sécurité communes, comme leur niveau de sécurité, selon ce qui est indiqué à la section 5.3)
- établir les limites physiques et logiques des zones
- spécifier les règles de circulation des données entre les zones
- utiliser des mesures de cybersécurité aux limites des zones pour faire respecter ces règles et détecter les violations de la politique de sécurité
- déployer des mesures au sein des zones

En suivant l'approche ci-dessus, on peut obtenir une configuration des zones qui contribue à l'établissement d'une défense en profondeur.

La CCSN aimerait savoir ce qui suit :

Q15. Que pensez-vous de l'application de l'approche graduelle et de la défense en profondeur en matière de cybersécurité pour votre activité autorisée?

6. Exigences potentielles de cybersécurité pour les sites à sécurité élevée

La section suivante s'applique à tous les sites à sécurité élevée (SSE). Les modifications proposées au RSN exigeraient que ces sites évaluent leur vulnérabilité aux cybermenaces et que les cybermenaces soient incluses dans les EMR des titulaires de permis. L'objectif de cette proposition est de s'assurer que les titulaires de permis sont en mesure de détecter et de contrer les cyberattaques qui ciblent les renseignements de nature délicate, y compris les renseignements règlementés et les systèmes réglementés remplissant des fonctions importantes pour la sûreté et la sécurité nucléaires, la préparation aux situations d'urgence et les garanties. À la suite de ce changement proposé, les titulaires de permis touchés devront, dans le cadre de leur programme de sécurité global, élaborer un programme de cybersécurité et des mesures pour gérer les risques indiqués dans leurs EMR. Pour chaque MCP d'un site à sécurité élevée qui n'inclut pas la norme N290.7 [1] comme document du fondement d'autorisation aux fins de la vérification de la conformité, la CCSN propose que la norme N290.7 [1] devienne une publication du fondement d'autorisation, dans la section du MCP de l'installation traitant des critères de vérification de la conformité. Ainsi, la mise en œuvre d'un programme de cybersécurité conforme à la norme N290.7 sera obligatoire.

La CCSN aimerait savoir ce qui suit :

Q16. Dans le cas des titulaires de permis de SSE touchés par l'exigence proposée de mettre en œuvre un programme de cybersécurité conforme à la norme N290.7, cette exigence serait-elle appropriée? Dans la négative, quelles exigences en matière de cybersécurité seraient appropriées et pourquoi?

7. Exigences et orientations potentielles en matière de cybersécurité pour la protection des installations (y compris les réacteurs de recherche) ayant des matières nucléaires de catégorie III, et pour les accélérateurs de catégorie IB

La section suivante s'applique aux titulaires de permis figurant dans le tableau 2. Les modifications proposées au RSN exigeraient que ces sites évaluent leur vulnérabilité aux cybermenaces et que les cybermenaces soient incluses dans les EMR des titulaires de permis. L'objectif de cette exigence proposée est de s'assurer que les titulaires de permis sont en mesure de détecter et de contrer les cyberattaques ciblant les renseignements de nature délicate, y compris les renseignements règlementés et les systèmes réglementés qui remplissent des fonctions importantes pour la sûreté et la sécurité nucléaires, la préparation aux situations d'urgence et les garanties. Avec cette proposition, les titulaires de permis touchés devront, dans le cadre de leur programme de sécurité global, élaborer un programme de cybersécurité et des mesures pour gérer les risques relevés dans leurs EMR.

Le personnel de la CCSN et les représentants de l'industrie canadienne ont corédigé la norme N290.7 [1] qui traite de la « cybersécurité dans les centrales nucléaires et les petites installations de réacteur pour les systèmes et composants informatiques suivants :

(a) systèmes importants pour la sûreté nucléaire
(b) sécurité nucléaire
(c) préparation aux situations d'urgence
(d) fiabilité de la production
(e) garanties
(f) biens ou systèmes auxiliaires qui, s'ils étaient compromis, exploités ou défaillants, pourraient avoir un impact négatif sur les éléments a), b), c), d) ou e) ».

La norme N290.7 [1] est basée sur les principes de cybersécurité décrits à la section 5, et compte tenu de la portée de la norme, la CCSN estime qu'il est raisonnable de l'appliquer en utilisant une approche graduelle pour les titulaires de permis énumérés dans le tableau 2.

La CCSN aimerait savoir ce qui suit :

Q17. Les éléments énoncés dans la norme conviendraient-ils aux titulaires de permis énumérés dans le tableau 2 de la section 1.1, comme les petites installations dotées d'un réacteur nucléaire, les installations de traitement du combustible, les installations de conversion du combustible et les accélérateurs de catégorie IB, si la norme est appliquée selon une approche graduelle et que les titulaires de permis peuvent proposer d'autres méthodes, approches, mesures de sécurité, etc. et que les titulaires de permis peuvent proposer d'autres méthodes, approches, mesures de sécurité, etc.? Dans la négative, quelles mesures seraient appropriées?

Q18. Êtes-vous d'accord avec l'exigence proposée que tous les titulaires de permis qui mènent des activités impliquant des matières nucléaires de catégorie III mettent en œuvre un programme de cybersécurité? Dans la négative, pourquoi?

8. Exigences et orientations potentielles en matière de cybersécurité pour les titulaires de permis de substances nucléaires

Cette section s'applique aux sources scellées de catégories 1 et 2, y compris les activités représentatives indiquées dans le tableau 3.

8.1 Exigences et orientations potentielles en matière de cybersécurité des systèmes de protection physique

Il incombe aux titulaires de permis de mettre en œuvre des mesures de sécurité physique pour empêcher le retrait non autorisé de sources scellées ou de matières nucléaires et pour prévenir le sabotage des activités autorisées.

