Office de surveillance des activités en matière de sécurité nationale | National Security and Intelligence Review Agency

Canada

OSSNR

2021 // Rapport Annuel

Numéro ISSN : 2563-5786
No de catalogue : PS106-9F-PDF

Le 18 Juillet 2022

Le très honorable Justin Trudeau, C.P., député
Premier ministre du Canada
Bureau du premier ministre et du Conseil privé
Ottawa (Ontario)
K1A 0A2

Monsieur le Premier ministre,

Au nom de l'Office de surveillance des activités en matière de sécurité nationale et de renseignement, j'ai le plaisir de vous présenter notre troisième rapport annuel. Conformément au paragraphe 38(1) de la *Loi sur l'Office de surveillance des activités en matière de sécurité nationale et de renseignement*, le rapport comprend des renseignements sur nos activités menées en 2021 ainsi que nos conclusions et nos recommandations.

Conformément à l'alinéa 52(1)b) de la *Loi sur l'Office de surveillance des activités en matière de sécurité nationale et de renseignement*, notre rapport a été préparé après la consultation des administrateurs généraux concernés afin de s'assurer qu'il ne contienne pas de renseignements dont la communication porterait atteinte à la sécurité nationale, à la défense nationale ou aux relations internationales ou bien des renseignements protégés par le secret professionnel de l'avocat ou du notaire ou par le privilège relatif au litige.

Veuillez agréer, Monsieur le Premier ministre, l'assurance de ma très haute considération,

L'honorable Marie Deschamps, C.C.

Présidente // Office de surveillance des activités en matière de sécurité nationale et de renseignement

Table des matières

Message des membres

L'Office de surveillance des activités en matière de sécurité nationale et de renseignement (OSSNR) poursuit sa mission qui consiste à accroître la responsabilisation à l'égard des activités liées à la sécurité nationale et au renseignement au Canada. En 2021, notre organisme a continué de croître en taille et d'améliorer sa capacité à tirer pleinement parti de son vaste mandat d'examen et d'enquête couvrant les activités de sécurité nationale et de renseignement des ministères et des organismes à l'échelle du gouvernement fédéral.

Nous sommes heureux de vous présenter notre troisième rapport annuel portant sur nos progrès et nos activités réalisés dans le cadre de notre deuxième année complète de fonctionnement. Malgré les défis récurrents rencontrés pendant la pandémie de COVID-19 ainsi les retards causés par un cyberincident, nous avons effectué un large éventail d'examens et d'enquêtes et nous avons continué d'améliorer nos processus dans l'ensemble de l'organisme. En effet, nous avons poursuivi la réforme des processus et des méthodes employés pour réaliser les examens et les enquêtes, ce qui nous a grandement aidés à améliorer l'uniformité et l'efficacité de nos travaux. Ces réformes, conjuguées à notre expérience croissante, nous ont permis de mettre en œuvre et d'exécuter notre plan d'examen. Ces réalisations ont été possibles grâce à l'élaboration d'un cadre stratégique organisationnel beaucoup plus solide, appuyé par un groupe organisationnel qui se soucie vraiment de la prestation des services et de la santé de l'organisme.

Conformément à notre engagement continu en faveur de la transparence et de la mobilisation du public, ce rapport présentera notre intention d'utiliser les futurs rapports annuels pour évaluer et suivre publiquement la mise en œuvre des recommandations précédentes. Dans le même esprit de responsabilisation des organisations examinées et de la nôtre, nous avons formalisé des normes qui nous permettront d'évaluer la rapidité des réponses. Nous espérons que ces initiatives, en plus du processus de vérification rigoureux que nous élaborons actuellement dans le but d'évaluer notre confiance dans chacun des examens, permettront d'accroître la confiance des Canadiens et des Canadiennes envers nos recommandations et nos conclusions.

Nous tenons à remercier le personnel du Secrétariat de l'OSSNR pour ses efforts, sa patience et sa résilience tout au long de cette année difficile et nous espérons que vous partagez notre enthousiasme en ce qui concerne les nombreuses possibilités qui s'offrent à nous pour l'année à venir.

Marie Deschamps
Craig Forcese
Ian Holloway
Faisal Mirza
Marie-Lucie Morin

Résumé

1. L'année 2021 a été la deuxième année d'activité complète de l'Office de surveillance des activités en matière de sécurité nationale et de renseignement (OSSNR). En vertu de sa vaste compétence prévue par la *Loi sur l'Office de surveillance des activités en matière de sécurité nationale et de renseignement*, l'OSSNR a mené des examens et des enquêtes sur des questions de sécurité nationale et de renseignement se rapportant non seulement au Service canadien du renseignement de sécurité (SCRS) et au Centre de la sécurité des télécommunications (CST), mais aussi à plusieurs ministères et organismes fédéraux, notamment :

    - Le ministère de la Défense nationale (MDN) et les Forces armées canadiennes (FAC);
    - La Gendarmerie royale du Canada (GRC);
    - Immigration, Réfugiés et Citoyenneté Canada (IRCC);
    - L'Agence des services frontaliers du Canada (ASFC);
    - Transports Canada (TC);
    - Tous les ministères et organismes qui participent à des activités liées à la sécurité nationale et au renseignement dans le contexte des examens annuels de la *Loi sur la communication d'information ayant trait à la sécurité du Canada* et de la *Loi visant à éviter la complicité dans les cas de mauvais traitements infligés par des entités étrangères*.

2. En 2021, la capacité de l'OSSNR a continué d'augmenter et l'organisme a poursuivi ses efforts en vue d'améliorer son expertise technique et son savoir-faire spécialisé.

Points saillants des examens

Service canadien du renseignement de sécurité

3. Au cours de l'année 2021, l'OSSNR a réalisé quatre examens qui ont permis d'approfondir sa connaissance d'importants secteurs d'activité du SCRS :

    - Un examen des questions culturelles, de gouvernance et systémiques soulevées dans le contexte où le SCRS sollicite et reçoit des services juridiques du ministère de la Justice et où il prépare et exécute les mandats dont il a besoin pour recueillir des renseignements;

- Une étude de l'ensemble des capacités techniques du SCRS ainsi que de sa structure de gouvernance connexe et des domaines d'intérêt ou de préoccupation auxquels l'OSSNR pourrait revenir dans le cadre d'examens futurs;
- Un deuxième examen annuel sur les mesures de réduction de la menace (MRM) du SCRS qui approfondit les conclusions de l'examen précédent en se penchant sur un plus grand nombre de MRM;
- Un examen annuel de la conformité des activités du SCRS.