Les mesures de sécurité physique (p. ex., caméras numériques, alarmes, détecteurs de mouvement, détection d'entrée forcée, systèmes de communication, etc.) ne sont plus exclusivement des dispositifs câblés et autonomes. Ce sont souvent des dispositifs numériques et ils sont de plus en plus souvent reliés par des réseaux informatiques. On peut les contrôler à distance pour évaluer rapidement les incidents potentiels et dépêcher du personnel de sécurité sur le site et hors site, par exemple des agents de sécurité et des policiers. Les systèmes téléphoniques s'appuient également de plus en plus sur les technologies numériques, les lignes terrestres en cuivre étant remplacées par des téléphones utilisant la voix par protocole Internet (voix sur IP).

Les adversaires pourraient utiliser des cyberattaques pour compromettre les technologies numériques afin de modifier leur fonction ou leur rendement. Lorsque ces technologies sont utilisées pour les systèmes de protection physique, elles offrent à un adversaire des possibilités supplémentaires s'il désire planifier un acte malveillant visant des matières radioactives. Par exemple, dans le cadre d'une attaque combinée, un adversaire pourrait effectuer une cyberattaque pour dégrader un système de protection physique afin d'augmenter ses chances de réussir à subtiliser une source scellée ou une matière radioactive ou d'obtenir un accès non autorisé à l'installation.

Par exemple, un adversaire pourrait lancer une cyberattaque pour :

- accéder à un système de contrôle de l'entrée pour obtenir des numéros d'identification personnels (NIP) pour les serrures sans clé
- transmettre un ancien flux vidéo provenant d'une caméra numérique aux postes de sécurité (poste central et poste à distance) ou geler l'image envoyée par la caméra
- modifier un système de détection d'intrusion pour désactiver les alarmes afin d'éviter qu'elles ne soient transmises aux poste central de sécurité et poste à distance

La CCSN estime donc qu'il est raisonnable de s'attendre à ce que les titulaires de permis tenus de mettre en œuvre des systèmes de protection physique vérifient si leurs mesures de sécurité physique, y compris leurs postes de surveillance, sont vulnérables aux cyberattaques, et également qu'ils renforcent leurs systèmes de protection physique. Étant donné que les vulnérabilités peuvent varier d'un titulaire de permis et d'un système à l'autre, il serait difficile pour la CCSN de fournir des exigences normatives pour chaque titulaire de permis afin d'atteindre cet objectif. Par conséquent, la CCSN préférerait recourir à une approche fondée sur le rendement pour atténuer les effets négatifs des cyberattaques. Les exigences fondées sur le rendement seraient définies dans une orientation supplémentaire fournie dans la série de REGDOC-2.12.

La CCSN peut exiger des titulaires de permis qu'ils démontrent comment ils atteindront cet objectif au mieux de leur capacité en fournissant à la CCSN des preuves à l'appui de leurs affirmations. Toutes les preuves étayant leur dossier de sécurité devraient provenir de sources réputées et vérifiables par la CCSN. Dans les cas où des approches expérimentales ou nouvelles sont utilisées, les preuves fournies devraient pouvoir être reproductibles.

La CCSN peut également exiger que les titulaires de permis mettent en œuvre les meilleures pratiques de l'industrie en matière de cybersécurité afin de défendre leurs systèmes de protection

physique contre les cyberattaques. Un exemple de bonne pratique pour les utilisateurs de sources radioactives est présenté dans le document *Cybersecurity Best Practices for Users of Radioactive Sources* [31] de l'Office of Radiological Security de la National Nuclear Security Administration (NNSA).

Les documents suivants présentent des attentes ou des orientations potentielles en matière de sécurité des systèmes de protection physique :

- N290.7, *Cybersécurité pour les centrales nucléaires et les installations dotées de petits réacteurs* [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].

Remarque : Les titulaires de permis peuvent confier en sous-traitance la conception et l'installation de leurs systèmes, mesures et interventions en matière de sécurité à des fournisseurs tiers. Le cas échéant, la CCSN peut juger raisonnable d'exiger que les titulaires de permis soient en mesure de démontrer que l'entrepreneur a mis en œuvre des moyens pour prévenir les intrusions cybernétiques et qu'il peut maintenir la fonctionnalité continue des mesures de sécurité qu'il a installées au nom du titulaire de permis.

La CCSN aimerait savoir ce qui suit :

Q19. Quelles mesures avez-vous mises en œuvre pour protéger vos mesures de sécurité physique contre les cyberattaques?

Q20. Pouvez-vous indiquer les impacts potentiels si la CCSN vous obligeait à mettre en œuvre des mesures de cybersécurité pour vos systèmes de protection physique (y compris le poste central de sécurité) contre les cyberattaques?

8.2 Exigences et orientations potentielles en matière de cybersécurité aux fins de sûreté, de préparation aux situations d'urgence et de garanties

Une approche graduelle est un élément important de la gestion des risques pour la sécurité. La profondeur et l'étendue des mesures de sécurité doivent être proportionnelles au risque de compromission des systèmes informatiques qui exécutent ou soutiennent les fonctions de sûreté, de préparation aux situations d'urgence et de garanties.

Dans cette optique, la CCSN détermine les exigences réglementaires et les orientations qui conviendraient aux activités représentatives présentées dans le tableau 3. La CCSN a l'intention de mettre en place des exigences et des orientations concernant l'application de mesures de cybersécurité pour les systèmes de sûreté, de préparation aux situations d'urgence et de garanties. Ces exigences seront définies dans les orientations supplémentaires fournies dans la série de REGDOC-2.12.

Les étapes proposées pour mettre en place et maintenir des mesures de cybersécurité sont les suivantes :

1) Examen et détermination de tous les systèmes, fonctions, systèmes auxiliaires ou dispositifs qui, s'ils étaient compromis par une cyberattaque, entraîneraient des conséquences négatives.

Ces dernières comprennent tout rejet qui pourrait affecter la santé des travailleurs ou du public, ou qui pourrait endommager l'environnement. La sécurité des patients, qui est réglementée par Santé Canada, est considérée comme une conséquence négative qui, toutefois, ne ressort pas du présent document.

2) Détermination de toutes les menaces qui pèsent sur les systèmes, dispositifs ou fonctions relevés à l'étape précédente. Les sources de menaces sont disponibles dans le domaine public et privé, et comprennent l'Évaluation des cybermenaces nationales [33] du Canada produite par le Centre canadien pour la cybersécurité.
3) Quantification des menaces, autant que possible, d'après la probabilité que celles-ci se produisent, et quantification de leurs impacts. Tous les impacts (radiologiques et autres) doivent être déterminés. Au cours de cette étape, les titulaires de permis devraient également relever toutes les vulnérabilités associées aux systèmes qu'ils ont mis en place, ainsi que toutes les mesures de sécurité existantes.
4) Mise en œuvre de mesures correctives pour supprimer les vulnérabilités, ou de mesures de cybersécurité pour tenir compte des risques et des vulnérabilités relevés à l'étape précédente.
5) Élaboration d'une capacité d'intervention en cas d'incident afin de détecter les cyberattaques, de les contrer, de tirer des leçons, de mettre en œuvre des mesures correctives et de présenter des rapports à la CCSN. Les exigences concernant la réponse aux incidents seront similaires à celles qui sont prévues pour la sécurité de l'information, à la section 3.5.
6) Examen régulier de l'efficacité des mesures de cybersécurité, mise en œuvre des changements, documentation des changements et communication de ceux-ci, le cas échéant.

Les technologies opérationnelles (TO) consistent en matériel et logiciels qui surveillent, communiquent et contrôlent les composantes physiques (c.-à-d. les systèmes et équipements de procédés industriels). Ces technologies peuvent servir à assurer des fonctions importantes pour la sûreté nucléaire, la sécurité nucléaire, la préparation aux situations d'urgence et les garanties. La compromission des TO peut entraîner des dommages aux systèmes ou aux équipements, la non-détection d'une condition dangereuse, ou encore toucher autrement les fonctions établies. Les méthodes et les mesures utilisées pour assurer la cybersécurité des TO sont différentes de celles qui sont utilisées pour protéger la technologie de l'information (TI).

Les documents suivants peuvent fournir des attentes et des orientations potentielles pour la protection des TO :

- N290.7, *Cybersécurité pour les centrales nucléaires et les installations dotées de petits réacteurs* [1]
- NIST : SP 800-82, *Guide to Industrial Control Systems Security* [34]

Des mesures de sécurité supplémentaires peuvent être requises en fonction des opérations, des menaces et des risques propres à chaque titulaire de permis.

La CCSN aimerait savoir ce qui suit :

Q21. Croyez-vous que les contrôles de base en matière de cybersécurité pour les systèmes informatiques des petites et moyennes organisations, établis par le Centre canadien pour la cybersécurité, conviennent aux activités autorisées de votre organisation? Pourquoi? Dans la négative, pourquoi?

Q22. Êtes-vous d'accord avec les étapes pour établir et maintenir les mesures de cybersécurité suggérées à la section **Error! Reference source not found.**? Pourquoi? Dans la négative, pourquoi? Quelle méthode utilisez-vous actuellement (ou recommandez-vous d'utiliser) pour établir des mesures de cybersécurité?

Q23. Quels impacts ces exigences et orientations potentielles auraient-elles sur vos activités autorisées?

Q24 : Quelle norme de cybersécurité utilisez-vous (ou recommandez-vous d'utiliser) pour vos systèmes TO qui soutiennent la sûreté, la préparation aux situations d'urgence et les mesures de protection?

Q25 : Pour les activités impliquant la sécurité des patients, d'autres organismes de réglementation exigent-ils des exigences en matière de cybersécurité? Dans l'affirmative, quelles sont ces exigences?

9. Exigences et orientations potentielles en matière de cybersécurité pour les entités qui transportent ou font transporter des matières nucléaires ou des sources scellées

Cette section s'applique aux entités qui transportent ou font transporter ce qui suit :

1) les matières nucléaires de catégories I, II et III
2) les sources scellées de catégories 1 et 2.

Le partenariat « douanes et commerce contre le terrorisme » (CTPAT) du Département américain de la sécurité intérieure, a publié sur son site Web des orientations concernant la sécurité des différents modes de transport. Ces orientations comprennent des conseils en matière de cybersécurité. Par exemple, la section 4 des critères *Minimum Security Criteria – Highway Carriers* [35] présente des mesures de cybersécurité possibles applicables aux transporteurs routiers.

9.1 Exigences et orientations potentielles en matière de cybersécurité pour les entités qui transportent ou font transporter des matières nucléaires de catégories I, II et III

En ce qui concerne les matières nucléaires de catégories I et II, le plan de sécurité du transport (PST) définit les exigences relatives aux mesures de sécurité et aux communications. Lorsque ces exigences sont satisfaites par des moyens numériques, le PST doit inclure des mesures de cybersécurité. Lorsque les communications s'appuient sur la transmission de données numériques, la sécurité de l'information doit être appliquée pour garantir la confidentialité, l'intégrité et la disponibilité d'information numériques.

Les titulaires de permis qui organisent l'expédition de matières de catégories I, II et III sont assujettis à des exigences concernant les programmes de cybersécurité et de protection de l'informtion définies dans les sections précédentes du présent document de travail. La CCSN propose que ces programmes soient appliqués pour gérer les mesures de cybersécurité et de

protection de l'information dans le cadre du PST. La CCSN propose que ces programmes traitent des situations où le transport est assuré par une tierce partie.

La CCSN aimerait savoir ce qui suit :

Q26. Pensez-vous que les mesures de cybersécurité contenues dans les orientations américaines du CTPAT ci-dessus seraient appropriées pour votre organisation? Dans la négative, pourquoi? Quelles mesures supplémentaires ou autres recommanderiez-vous?