Centre de la sécurité des télécommunications

4. En 2021, l'OSSNR a réalisé deux examens sur les activités du CST et a demandé au CST d'effectuer une étude ministérielle comprenant :

    - Un examen du cadre de gouvernance du CST qui oriente le déroulement des cyberopérations défensives et actives et qui permet, notamment, de déterminer si le CST a pris en considération ses obligations juridiques et les répercussions de ses opérations sur la politique étrangère de manière appropriée;
    - Un examen axé sur l'échange de renseignements interne au sein du CST entre les différents volets de son mandat, c'est-à dire le renseignement étranger, la cybersécurité et l'assurance de l'information.
    - Une étude ministérielle visant à déterminer si la communication par le CST de renseignements permettant d'identifier des Canadiens et des Canadiennes a été effectuée conformément à la *Loi sur le Centre de la sécurité des télécommunications* et si elle était essentielle aux affaires internationales, à la défense, à la sécurité ou à la cybersécurité.

Ministère de la Défense nationale et Forces armées canadiennes

5. En 2021, l'OSSNR a réalisé deux examens au sujet du MDN et des FAC, puis a entrepris deux autres examens :

    - Le premier examen achevé constitue un exercice d'évaluation fait dans le but d'acquérir des connaissances de base sur l'entreprise du renseignement de défense, où la majeure partie des fonctions de renseignement du MDN et des FAC sont situées;
    - Le deuxième examen achevé constitue un suivi de l'examen réalisé l'année précédente sur l'Unité nationale de contre-ingérence des Forces canadiennes et met l'accent sur les pratiques opérationnelles en matière de collecte et de protection des renseignements personnels.

Examens interministériels

6. L'OSSNR a réalisé deux examens multiministériels obligatoires en 2021 :

    - Un examen des directives émises à l'égard de la *Loi visant à éviter la complicité dans les cas de mauvais traitements infligés par des entités étrangères*;
    - Un examen sur l'échange de renseignements au sein du gouvernement fédéral en vertu de la *Loi sur la communication d'information ayant trait à la sécurité du Canada*.

7. L'OSSNR a également effectué un examen interministériel dans le cadre de son mandat général pour examiner toute activité menée par un ministère qui a trait à la sécurité nationale ou au renseignement :

    - Un examen pour cartographier la collecte et l'utilisation de données biométriques dans plusieurs ministères et organismes fédéraux dans le cadre d'activités de sécurité et de renseignement liées aux voyages internationaux et à l'immigration constituant le « continuum frontalier ».

Enquêtes sur les plaintes

8. En 2021, le nombre d'enquêtes sur les plaintes de l'OSSNR a grandement augmenté en raison de 58 plaintes qui lui ont été renvoyées par la Commission canadienne des droits de la personne en vertu du paragraphe 45(2) de la *Loi canadienne sur les droits de la personne*.

9. En partie en raison de difficultés inhérentes à la pandémie de COVID-19, l'OSSNR a connu des retards dans ses enquêtes causés par une diminution de la capacité de réponse rapide pour accéder aux renseignements et aux éléments de preuve.

10. En 2021, l'OSSNR a achevé son initiative de réforme du processus d'enquête après des consultations avec de nombreux intervenants. L'OSSNR note que les enquêtes réalisées dans le cadre de ce nouveau modèle montrent déjà une amélioration d'efficacité.

01 //

Introduction

1.1 Qui sommes-nous?

11. Créé en juillet 2019, l'Office de surveillance des activités en matière de sécurité nationale et de renseignement (OSSNR) est un organisme indépendant qui relève du Parlement et qui réalise des examens et fait des enquêtes sur les activités en matière de sécurité nationale et de renseignement du gouvernement fédéral. Avant la création de l'OSSNR, il existait plusieurs lacunes dans le cadre de responsabilisation en matière de sécurité nationale du Canada. Il est à noter que les organismes d'examen qui ont précédé l'OSSNR n'avaient pas la possibilité de collaborer ou de partager leurs informations classifiées, ce qui faisait en sorte qu'ils étaient limités à la conduite d'examens pour leur ministère ou leur organisme spécifique.

12. En revanche, l'OSSNR a le pouvoir d'examiner de façon intégrée toute activité de sécurité nationale ou de renseignement du gouvernement du Canada. Comme il est indiqué dans le rapport annuel de 2019, grâce au rôle élargi de l'OSSNR, le Canada dispose maintenant de l'un des systèmes les plus complets en matière d'examen indépendant de la sécurité nationale.[1]

1.2 Mandat

13. L'OSSNR a le double mandat de mener des examens et des enquêtes sur les activités en matière de sécurité nationale et de renseignement du Canada. L'annexe B contient un aperçu financier et administratif de l'OSSNR.

Examens

14. Le mandat d'examen de l'OSSNR est vaste, comme l'indique le paragraphe 8(1) de la *Loi sur l'Office de surveillance des activités en matière de sécurité nationale et de renseignement* (Loi sur l'OSSNR)[2]. Ce mandat comprend l'examen des activités du Service canadien du renseignement de sécurité (SCRS) et du Centre de la sécurité des télécommunications (CST) ainsi que des activités liées à la sécurité nationale ou au

renseignement de tout autre ministère ou organisme fédéral. Cela comprend, sans s'y limiter, les activités de sécurité nationale ou de renseignement de la Gendarmerie royale du Canada (GRC), de l'Agence des services frontaliers du Canada (ASFC), du ministère de la Défense nationale (MDN) et des Forces armées canadiennes (FAC), d'Affaires mondiales Canada (AMC) et du ministère de la Justice. De plus, l'OSSNR examine toute question de sécurité nationale ou de renseignement qu'un ministre de l'État renvoie à l'OSSNR. L'annexe C contient un résumé des examens effectués en 2021.

15. Les examens de l'OSSNR ont pour but de déterminer si les activités du Canada en matière de sécurité nationale et de renseignement sont conformes aux lois et aux directives ministérielles applicables et si elles sont raisonnables et nécessaires. Dans le cadre de ses examens, l'OSSNR peut formuler toute conclusion ou recommandation qu'il juge appropriée.

16. Les examens sur le SCRS et le CST demeureront toujours une partie essentielle du travail de l'OSSNR puisque la mission de ces organisations consiste entièrement à traiter des questions liées à la sécurité nationale et au renseignement. Toutefois, contrairement aux organismes d'examen qui l'ont précédé, l'OSSNR a un mandat d'examen dont la portée est globale. L'OSSNR continuera ainsi de considérer comme une priorité l'examen des autres ministères qui participent à des activités de sécurité nationale et de renseignement pour vérifier s'ils respectent leurs obligations. Les examens de l'OSSNR contribuent à tenir le Parlement et la population canadienne au fait du caractère licite et raisonnable des activités du Canada en matière de sécurité nationale et de renseignement.

Enquêtes

17. En plus de son mandat d'examen, l'OSSNR a la responsabilité d'enquêter sur les plaintes liées à la sécurité nationale ou au renseignement. Cette obligation est énoncée à l'alinéa 8(1)d) de la Loi sur l'OSSNR et consiste à enquêter sur les plaintes concernant :

    - Les activités du SCRS ou du CST;
    - Les décisions de refuser ou de révoquer certaines habilitations de sécurité du gouvernement fédéral;
    - Les rapports ministériels présentés en vertu de la *Loi sur la citoyenneté* qui recommandent le refus de certaines demandes de citoyenneté.

18. Ce mandat consiste également à enquêter sur les plaintes relatives à la sécurité nationale transmises par la Commission civile d'examen et de traitement des plaintes de la GRC (le mécanisme de traitement des plaintes de la GRC)[3] et la Commission canadienne des droits de la personne.

02 //

Examens

2.1 Examens sur le Service canadien du renseignement de sécurité

Aperçu

19. L'OSSNR a pour mandat d'examiner les activités du Service canadien du renseignement de sécurité (SCRS). En vertu de la Loi sur l'OSSNR, l'OSSNR doit également présenter au ministre de la Sécurité publique et de la Protection civile un rapport annuel sur les activités du SCRS portant, notamment, sur le respect par le SCRS, de la loi et des directives ministérielles applicables et sur le caractère raisonnable et la nécessité de l'exercice des pouvoirs du SCRS.

20. En 2021, l'OSSNR a effectué quatre examens du SCRS qui sont résumés ci-dessous. Elle a également amorcé deux autres examens : l'un sur le cadre de justification du SCRS et l'autre sur le régime des ensembles de données du SCRS. Plusieurs autres examens de l'OSSNR en cours de réalisation comprennent un volet touchant le SCRS.

Examen de l'OSSNR découlant de la décision 2020 CF 616 de la Cour fédérale, Rétablir la confiance : Réforme des processus de consultation juridique du SCRS et des mandats du ministère de la Justice

21. Dans le cadre d'une décision de la Cour fédérale de 2020 (2020 *CF 616*), il a été recommandé « qu'un examen externe exhaustif soit effectué afin de relever l'ensemble des lacunes et des défaillances systémiques, culturelles et liées à la gouvernance qui ont eu pour conséquences que le SCRS a mené des activités opérationnelles dont il a reconnu l'illégalité et a manqué à son obligation de franchise. » En se fondant sur cette recommandation, le ministre de la Sécurité publique et de la Protection civile et le ministre de la Justice ont renvoyé l'examen à l'OSSNR en vertu de l'alinéa 8(1)c) de la Loi sur l'OSSNR. L'OSSNR a donc réalisé un examen sur la façon dont le SCRS demande et obtient des services juridiques auprès du ministère de la Justice et dont il prépare et exécute les mandats qui sont nécessaire pour recueillir des renseignements.

22. Cet examen a permis de constater que le service de renseignement et ses avocats ont de la difficulté à s'organiser de manière à pouvoir respecter leurs obligations juridiques, notamment celles envers la Cour fédérale. L'OSSNR a également constaté que le SCRS n'avait pas réussi à professionnaliser pleinement et durablement le processus d'obtention de mandat à titre de secteur spécialisé nécessitant de la formation, de l'expérience et de l'investissement. L'examen a aussi révélé le besoin de transformer la relation entre le SCRS et ses avocats.

23. L'examen a été dirigé par deux membres de l'OSSNR : Marie Deschamps et Craig Forcese. L'un des deux membres a participé directement à la gestion du processus d'examen, aux séances d'information, aux entrevues et à l'examen des documents dans le cadre de cet examen. Ces travaux comprennent une douzaine d'entrevues confidentielles avec des employés du SCRS et du ministère de la Justice dont le point de vue était essentiel pour vérifier les connaissances que l'OSSNR avait tirées des documents et des séances d'information officiels.

24. En organisant ces entrevues, l'OSSNR a assuré une solide représentation couvrant l'éventail des fonctions du mandat et des processus de prestation de conseils juridiques. Les entrevues ont permis de soulever des questions et des préoccupations dont l'OSSNR n'aurait pas été au courant autrement. Cette information a aidé l'OSSNR à formuler des recommandations sur des questions systémiques, culturelles et liées à la gouvernance qui contribuent au manque d'efficacité nuisant à la capacité du SCRS et du ministère de la Justice de réaliser leurs mandats.

25. De nombreuses personnes interviewées ont soulevé des préoccupations quant au fait que ces problèmes nuisent à la capacité du Service de renseignement de réaliser le mandat que lui a assigné le Parlement. Il est dans l'intérêt du public de remédier à ces difficultés le plus rapidement possible. Même si le SCRS et le ministère de la Justice ont apporté des améliorations, certaines difficultés demeurent évidentes.

26. L'OSSNR a divisé ses conclusions et ses recommandations en trois principaux volets :

- La prestation de conseils juridiques par le ministère de la Justice;
- La gestion du processus d'obtention de mandats par le SCRS et le ministère de la Justice;
- L'investissement dans les personnes.

Prestation de conseils juridiques par le ministère de la Justice

27. Le SCRS mène ses activités dans un environnement qui évolue rapidement et qui présente des difficultés sur le plan juridique. Les conseils juridiques rapides, souples et réalisables

sont essentiels. Le ministère de la Justice fournit des conseils juridiques sur des questions touchant la sécurité nationale à d'autres ministères et organismes par le biais du Groupe litiges et conseils en sécurité nationale (GLCSN). Cet examen a mis en lumière des facteurs qui empêchent le GLCSN de fournir au SCRS les conseils juridiques dont il a besoin.

28. Le ministère de la Justice a employé un modèle centralisé « à l'unisson » pour la prestation de ses services juridiques. Le modèle « à l'unisson » reflète un désir que des conseils juridiques uniformes et cohérents soient formulés au nom du procureur général du Canada. Bien que le principe de l'approche « à l'unisson » soit louable, l'OSSNR a constaté que le GLCSN avait de la difficulté à fournir des conseils juridiques en temps opportun, adaptés et utiles dans le contexte du SCRS. La façon dont le ministère de la Justice fournit des conseils n'était souvent pas adaptée aux opérations du SCRS. Par exemple, le GLCSN présente ses conseils à titre d'évaluation du risque juridique au moyen de la grille de gestion des risques juridiques utilisée à l'échelle du ministère de la Justice. Dans la grille, les risques sont classés selon un code de couleur qui ressemble à un feu de circulation : une cote de risque « verte » représente un faible risque juridique pour le SCRS, une cote de risque « rouge » représente un risque juridique élevé et, de façon plus ambiguë, une cote de risque « jaune » représente un risque juridique modéré. Les cotes de risque « jaune » sont les plus fréquentes et les plus frustrantes pour le SCRS, surtout lorsqu'elles ne sont pas accompagnées de discussions sur la façon d'atténuer le risque, ce qui, selon l'information fournie à l'OSSNR, est actuellement une pratique courante.