Q27. Êtes-vous d'accord avec la proposition de la CCSN selon laquelle les titulaires de permis devraient gérer la cybersécurité pour le transport dans le cadre de leurs programmes de cybersécurité et de sécurité de l'information? Dans la négative, comment suggérez-vous de gérer la cybersécurité et la sécurité de l'information pour le transport?

9.2 Exigences et orientations potentielles en matière de cybersécurité pour les entités qui transportent ou font transporter des sources scellées de catégories 1 et 2

Dans le cas des sources scellées de catégories 1 et 2, un plan de sécurité du transport (PST) définit les exigences concernant les mesures de sécurité et les communications. Pour les sources scellées de catégorie 2, on emploie un PST générique.

La CCSN propose que les PST comprennent des mesures afin de :

1) protéger les mesures de sécurité physique qui reposent sur la technologie numérique (le cas échéant) pour contrer les cyberattaques
2) protéger la confidentialité, l'intégrité et la disponibilité des renseignements réglementés
3) protéger la confidentialité, l'intégrité et la disponibilité des canaux de communication numériques

La CCSN propose que le processus d'approvisionnement comprenne des éléments qui traitent des situations où le transport est assuré par une tierce partie.

La CCSN aimerait savoir ce qui suit :

Q28. Pensez-vous que les mesures de cybersécurité contenues dans les orientations du CTPAT citées en référence seraient appropriées pour votre organisation? Dans la négative, pourquoi? Quelles mesures supplémentaires ou autres recommanderiez-vous?

Q29. Êtes-vous d'accord avec la proposition de la CCSN selon laquelle le PST devrait inclure des mesures visant à protéger les renseignements réglementés, les communications numériques et les mesures de sécurité physique qui reposent sur la technologie numérique?

Annexe A : Exemples d'information nucléaire et liste des classifications recommandées

Source : AIEA, Collection Sécurité nucléaire n° 23-G, Annexe II

Catégorie	Type de document	Description	Sensibilité	Classification recommandée
Plans	Plans de sécurité des installations	Ils contiennent généralement des descriptions détaillées des mesures de sécurité en vigueur sur un site et des renseignements précis concernant l'endroit où les matières sont entreposées sur le site concerné. Pour les installations nucléaires, les plans contiennent également des renseignements sur d'autres zones essentielles pour l'exploitation du site. Dans le cas des sites à sécurité élevée, ces renseignements portent la classification secrète.	Sensible	Confidentiel jusqu'au niveau secret
Rapports relatifs à la sécurité	Rapports d'enquête, d'inspection et d'évaluation sur la sécurité et autres rapports sur les mesures de protection physique ou de sécurité technique appliquées sur un site ou dans une installation	La consultation de ces rapports peut donner à des adversaires des renseignements sur l'emplacement des matières, les mesures prises pour les protéger et les éventuelles vulnérabilités constatées, les aidant ainsi à contourner les mesures de sécurité et à échapper aux contrôles de même nature.	Sensible	Secret
	Rapports présentant des caractéristiques essentielles ou mettant en lumière des prescriptions pour améliorer la sécurité, y compris dans des zones essentielles (s'il y a lieu)	Les informations de cette nature peuvent être utiles à des adversaires qui souhaitent contourner les dispositifs de sécurité et pourraient les aider à s'attaquer à une installation.	Sensible	Secret
	Résultats d'enquêtes sur la sécurité menées sur un site ou dans une installation, y compris celles qui portent sur les fuites et les pertes de renseignements de nature délicate	Les informations de cette nature peuvent être utiles à des adversaires qui souhaitent contourner les dispositifs de sécurité et pourraient les aider à s'attaquer à une installation.	Sensible	Secret
	Rapports décrivant les vulnérabilités du système de gestion de la sécurité et les conséquences d'une défaillance	Les informations de cette nature peuvent être utiles à des adversaires qui souhaitent contourner les dispositifs de sécurité.	Sensible	Secret
Caractéristiques de la construction	Caractéristiques de la construction et de la disposition des lieux où des matières peuvent être entreposées ou traitées, y compris les dessins et les plans conservés sur n'importe quel support, qui montrent des éléments de protection physique servant à prévenir les actes malveillants	Les cartes et plans officiels d'un site peuvent être communiqués si la direction le décide, dans la mesure où ils n'indiquent pas les fonctions d'un bâtiment, les matières qui y sont entreposées, l'emplacement des clôtures de sécurité internes et les autres mesures de sécurité appliquées dans le bâtiment concerné.	Sensible	Jusqu'au niveau secret

Catégorie	Type de document	Description	Sensibilité	Classification recommandée
		La classification dépend de la catégorie ou du niveau d'activité des matières entreposées.		
	Caractéristiques de la construction des zones essentielles dans les centrales nucléaires et les autres installations nucléaires	Les informations de cette nature peuvent aider des adversaires à contourner les dispositifs de sécurité et peuvent éventuellement faciliter le choix d'une cible à des fins de sabotage.	Sensible	Secret
Systèmes de protection	Renseignements sur tout dispositif de protection physique : alarmes, caméras de surveillance, contrôle d'accès, personnel de sécurité, etc.		Sensible	Secret
	Types et emplacement des capteurs des systèmes de détection des intrusions, des caméras de surveillance associées et des schémas de câblage, emplacement des alimentations électriques essentielles et des passages de câbles et programmes d'entretien et de test pour ces équipements		Sensible	Secret
	Renseignements sur les systèmes de contrôle d'accès automatisés, y compris l'emplacement des serveurs informatiques, des serveurs de sauvegarde et de leurs alimentations électriques	Tout renseignement de cette nature serait utile à un adversaire qui souhaiterait contourner les systèmes de sécurité d'une installation.	Sensible	Secret
	Magasins : procédures de sécurité relatives à la délivrance, à la réception et au contrôle du stock de matières; nom des détenteurs de clés autorisés; mesures de surveillance et de gardiennage	Peuvent être utiles à des adversaires qui préparent des actes malveillants.	Sensible	Secret
	Cartes générales montrant la position et les limites d'une installation, mais ne donnant aucun renseignement sur ce qu'elle renferme	Sur Internet, des applications de cartographie en libre accès permettent d'obtenir clairement de telles informations.	Non sensible	Non classifié
	Autres questions liées à la protection physique : emplacement, organisation, effectifs et appareils du poste central de sécurité; emplacement du poste de sécurité secondaire; type de barrière pour la zone intérieure	Tout renseignement de cette nature serait très utile à un adversaire qui souhaiterait contourner les systèmes de sécurité d'une installation nucléaire.	Sensible	Secret