29. Par conséquent, certaines personnes au sein du SCRS considèrent que le ministère de la Justice constitue un obstacle en raison de sa bureaucratie, du fait qu'elles perçoivent qu'il n'est pas au fait des opérations et de son approche inefficace en ce qui concerne la communication de conseils juridiques.

30. Toutefois, les problèmes liés à l'obtention de conseils juridiques opportuns, adaptés et utiles ne proviennent pas uniquement du ministère de la Justice. L'OSSNR a appris que le SCRS n'a pas toujours partagé toutes les informations pertinentes qu'il détenait avec le ministère de la Justice, ce qui suscite une certaine méfiance. Le processus interne de demande de conseils juridiques au SCRS contribue également aux retards et au manque de pertinence. Les conseils, une fois filtrés par les hiérarchies bureaucratiques, qui parviennent aux enquêteurs opérationnels du SCRS sont parfois peu pertinents.

31. L'OSSNR a été informé que le processus laborieux de demande et d'obtention de conseils a parfois causé [Discussion sur les effets nuisibles et les risques dans le contexte des opérations].

32. Le SCRS et le ministère de la Justice mènent souvent leurs activités dans un contexte de doute juridique en raison du manque de clarté de la loi. Une interprétation judiciaire s'avère

souvent nécessaire pour clarifier les normes juridiques. Toutefois, le processus relatif aux mandats complexes, abordé ci-dessous, rend cette avenue plus difficile.

33. Le ministère de la Justice est conscient de la nécessité d'apporter des changements. Parmi les initiatives récentes de grande envergure, mentionnons le projet Vision, qui promet des partenariats stratégiques axés sur la clientèle. De nouvelles procédures ont été mises en œuvre au sein du GLCSN pour éliminer le cloisonnement interne entre les conseillers juridiques et les avocats plaideurs dans le but d'améliorer la formation et l'accès aux conseils juridiques et de faciliter l'uniformité des conseils juridiques. Le GLCSN semble également avoir le désir d'adopter une approche différente pour la prestation de conseils juridiques, notamment en offrant des conseils juridiques qui font la promotion d'une mobilisation collaborative et itérative avec le SCRS afin que ce dernier puisse atteindre ses objectifs opérationnels dans les limites de la loi. Toutefois, à l'automne 2021, le SCRS et le ministère de la Justice ne semblaient pas avoir systématiquement mis ce modèle en application.

34. Pour faciliter une prestation de conseils adéquate, le SCRS doit fournir tous les faits au GLCSN et mobiliser le Groupe sur le plan opérationnel. Une participation précoce et continue tout au long des étapes d'une enquête ou d'une opération permettrait aux avocats de donner des conseils juridiques informels qui, à leur tour, permettraient au SCRS de corriger le tir avant que trop de temps ne se soit écoulé. Un processus plus itératif d'intégration des conseils juridiques tout au long d'une opération pourrait régler les difficultés signalées selon lesquelles des opérations sont interrompues en raison de conseils juridiques inopportuns ou ambigus.

Gestion du processus relatif aux mandats

35. Le SCRS organise le processus de demande de mandat en fonction d'un système interne de préparation et d'approbation avant de passer à l'étape législative consistant à demander l'approbation du ministre pour la demande de mandat. Un certain nombre de concepts et d'attentes juridiques entrent en jeu dans le processus relatif aux mandats, notamment l'obligation de franchise envers la Cour.

36. Les préoccupations relatives à l'obligation de franchise envers la Cour fédérale s'inscrivent dans deux catégories : la communication d'information requise pour assurer la crédibilité des sources qui fournissent l'information utilisée dans la demande et la communication d'information sur les questions qui pourraient possiblement être préoccupantes eu égard au contexte plus large d'un mandat et la façon dont il sera exécuté.

37. Malgré les tentatives antérieures de réforme, le processus relatif aux mandats adopté par le SCRS et appuyé par le ministère de la Justice a à maintes reprises donné lieu à des manquements à l'obligation de franchise. De nombreuses réformes semblent avoir contribué à la complexité bureaucratique du processus relatif aux mandats, sans toutefois régler les problèmes de franchise.

38. Le SCRS a eu de la difficulté à veiller à ce que l'information requise pour assurer la crédibilité des sources soit correctement intégrée aux demandes de mandat. L'OSSNR a été informé à plusieurs reprises que des agents du SCRS intervenant aux premières étapes de la préparation des demandes de mandat ne comprennent pas clairement les attentes juridiques entourant l'obligation de franchise. Les lacunes des systèmes de gestion de l'information liés aux sources humaines au SCRS ont également entraîné d'importantes omissions, violant ainsi l'obligation de franchise. Ces défis produisent ce que l'OSSNR appelle un problème d' « omissions récurrentes ».

39. En 2019, le SCRS a voulu professionnaliser les travaux liés aux déposants en créant la Sous-section des déposants (SSD). La mise sur pied de la SSD par le SCRS constitue une étape importante et, dotée des ressources et des employés nécessaires, elle serait bien placée pour répondre aux problèmes de longue date liés à l'obligation de franchise. Toutefois, lors de sa création, la SSD a été placée [Nom de la section]. [Nom] a un vaste mandat qui ne cadre pas avec les fonctions de la SSD dans la préparation de demandes de mandats solides sur le plan juridique. Cette anomalie en matière de gouvernance peut possiblement expliquer les défis actuels en matière d'administration et de ressources humaines auxquelles fait face la SSD. La viabilité de la SSD est en péril et l'OSSNR a effectivement entendu dire que la Sous-section pourrait actuellement être décrite comme étant en état de crise. Le SCRS n'a pas offert à la SSD des ressources proportionnelles à l'importance de cette Sous-section dans l'exécution de sa mission.

40. Les avocats du GLCSN jouent plusieurs rôles essentiels dans le processus de demande de mandat et participent étroitement à assurer le respect de l'obligation de franchise. Il est essentiel pour eux d'entretenir une relation étroite, collaborative et productive avec le SCRS. Le moral des avocats du GLCSN chargés des mandats pourrait avoir été affecté par la décision récente de la Cour fédérale qui a déclenché cet examen. Avec l'augmentation récente du personnel, il semble que le GLCSN dispose actuellement de l'effectif requis pour gérer le nombre annuel de demandes de mandat présentées par le SCRS, mais que les difficultés liées au recrutement persistent. Le GLCSN devrait être doté de sorte à garantir que les opérations du SCRS ne seront pas contrecarrées par le manque de disponibilité des avocats responsable des mandats.

41. Le processus de demande de mandat doit être renforcé par un examen de l'affidavit effectué au stade quasi final par un avocat indépendant. En pratique, il s'agit d'un avocat du Groupe de la sécurité nationale du ministère de la Justice. À l'origine, on envisageait que ce rôle consistait à effectuer une remise en question rigoureuse de la demande de mandat. Cependant, le rôle principal de l'avocat indépendant semble être davantage orienté sur la forme et non sur le fond, conçu pour vérifier les citations plutôt que pour exercer avec assurance la fonction d'avocat du diable.

42. L'OSSNR est d'avis que la présence d'une fonction de remise en question rigoureuse effectuée par un avocat bien informé, adéquatement appuyé et n'étant pas préalablement impliqué dans le processus de demande de mandat est pertinente et nécessaire. Toutefois, l'OSSNR propose que le modèle actuel d'avocat indépendant soit abandonné au profit d'une fonction de remise en question effectuée par Sécurité publique Canada, dont le rôle précis est de surveiller le processus de demande de mandat du SCRS.

43. En collaboration avec l'unité de Sécurité publique Canada chargée de l'examen des mandats, un avocat spécialisé et expérimenté pourrait effectuer une véritable remise en question du mandat, analogue à ce qu'un avocat de la défense ferait si les mandats faisaient l'objet d'un processus accusatoire. L'OSSNR est d'avis qu'un tel examen aiderait à prévenir les lacunes en matière d'obligation de franchise découlant d'une omission de divulguer tous les renseignements importants sur des questions potentiellement préoccupantes au sujet du contexte plus général du mandat et de la façon dont il sera exécuté.

44. Une fois qu'un juge a émis un mandat, le SCRS peut l'exécuter, conformément à la portée et aux modalités du mandat. Toutefois, les coordonnateurs régionaux des mandats du SCRS n'ont pas reçu une formation suffisante pour donner les conseils requis pour l'exécution des mandats.

Investissement dans les personnes

45. Les préoccupations au sujet de la formation inadéquate au SCRS était un thème récurrent dans cet examen. Ces préoccupations ont été notées dans les documents internes du SCRS. Le SCRS reconnaît qu'il n'est actuellement pas une organisation qui facilite l'apprentissage et qu'il n'a pas de culture d'apprentissage. Bref, il y a trop peu de possibilités pour la formation nécessaire pour soutenir un service de renseignement professionnel moderne opérant dans un environnement complexe.

Conclusions

46. Ce rapport se termine par des observations sur les défis transversaux en matière de culture et de gouvernance qui découlent, du moins en partie, des défis caractérisant la prestation de conseils juridiques et le processus relatif aux mandats. L'OSSNR divise ces grands phénomènes transversaux en deux catégories : le moral et les attitudes, et la réalisation de la mission.

47. Le moral bas au SCRS était un thème fréquent tout au long de cet examen. Les problèmes systémiques dans le processus de demande de mandat sont probablement l'une des causes de ce problème : le moral est affecté lorsqu'un système de demandes de mandat empêche de façon répétée les agents du SCRS de s'acquitter de leurs fonctions prescrites et ternit la réputation de l'organisation en raison de manquements à l'obligation de franchise.

48. Parallèlement, le fait de ne pas régler le problème du processus relatif aux mandats nuit à la capacité du SCRS et du ministère de la Justice de remplir leur mandat. Le ministère de la Justice doit cesser d'être perçu comme un obstacle et devenir un conseiller franc et direct, parfaitement au fait des objectifs opérationnels.

49. Au sein du SCRS, le processus de demande de mandat était parfois comparé au fait de gagner à la loterie, non pas parce que la Cour fédérale refuse de délivrer des mandats, mais en raison des ressources nécessaires pour préparer et remplir la demande. En outre, la lourdeur du processus actuel de demande de mandat freine la progression de certaines activités de collecte.

50. En somme, cet examen a été déclenché par le non-respect de l'obligation de franchise. Il conclut que les manquements répétés dans ce domaine sont à la fois causés par des modèles culturels et de gouvernance profondément ancrés et en sont la cause. Ce cercle vicieux a aggravé les défis de la réforme du processus d'obtention de mandat.

51. Les réformes sélectives ou documentaires qui masquent sans régler les défis systémiques, culturels et de gouvernance primordiaux subiront le même sort que les réformes précédentes : les problèmes continueront.

52. L'OSSNR a l'intention de procéder à un examen de suivi d'ici deux ans pour mesurer les progrès réalisés par le SCRS, le ministère de la Justice et Sécurité publique Canada dans la résolution du problème systémique lié au processus d'obtention de mandats visé par cet examen. De plus, dans le cadre d'autres examens réguliers concernant les mandats, l'OSSNR documentera les récurrences de problèmes systémiques. Entre-temps, étant donné que cet examen découle d'une décision de la Cour fédérale, il est essentiel que le ministre

et le SCRS le communiquent intégralement aux juges désignés de cette cour. Le rapport complet caviardé de l'OSSNR peut être consulté sur son site Web.[4]

Réponse aux recommandations de l'OSSNR

53. Les recommandations de l'OSSNR, la réponse du SCRS, du ministère de la Sécurité publique et du ministère de la Justice, et d'autres détails concernant cet examen figurent à l'annexe D du présent rapport.

Étude sur les capacités techniques du SCRS

54. Les menaces à la sécurité nationale du Canada augmentent constamment et les changements technologiques offrent au SCRS une variété de nouvelles possibilités en matière d'enquête. Par conséquent, le SCRS doit développer et acquérir de nouvelles capacités techniques et doit adapter (réaffecter) ses outils existants pour soutenir les activités de collecte qui lui sont confiées.[5] Ce processus présente un risque possible sur le plan de la conformité puisque les cadres juridiques et de gouvernance actuels du SCRS peuvent ne pas tenir compte du nouveau déploiement ou de l'adaptation de ces capacités techniques. De plus, certains membres du personnel ainsi que les conseillers juridiques qui les soutiennent peuvent ne pas comprendre entièrement comment ces outils sont utilisés sur le plan opérationnel, ce qui a une incidence sur leur capacité à indiquer si le SCRS dispose du cadre stratégique et juridique nécessaire pour soutenir l'utilisation de la technologie. En raison de ces risques, l'OSSNR doit rester à jour en ce qui a trait aux capacités techniques du SCRS et aux pouvoirs qui y sont associés en relation avec les mandats.