Catégorie	Type de document	Description	Sensibilité	Classification recommandée
Informations relatives à la quantité et à la forme des matières	Informations sur la quantité, le type et la forme des matières nucléaires, sources comprises, reçues ou conservées à des endroits précis dans tous les types de sites et de centrales nucléaires, y compris les lieux exacts où du combustible usé est conservé	Ce type d'information pourrait être utile à des adversaires qui choisissent des cibles lorsqu'ils préparent des attaques.	Sensible	Secret
	Débit – capacité nominale, débit réel et données rétrospectives sur le débit dans une installation soumise au régime des garanties de l'AIEA	Ces informations générales sont souvent publiques, en particulier pour les centrales nucléaires.	Non sensible	Non classifié
	Inventaires nationaux ou locaux d'autres matières radioactives (y compris des matières retirées du service) indiquant leur quantité, leur type, leur forme et leur emplacement exact	Ce type d'information pourrait être utile à des adversaires qui choisissent des cibles lorsqu'ils préparent des attaques pour voler des matières radioactives. Pour ces inventaires, il conviendrait de déterminer quelles informations sont déjà accessibles au public. Ces informations ne sont pas toutes considérées comme de nature délicate. Les méthodes qui s'appuient sur la connaissance du risque aident à déterminer si une information doit être qualifiée de sensible.	Sensible	Non classifié
Transport de matières	Informations sur les mouvements de matières nucléaires de catégories I, II ou III	Ce type d'information pourrait aider à choisir les cibles dans le cadre de la préparation d'actes malveillants mettant en jeu des matières nucléaires pendant leur transport.	Sensible	Secret
	Véhicules hautement protégés (VHP) : Accès visuel à l'intérieur de la cabine du conducteur et du compartiment de chargement; caractéristiques de la conception et de la construction du véhicule relatives à la sécurité physique; conception et contrôle des alarmes, des systèmes d'immobilisation et des clés destinées à des serrures spéciales; clés du compartiment de chargement, clés de secours et code de la serrure à combinaison, si une telle serrure est utilisée; système de géolocalisation du véhicule, si un tel système est installé sur le VHP; fonctionnement du système et communications	Les VHP sont des véhicules spécialement conçus pour transporter des matières nucléaires en toute sécurité. Ainsi, toutes les informations dont le type est énuméré dans la présente section pourraient être utiles à un adversaire préparant une tentative de vol ou de sabotage de matières nucléaires pendant leur transport.	Sensible	Secret

Catégorie	Type de document	Description	Sensibilité	Classification recommandée
	Conteneurs de transport de matières nucléaires : Degré de résistance des conteneurs de transport aux attaques menées par différents moyens; informations sur la conception de conteneurs particuliers (conteneurs spécialement protégés)	Utile pour un adversaire qui prépare un sabotage dans le but de disséminer des matières nucléaires ou qui projette de voler des matières pendant un transport / utile pour un adversaire qui prépare un sabotage dans le but de disséminer des matières nucléaires ou qui projette de voler des matières pendant un transport.	Sensible	Non classifié
	Caractéristiques des conteneurs et données techniques les concernant	Sur Internet, on trouve souvent des informations sur la conception de ces conteneurs, sans renseignements détaillés sur la construction de ce type de matériel.	Non sensible	Non classifié
	Colis de transport : informations sur la conception des colis de transport	Utile pour un adversaire qui prépare un sabotage dans le but de disséminer des matières nucléaires ou qui projette de voler des matières pendant un transport.	Sensible	Non classifié
	Informations sur les mouvements d'autres matières radioactives	Ce type d'information, en particulier s'il concerne le transport de sources de rayonnements puissantes, pourrait être utilisé pour préparer un vol de matières.	Sensible	Non classifié
Systèmes informatiques importants pour la sécurité et la sûreté	Renseignements sur les systèmes informatiques où sont stockées et traitées des renseignements de nature délicate, y compris les systèmes utilisés à des fins de sécurité, l'architecture système, les mesures de sécurité informatique appliquées et l'emplacement des supports de sauvegarde	Informations utiles pour un adversaire qui se prépare à commettre un acte malveillant dans une installation.	Sensible	Secret
	Renseignements sur les systèmes de contrôle d'accès, les systèmes de détection des intrusions, les systèmes d'alarme, les systèmes d'évaluation et de surveillance et sur d'autres fonctions et dispositifs de sécurité; emplacement du matériel et des logiciels de sauvegarde	Informations utiles pour un adversaire qui se prépare à commettre un acte malveillant dans une installation.	Sensible	Secret
	Renseignements sur les systèmes informatiques liés à la sûreté, notamment leur emplacement, leur rôle, les chemins de mise à jour, les alimentations électriques et les sauvegardes	Ces systèmes sont dotés de fonctions de contrôle et de suivi des opérations. Si un adversaire parvenait à les compromettre, il pourrait, au minimum, perturber l'exploitation d'une installation et, dans le pire des cas, les perturbations pourraient provoquer un rejet de matières radioactives.	Sensible	Non classifié