55. L'étude de l'OSSNR sur les capacités techniques du SCRS constitue un premier pas dans cette direction en examinant l'ensemble des capacités du SCRS et la structure de gouvernance qui lui est associée ainsi qu'en identifiant les questions d'intérêt et les préoccupations sur lesquels l'OSSNR pourra revenir lors d'examens futurs.

56. L'éventail complet des capacités techniques que le SCRS utilise actuellement pour appuyer ses activités de collecte de renseignements a été examiné. L'OSSNR a examiné les cadres stratégiques et juridiques pertinents communiqués par le SCRS, mais n'a pas effectué de vérification indépendante des déclarations ou des activités elles-mêmes. L'OSSNR a également examiné le lien tripartite entre l'échange de renseignements et de connaissances et le soutien qui existe entre les directions opérationnelles, les directions technologiques et les avocats du ministère de la Justice du SCRS en ce qui concerne le déploiement des capacités à l'appui des opérations.

Réalité des risques

L'examen de l'OSSNR sur l'utilisation par le SCRS d'un outil de géolocalisation a permis de constater que l'absence de « politiques et procédures élaborées concernant l'évaluation des technologies de collecte nouvelles et émergentes » a contribué directement au risque que le SCRS enfreigne l'article 8 de la *Charte canadienne des droits et libertés* lors de la mise à l'essai du dispositif.

- *Étude de l'OSSNR (2018-05)*

57. En plus des connaissances de base que l'OSSNR a acquises sur les capacités techniques du SCRS, l'OSSNR a formulé plusieurs observations identifiant des domaines d'intérêt pour des examens futurs possibles. Par exemple, l'OSSNR a fait remarquer, et le SCRS est d'accord, que le principal ensemble de politiques liées à l'utilisation des capacités techniques est désuet et en cours de révision, bien que l'échéancier pour l'exécution de cette tâche[6] ne soit pas clair. Entre-temps, l'ensemble des politiques est étayé, comme l'exigent les directives de la haute direction et d'autres politiques et pratiques pertinentes. L'absence de politiques et de procédures à jour peut entraîner des risques accrus en matière de conformité, ce qui constitue une question d'intérêt pour de futurs examens de l'OSSNR.

58. De plus, le cadre dans lequel le SCRS évalue la conformité et le risque dans ce domaine est en pleine transition. Le SCRS a indiqué qu'il croyait que de nouvelles initiatives, comme la création du Comité d'examen de la technologie opérationnelle en mai 2021, permettraient de répondre plus efficacement aux besoins des intervenants et de combler les lacunes en matière de conformité. L'objectif du Comité consiste à examiner toutes les nouvelles technologies utilisées pour les activités de renseignements, ainsi que les technologies existantes qui seront utilisées d'une manière nouvelle ou différente. La création du Comité d'examen de la technologie opérationnelle suggère que des mesures sont prises en vue d'atténuer le risque de manquements à la conformité lié au déploiement de technologies à l'appui des opérations. De toute évidence, il s'agit d'une tribune où les risques potentiels peuvent être cernés et atténués de façon proactive. L'évolution de la façon dont la conformité est surveillée par rapport aux capacités techniques intéressera l'OSSNR à l'avenir.

59. Des questions se posent quant à la façon dont le SCRS surveille la valeur opérationnelle des capacités techniques. Le SCRS doit renforcer son programme de mesure du rendement en ce qui concerne son déploiement de technologies à l'appui des opérations. Un régime de mesure du rendement, en cours d'élaboration, deviendra une caractéristique importante du cadre de gouvernance, ce qui aura des répercussions connexes en matière de conformité pour d'éventuels examens de l'OSSNR.

60. Dans l'ensemble, il sera important que l'OSSNR se tienne à jour sur les volets techniques des opérations de collecte de renseignement du SCRS, surtout en raison de la vitesse à laquelle les technologies et les capacités techniques connexes évoluent.

61. Dans le cadre de cet effort, il est peut-être possible de tirer parti des exigences actuelles en matière de rapports déjà établies par le SCRS. Par exemple, l'article 3 de la Directive ministérielle au Service canadien du renseignement de sécurité – Responsabilisation (10 septembre 2019) exige que le SCRS informe le ministre de la Sécurité publique et de la Protection civile des activités opérationnelles dans lesquelles « une nouvelle autorité, technique ou technologie est utilisée ». Ces avis pourraient fournir à l'OSSNR une connaissance continue et à jour de l'ensemble des capacités du SCRS et de la façon dont les technologies sont déployées sur le plan opérationnel. De plus, le partage des avis renforcerait les efforts du SCRS en matière de transparence proactive, qui sont conformes aux engagements de fournir des séances d'information explicatives à la Cour fédérale sur les nouvelles technologies utilisées dans les opérations justifiées.

62. L'OSSNR a recommandé que la version complète, non caviardée, de l'étude soit transmise aux juges désignés de la Cour fédérale.

Examen des activités de réduction de la menace du SCRS : Accent sur la communication de renseignements à des parties externes

63. En vertu de la *Loi antiterroriste* de 2015, le SCRS a le pouvoir de prendre des mesures de réduction de la menace (MRM). L'OSSNR doit examiner, chaque année, au moins l'un des volets du rendement du SCRS dans l'exercice de ses pouvoirs de réduction de la menace.[7] L'OSSNR reconnaît que les pouvoirs de réduction de la menace du SCRS peuvent être un outil efficace pour réduire une menace envers la sécurité nationale, mais ils impliquent aussi une plus grande responsabilité compte tenu de leur nature et de leur capacité à avoir une incidence importante non seulement sur le sujet d'une MRM donnée, mais aussi sur d'autres personnes potentiellement concernées par sa portée.

64. Cette année, l'OSSNR a produit son deuxième examen annuel sur les MRM du SCRS. L'examen visait à approfondir les conclusions de l'examen précédent en se penchant sur un

plus grand nombre de MRM dans le cadre desquelles le SCRS a communiqué de l'information à des parties externes, et, ce faisant, leur a donné la possibilité de prendre des mesures, à leur discrétion et en vertu de leurs pouvoirs, dans le but de réduire les menaces cernées. L'examen portait sur les caractéristiques de ces MRM, mais se concentrait sur la mesure dans laquelle le SCRS a correctement identifié, documenté et examiné les effets négatifs possibles que ces mesures pourraient avoir sur les personnes concernées.