Catégorie	Type de document	Description	Sensibilité	Classification recommandée
Agents de sécurité et forces d'intervention	Agents de sécurité dans une installation : Effectif global et moyens actuels	Rendre publique l'existence d'un plan de ce type peut rassurer la population et avoir un effet dissuasif. Remarque : Rendre publique l'existence d'une force n'est pas un renseignement de nature délicate, mais les capacités de la force sont des renseignements de nature délicate et classifiés.	Sensible	Secret
	Agents de sécurité dans une installation : Effectif et moyens actuels sur un site particulier	Les informations de cette nature peuvent être utiles à un adversaire qui prépare une intrusion dans un site à des fins de sabotage ou de vol.	Sensible	Secret
	Agents de sécurité dans une installation : Taille des équipes sur un site		Sensible	Secret
	Armes et autre matériel spécial mis à la disposition des agents de sécurité et nombre d'utilisateurs entraînés à la manipulation des armes à feu parmi les agents de sécurité d'un site particulier	Toutes les informations qui pourraient aider un adversaire à estimer à l'avance l'ampleur de la réaction et les moyens dont dispose une entité opérationnelle tactique devraient être protégées contre la divulgation.	Sensible	Secret
	Emplacement, moyens, armes et véhicules spéciaux d'intervention de la force d'intervention et délai d'intervention sur un site			Secret
	Plans d'intervention			Secret
	Escortes accompagnant le transport de matières nucléaires : Déploiement et moyens de l'escorte / radiofréquences utilisées pour communiquer avec une force d'intervention ou la police locale	Ces informations pourraient être utiles à un adversaire qui prévoit d'attaquer un convoi.	Sensible	Secret
Comptabilité des matières nucléaires	Description : Principes généraux de la comptabilité des matières nucléaires	Des principes généraux de ce type ont été publiés.	Non sensible	Non classifié
	Description : Questionnaires concernant l'information de conception et la description de celle-ci et emplacement des zones de bilan matières (ZBM) et des points de mesure principaux (PMP)	De telles informations détaillées sur l'emplacement et les quantités de matières nucléaires pourraient être utiles à un adversaire qui prépare un acte malveillant.	Sensible	Non classifié
	Description : Forme physique et chimique des matières qui font l'objet de mesures aux PMP		Sensible	Non classifié
	Données d'instrumentation et de mesures : Précision et exactitude des techniques courantes de laboratoire	Ces informations sont souvent publiques.	Non sensible	Non classifié

Catégorie	Type de document	Description	Sensibilité	Classification recommandée
	Données d'instrumentation et de mesures : Données montrant la sensibilité des mesures ou les seuils d'alarme pour la différence d'inventaire (DI) dans une centrale particulière	Les données relatives à la précision et à l'exactitude des mesures réelles ou caractéristiques, qu'ils soient agrégés ou détaillés, pourraient être utiles à un adversaire qui prépare un vol de matières.	Sensible	Non classifié
	Données relatives aux flux de matières nucléaires et à l'inventaire de telles matières conservées dans les systèmes informatiques, sur supports papier et sur n'importe quel support de stockage	Ces informations pourraient révéler un emplacement et des mouvements de matières nucléaires.	Sensible	Non classifié
	Différence d'inventaire : Données annuelles de DI pour un site qui ne révèle pas la ZBM concernée	Dans de nombreux États, les données annuelles agrégées de DI sont ou peuvent être publiés.	Non sensible	Non applicable
	Différence d'inventaire : DI dans une ZBM ou à un PMP		Sensible	Non classifié
	Différence d'inventaire : Détails d'une enquête sur une DI particulier, sauf si la communication de ces informations a officiellement été autorisée	Cependant, les détails des DI ou les résultats d'une enquête peuvent être utilisés par un adversaire qui cible un site spécifique. Par conséquent, ces informations doivent être qualifiées de sensible.	Sensible	Non classifié Peut être plus élevée selon la nature spécifique de la source
	Différence d'inventaire : Erreur admissible pour une DI ou autres indications précises quant à l'incertitude qui s'attache aux DI		Sensible	Non classifié Peut être plus élevée selon la nature spécifique de la source
Demandes d'autorisation	Demandes d'autorisation qui ne contiennent pas d'informations détaillées sur les mesures de sécurité ni sur le type, la forme et la quantité de matières	Le contenu d'une telle demande varie en fonction du cadre législatif et réglementaire et de l'utilisation finale prévue. Si la demande contient des renseignements de nature délicate qui pourraient être utiles à un adversaire, elle devrait également être traitée comme un renseignement de nature délicate.	Non sensible	Non classifié
	Demandes d'autorisation contenant des informations détaillées, par exemple sur des mesures de sécurité et sur le type, la forme et la quantité de matières	Le contenu d'une telle demande varie en fonction du cadre législatif et réglementaire et de l'utilisation finale prévue. Si la demande contient des renseignements de nature délicate qui pourraient être utiles à un adversaire, elle devrait également être traitée comme un renseignement de nature délicate.	Sensible	Secret