65. L'OSSNR a constaté que plusieurs types de parties externes différentes prenaient part aux MRM. Ces parties externes disposaient de divers leviers de contrôle au moyen desquels elles pouvaient prendre des mesures pour réduire une menace.

66. L'OSSNR a remarqué que les documents du SCRS sur les renseignements divulgués aux parties externes dans le cadre de MRM n'étaient pas uniformes et, parfois, manquaient de clarté et de précisions. L'OSSNR a également constaté que le SCRS n'a pas systématiquement cerné ou documenté les pouvoirs ou les capacités des parties externes de prendre des mesures ou les effets négatifs possibles des MRM. L'OSSNR a également noté que le SCRS ne documente pas toujours les résultats d'une certaine MRM, ni les mesures prises par des parties externes pour réduire une menace.

67. Sans une documentation robuste, le SCRS n'est pas en mesure d'évaluer l'efficacité de ses mesures ni de connaître la véritable incidence de ses actions sur ces mesures.

68. L'OSSNR recommande que lorsqu'une MRM comprend la communication de renseignements à des parties externes, le SCRS doit clairement indiquer et documenter la portée et l'ampleur des renseignements qui seront communiqués dans le cadre de la mesure proposée. L'OSSNR recommande que le SCRS définisse et documente pleinement les pouvoirs et la capacité de la partie externe de prendre des mesures précises pour réduire une menace, de même que les effets négatifs possibles que pourrait causer la mesure. En plus de recommander que le SCRS se conforme à ses politiques de tenue des dossiers, l'OSSNR recommande que le SCRS modifie sa politique sur les MRM pour y intégrer une exigence de documenter systématiquement les résultats des MRM, y compris les mesures prises par les parties externes. Cette pratique devrait éclairer les évaluations après action et la prise de décisions futures.

69. En outre, l'OSSNR a constaté que le cadre d'évaluation actuel utilisé dans le processus d'approbation des MRM est trop étroit et ne tient pas suffisamment compte de l'ensemble des répercussions des MRM du SCRS. L'OSSNR recommande que le SCRS tienne compte des répercussions négatives possibles résultant non seulement de la communication de renseignements par le SCRS, mais également des mesures prises par les parties externes dans le cadre de MRM.

70. Les diverses répercussions observées dans le cadre de l'examen de cette année, combinées aux lacunes cernées quant à la compréhension et à l'évaluation de ces répercussions par le SCRS, mettent en évidence l'importance de certaines recommandations formulées par l'OSSNR en 2020. L'OSSNR réitère sa recommandation de 2020 selon laquelle le SCRS doit prendre en compte de manière plus complète les répercussions négatives possibles de ces types de mesures sur les personnes concernées, même lorsqu'elles sont prises par des parties externes et non par le SCRS. Ces répercussions devraient non seulement être prises en compte lors de l'évaluation du caractère raisonnable et proportionnel d'une mesure proposée, mais également au moment de déterminer si un mandat est requis.

71. La *Loi sur le Service canadien du renseignement de sécurité* (Loi sur le SCRS) indique clairement que, lorsqu'une MRM proposée limiterait un droit ou une liberté protégés par la *Charte canadienne des droits et libertés* ou serait autrement contraire aux lois canadiennes, le SCRS doit obtenir un mandat judiciaire. L'OSSNR est fondamentalement en désaccord avec la façon dont le SCRS comprend et aborde l'analyse juridique visant à déterminer si un mandat est requis pour les MRM proposées. En 2020, le SCRS a répondu à cette recommandation en déclarant que [traduction] : « le ministère de la Justice examinera cette recommandation et en tiendra compte dans le cadre de ses travaux sur les MRM en vertu de la Loi sur le SCRS. »

72. Pour l'avenir, l'OSSNR a recommandé que le SCRS demande un mandat lorsqu'une MRM proposée pourrait porter atteinte aux droits d'une personne garantis par la Charte ou lorsqu'il serait autrement contraire aux lois canadiennes, et ce, peu importe si l'activité est menée directement par le SCRS ou par l'entremise d'une partie externe à laquelle le SCRS communique des renseignements.

73. L'OSSNR a pu utiliser son accès direct aux répertoires de renseignements du SCRS pour confirmer les renseignements qu'il devait vérifier et pour mener des enquêtes supplémentaires, au besoin. Pour cette raison, l'OSSNR a un niveau de confiance élevé envers les renseignements utilisés pour effectuer cet examen. L'OSSNR tient également à souligner la rapidité avec laquelle le SCRS a répondu à ses demandes d'information tout au long de l'examen.

Réponse aux recommandations de l'OSSNR

74. Les recommandations de l'OSSNR, la réponse de la direction du SCRS et d'autres détails au sujet de cet examen se trouvent à l'annexe D du présent rapport.

Examen annuel de l'OSSNR sur les activités du SCRS

75. Conformément à la Loi sur le SCRS, le SCRS est tenu de fournir des renseignements à l'OSSNR sur des activités précises.[8] De son côté, l'OSSNR a élaboré un processus pour examiner cette information tout au long de l'année et mettre en évidence toute observation importante dans le cadre des obligations de l'OSSNR en matière de rapports annuels au ministre de la Sécurité publique.[9] Ce processus vise à tenir l'OSSNR au courant des principales activités du SCRS afin qu'il puisse cerner les nouveaux problèmes et les lacunes en matière de conformité en temps opportun et planifier les examens et les obligations en matière de rapports annuels. En outre, ce processus facilite la réalisation d'un examen supplémentaire des activités pour en évaluer la conformité, le caractère raisonnable et la nécessité.

76. En 2021, l'OSSNR a officialisé ce processus et a entrepris un examen annuel conformément à son mandat d'examen (alinéa 8(1)a) de la Loi sur l'OSSNR). Pour accroître la transparence, l'OSSNR a demandé des catégories supplémentaires de renseignements au SCRS, notamment des demandes de mandat approuvées, des rapports de conformité, des vérifications internes, des évaluations internes et des communications entre le SCRS et la Cour fédérale ainsi qu'entre le SCRS et le ministre de la Sécurité publique. Ces catégories supplémentaires visaient à faire en sorte que l'OSSNR bénéficie de renseignements précis sur les politiques et la gouvernance du SCRS, en plus de ceux que le SCRS est tenu de fournir en vertu de la loi.

77. L'OSSNR a constaté que le SCRS satisfaisait aux exigences de déclaration prévues par la loi. Toutefois, ces exigences ne se traduisent pas toujours par des renseignements qui peuvent être utilisés pour les évaluations de l'OSSNR. Notamment, le SCRS n'a pas fourni de renseignements sur les catégories supplémentaires d'activités demandées par l'OSSNR. Le dialogue visant à combler ces lacunes se poursuivra en 2022.