Catégorie	Type de document	Description	Sensibilité	Classification recommandée
Argumentaires de sûreté, documents techniques et autres informations relatives à la sûreté ou à l'environnement	Argumentaires de sûreté de toutes catégories : Éléments détaillés sur les risques ou autres informations qui pourraient être utilisés pour évaluer les conséquences d'un rejet, ou bien renseignements sur les conséquences des rejets	La plupart des renseignements qui figurent dans les argumentaires de sûreté peuvent être rendus publics pour des questions de transparence, mais certains d'entre eux peuvent être considérés comme de nature délicate au regard de la sécurité nucléaire. Remarque : Si un renseignement a des conséquences sur la sécurité nucléaire, on devrait l'évaluer et le classifier au cas par cas.	Sensible	Non classifié
	Argumentaires de sûreté de toutes catégories : Renseignements sur les forces et les faiblesses des procédures, des structures et des systèmes de protection conçus pour contenir, contrôler ou protéger des matières nucléaires ou d'autres matières radioactives	Ces informations détaillées qui figurent dans les argumentaires de sûreté pourraient être utiles à un adversaire pour choisir des cibles et préparer une opération.	Sensible	Non classifié
	Argumentaires de sûreté de toutes catégories : Renseignements sur l'accès au processus de production, qu'il s'agisse du contrôle d'accès physique ou du retrait de matières du processus à des fins de contrôle et de surveillance		Sensible	Non classifié
Plans d'urgence et d'intervention et exercices	Urgence et intervention : Existence d'un plan d'urgence et intervention	Rendre publique l'existence d'un plan de ce type peut rassurer la population et avoir un effet dissuasif.	Non sensible	Non classifié
	Urgence et intervention : Contenu détaillé d'un plan d'urgence et intervention	Les détails du plan pourraient indiquer les moyens, les limites et les délais d'intervention, et pourraient donc être utiles à un adversaire qui prépare une attaque.	Sensible	Confidentiel
	Plans de sécurité d'urgence contenant des informations détaillées	Ces documents contiennent des informations sur les mesures de sécurité en vigueur, sur les moyens de la police ou des agents de sécurité et sur le type d'intervention probable en cas d'incident lié à la sécurité.	Sensible	Confidentiel
	Exercices : Fait qu'un exercice aura ou a eu lieu	Rendre publique l'existence d'exercices peut rassurer la population. Toutefois, il ne faut pas que le niveau de détail fourni, par exemple la date, l'heure ou le lieu d'un futur exercice, puisse être utile à un adversaire.	Non sensible	Non classifié

Catégorie	Type de document	Description	Sensibilité	Classification recommandée
	Exercices : Renseignements sur les exercices de sécurité réalisés sur un site, notamment le scénario, les aspects du plan de sécurité qui font l'objet d'une vérification, la participation éventuelle d'une force d'intervention et les résultats de l'exercice	Donne des informations aux adversaires sur la nature, la taille, les moyens et le délai de réaction de la force d'intervention et des renseignements sur la force d'intervention armée, la nature des tactiques employées et le plan de signalisation.	Sensible	Confidentiel
	Exercices : Renseignements sur les exercices de sécurité	Les exercices de sûreté sont souvent réalisés de manière ouverte et transparente. On peut généralement les considérer comme n'étant pas de nature délicate tant qu'ils ne révèlent pas d'informations détaillées sur des mesures de sécurité.	Non sensible	Non classifié
Informations personnelles	Informations issues des contrôles de fiabilité	Des informations de cette nature pourraient être utilisées pour exercer un chantage ou commettre une extorsion. Dans la plupart des pays, la réglementation relative à la protection de la vie privée impose de protéger ce type d'information.	Sensible	Non classifié
	Informations contenues dans les dossiers individuels			Non classifié
Inventaire des déchets radioactifs	Informations générales sur les inventaires à l'exclusion des informations qui pourraient être exploitées, par exemple le fait que des déchets soient entreposés dans un site particulier ou la quantité totale de déchets sans préciser leur emplacement	Ces informations donnent des renseignements sur les cibles à un adversaire qui prépare un sabotage.	Non sensible	Non classifié
	Informations qui pourraient être utilisées pour commettre un acte malveillant ou qui permettent de repérer un bâtiment particulier dans une installation, ainsi que les matières qu'il contient	Ces informations donnent des renseignements sur les cibles à un adversaire qui prépare un sabotage.	Sensible	Non classifié Informations confidentielles lorsqu'elles sont associées à des détails de sécurité spécifiques
Déclassement	Plans de déclassement de centrale	Les plans de déclassement d'installations sont souvent rendus publics.	Non sensible	Non classifié
	Déchets de déclassement : Fait qu'une installation d'entreposage doive être construite et emplacement de cette installation	Ces informations sont souvent publiques.	Non sensible	Non classifié

Catégorie	Type de document	Description	Sensibilité	Classification recommandée
	Déchets de déclassement : Renseignements sur la construction, les mesures de sécurité et le type de matière qui seront entreposées concernant de nouveaux bâtiments destinés au traitement et à l'entreposage des déchets et des matières contaminées résultant d'activités de traitement effectuées pendant un déclassement	Ces informations peuvent donner des renseignements utiles sur les cibles à un adversaire qui prépare un sabotage. Remarque : Les renseignements de sécurité et les données précises sur la quantité, le type et l'emplacement des déchets sont de nature confidentielle, et le reste des renseignements est probablement non classifié.	Sensible	Secret
Évaluations de la menace et critères appliqués pour déclencher des alertes sur la sécurité	Évaluations de la menace établies par l'État, les autorités nationales de sécurité et d'autres autorités compétentes	Proviennent généralement d'éléments relevant de la sécurité nationale, par exemple des informations obtenues par les services de renseignement. Remarque : Si ces renseignements contiennent des renseignements de nature délicate et détaillés sur la sécurité nationale, on peut les classifier à un niveau supérieur, mais les évaluations à leur sujet peuvent seulement y faire référence; elles ne peuvent contenir ces renseignements.	Sensible	Secret
	Renseignements sur la menace de référence	Proviennent généralement d'éléments relevant de la sécurité nationale, par exemple des informations obtenues par les services de renseignement.	Sensible	Secret
	Détails de l'étude visant à recenser les zones vitales	Pourraient être utiles à un adversaire pour déterminer les cibles et réaliser une attaque.	Sensible	Secret
	Raisons pour lesquelles un niveau d'alerte de sécurité est adopté ou modifié	Proviennent généralement d'éléments relevant de la sécurité nationale, par exemple des informations obtenues par les services de renseignement.	Sensible	Secret
Techniques nucléaires	Informations techniques détaillées sur la production ou le traitement de matières nucléaires (par exemple, le traitement et le retraitement de l'uranium enrichi)	Les informations de ce type pourraient être utiles à un adversaire.	Sensible	Non classifié
	Conceptions ou nouvelle technique présentés à des fins d'autorisation (p. ex., réacteur avancé, etc.)	Même si certains détails sur ces techniques peuvent être rendus publics, certaines particularités de la conception ou de la technique concernés pourraient être utiles à des adversaires à des fins de préparation. Ces informations peuvent être examinées afin d'y rechercher des informations de nature délicate.	Sensible	Non classifié

Catégorie	Type de document	Description	Sensibilité	Classification recommandée
	Informations détaillées qui faciliteraient le démontage de dispositif afin d'accéder à des sources ou qui contribueraient à contourner d'autres mesures de sécurité	Ces informations pourraient être utiles à un adversaire qui tente d'enlever des matières radioactives.	Sensible	Non classifié
	Études de vulnérabilité portant sur des conceptions technologiques	Si des études menées par des chercheurs peuvent être rendues publiques, toute information détaillée qui présente des vulnérabilités et qui pourrait être exploitée par un adversaire devrait être protégée contre toute divulgation non autorisée.	Sensible	Non classifié
Données historiques	Données historiques qui restent pertinentes et de nature délicate, que ces informations soient classées ou non	En dépit de leur ancienneté, les informations de cette nature peuvent encore être utiles à des adversaires.	Sensible	Non classifié

Références

1. Groupe CSA. CSA N290.7, *Cybersécurité pour les centrales nucléaires et les installations dotées de petits réacteurs.*

2. Agence internationale de l'énergie atomique (AIEA). *Mission 2015 du Service consultatif international sur la protection physique* (SCIPP) (en anglais seulement).

3. Commission canadienne de sûreté nucléaire (CCSN). *REGDOC-3.5.3, Principes fondamentaux de réglementation*

4. Commission canadienne de sûreté nucléaire (CCSN). *REGDOC 2.12.3 : La sécurité des substances nucléaires : Sources scellées et matières nucléaires de catégories I, II et III*, Version 2.

5. CCSN, *DIS-14-02, Moderniser les règlements de la CCSN et DIS-16-04, Petits réacteurs modulaires : Stratégie, approches et défis en matière de réglementation*

6. CCSN. *Rapport sur ce que nous avons entendu – DIS-14-02*

7. CCSN. *Rapport sur les ateliers avec les parties intéressées : Examen périodique du Règlement sur la sécurité nucléaire*

8. *Loi sur la sûreté et la réglementation nucléaires* (L.C. 1997, ch. 9).

9. *Règlement général sur la sûreté et la réglementation nucléaires* (L.C. 1997, ch. 9).

10. CCSN. REGDOC-2.12.1, *Sites à sécurité élevée, tome I : Force d'intervention pour la sécurité nucléaire* (2018) (document classifié).

11. CCSN. REGDOC-2.12.1, *Sites à sécurité élevée, tome II : Critères pour les systèmes et dispositifs de sécurité nucléaire* (2018) (document classifié).

12. CCSN. REGDOC-2.12.2, *Cote de sécurité donnant accès aux sites* (2013).

13. AIEA. Collection Sécurité nucléaire nº 23-G, *Sécurité de l'information nucléaire*

14. Gendarmerie royale du Canada (GRC). Guide G1-009, *Transport et transmission de renseignements protégés ou classifiés*

15. Centre de la sécurité des télécommunications du Canada (CRTC). *La gestion des risques liés à la sécurité des TI: Une méthode axée sur le cycle de vie* (ITSG-33) et son catalogue de contrôles de sécurité.

16. National Institute of Standards and Technology (NIST). SP 800-53 Rev 5, *Security and Privacy Controls for Information Systems and Organizations*

17. Organisation internationale de normalisation / Commission électrotechnique internationale, ISO/IEC 27001, *Management de la sécurité de l'information*

18. Centre canadien pour la cybersécurité. *Nettoyage des supports de TI*

19. Province de l'Ontario. Commissaire à l'information et à la protection de la vie privée de l'Ontario, *Comment se débarrasser des supports électroniques*

20. Cornell University. *Best Practices for Media Destruction* (page Web).

21. CCSN. REGDOC-3.1.1, *Rapports à soumettre par les exploitants de centrales nucléaires*, version 2

22. CCSN. REGDOC-3.1.2, *Exigences relatives à la production de rapports, tome 1 : Installations nucléaires de catégorie I non productrices de puissance et mines et usines de concentration d'uranium*

23. CCSN. REGDOC-3.1.3, Exigences relatives à la production de rapports pour les titulaires de permis de déchets de substances nucléaires, les installations nucléaires de catégorie II et les utilisateurs d'équipement réglementé, de substances nucléaires et d'appareils à rayonnement

24. NIST. SP 800-61, Rev 2, *Computer Security Incident Handling Guide*

25. AIEA. TDL-005, *Computer Security Incident Response Planning at Nuclear Facilities*

26. Sécurité publique Canada. *Élaboration d'un plan d'intervention en cas d'incident de la technologie opérationnelle et de la technologie de l'information*

27. AIEA. Collection Sécurité nucléaire n° 17, *La sécurité informatique dans les installations nucléaires*

28. Conseil du Trésor du Canada. *Directive sur la gestion de la sécurité*

29. Conseil du Trésor du Canada. *Manuel de la sécurité des contrats*

30. AIEA. Collection Sécurité nucléaire n° 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*, Janvier 2018. Consulté sur 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*, mars 2018. Consulté sur https://iiaglobal.com/wp-content/uploads/2019/09/ORS-Cybersecurity-Procurement-Requirements-030818.pdf

33. Centre canadien pour la cybersécurité. Évaluation des cybermenances nationales, 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*

Renseignements supplémentaires

1. Conseil du Trésor du Canada. *Norme sur le filtrage de sécurité*
2. NIST. *Glossary of Key Information Security Terms*