78. En 2022, l'OSSNR continuera d'examiner les activités du SCRS en s'appuyant sur les renseignements fournis par le SCRS, conformément à la Loi sur le SCRS et la Loi sur l'OSSNR.

Statistiques

79. L'OSSNR demande au SCRS de publier des statistiques et des données liées aux volets d'intérêt public et à la conformité de ses activités. L'OSSNR est d'avis que les statistiques suivantes permettront de renseigner le public sur la portée et l'ampleur des opérations du SCRS ainsi que sur l'évolution des activités d'une année à l'autre.

Demandes d'obtention de mandat

80. L'article 21 de la Loi sur le SCRS autorise le SCRS à présenter une demande de mandat à un juge s'il a des motifs raisonnables de croire que des pouvoirs plus intrusifs sont nécessaires pour enquêter sur une menace particulière envers la sécurité du Canada. Le SCRS peut avoir recours à des mandats, par exemple, pour intercepter des communications, pénétrer dans un lieu ou obtenir des renseignements, des dossiers ou bien des documents. Il convient de noter que chaque demande de mandat peut viser plusieurs personnes ou concerner l'utilisation de multiples pouvoirs d'intrusion.

81. L'OSSNR sait que les difficultés liées au processus d'obtention de mandats au sein du SCRS persistent. L'examen de l'OSSNR intitulé *Rétablir la confiance : Réforme des processus de prestation de conseils juridiques du ministère de la Justice et d'obtention de mandats du SCRS* a révélé que le processus actuel d'obtention de mandats continue d'être trop complexe, malgré les tentatives de réforme. L'examen a permis de constater que le SCRS n'avait pas réussi à professionnaliser pleinement et durablement le processus de demande de mandat. L'absence de responsabilisation et de communication claire, combinée à une complexité excessive, a contribué aux problèmes auxquels ce processus est confronté. L'examen a donné lieu à un certain nombre de conclusions et de recommandations liées à des problèmes systémiques du processus d'obtention de mandats du SCRS.

Demandes de mandat en vertu de l'article 21 présentées par le SCRS (2018 à 2021)

	2018	2019	2020	2021
Nombre total de mandats approuvés	24	23	15	31
Nouveaux mandats	10	9	2	13
Demandes de remplacement	11	12	8	14
Demandes supplémentaires	3	2	5	4
Nombre total de demandes rejetées	0	1	0	0

Mesures de réduction de la menace (MRM)

82. L'article 12.1 de la Loi sur le SCRS autorise le SCRS à prendre des mesures pour réduire les menaces à la sécurité du Canada, à l'intérieur ou à l'extérieur du Canada.[10] Le SCRS est autorisé à demander un mandat judiciaire s'il croit que certaines mesures intrusives

(décrites au paragraphe 21(1.1) de la Loi sur le SCRS) sont nécessaires pour réduire la menace. À ce jour, le SCRS n'a demandé aucune autorisation judiciaire pour entreprendre des MRM justifiées.

83. Les deux premiers examens sur l'utilisation par le SCRS de mesures de réduction de la menace ont révélé que le SCRS ne tenait pas suffisamment compte de toutes les répercussions de la mesure dans le cadre du processus d'approbation de ces activités. Plus précisément, ces répercussions n'ont pas été explicitement prises en compte au moment de déterminer si un mandat peut être nécessaire. Comme susmentionné dans le présent rapport, l'OSSNR s'attend à ce que le SCRS demande un mandat pour autoriser une mesure de réduction de la menace lorsque les droits d'une personne en vertu de la Charte seraient limités ou que la mesure serait autrement contraire aux lois canadiennes, que le SCRS entreprenne la mesure directement ou bien qu'elle soit entreprise par une partie externe.

Mesures de réduction de la menace approuvées et exécutées par le SCRS qui ont été justifiées (2015 à 2021)

	2015	2016	2017	2018	2019	2020	2021
MRM approuvées	10	8	15	23	24	11	23
MRM exécutées	10	8	13	17	19	8	17
MRM dans le cadre d'un mandat	0	0	0	0	0	0	0

Cibles du SCRS

84. Le SCRS a pour mandat d'enquêter sur les menaces à la sécurité du Canada, y compris l'espionnage, les activités influencées par l'étranger, la violence politique, religieuse ou idéologique et la subversion.[11] Des critères permettant au SCRS de mener des enquêtes sur une personne, un groupe ou une entité pour des questions liées à ces menaces sont établis à l'article 12 de la Loi sur le SCRS. Les sujets d'une enquête du SCRS, qu'il s'agisse de personnes ou de groupes, sont appelés des « cibles ».[12]

Cibles du SCRS (2018 à 2021)

	2018	2019	2020	2021
Nombre de cibles	430	467	360	352

Ensembles de données

85. L'analyse de données constitue l'un des principaux outils d'enquête du SCRS. Cet outil lui permet d'établir des liens et de cerner des tendances, ce qui ne serait pas possible avec des méthodes d'enquête traditionnelles. La *Loi sur la sécurité nationale* de 2017, adoptée par le Parlement en juin 2019, a accordé au SCRS une série de nouveaux pouvoirs, notamment un cadre juridique pour la collecte, la conservation et l'utilisation d'ensembles de données par le SCRS. Ce cadre autorise le SCRS à recueillir des ensembles de données (subdivisés en ensembles de données canadiens, étrangers et accessibles au public) qui peuvent aider le SCRS dans l'exercice de ses fonctions. Le cadre établit également des mesures de protection des droits et libertés des Canadiens, notamment la protection des renseignements personnels. Ces mesures de protection comprennent des exigences accrues en matière de responsabilité ministérielle. Le SCRS doit satisfaire à différentes exigences avant de pouvoir utiliser certains types d'ensemble de données.[13]

86. Selon la Loi sur le SCRS, l'OSSNR doit également être tenu au courant de certaines activités liées aux ensembles de données. Des rapports préparés à la suite de traitement d'ensembles de données doivent être fournis à l'OSSNR, sous certaines conditions et dans des délais raisonnables.[14] Même si le SCRS n'est pas tenu d'informer l'OSSNR des autorisations judiciaires ou des approbations ministérielles pour la collecte d'ensembles de données canadiens et étrangers, il a tenu l'OSSNR au courant de ces activités de façon proactive.

87. Bien que ce nouveau cadre ait permis au SCRS de s'acquitter de son mandat d'enquêter sur les menaces, le SCRS a souligné dans son rapport annuel public de 2020 que le cadre législatif actuel n'est pas exempt de défis. L'OSSNR examine actuellement la mise en œuvre par le SCRS de son régime d'ensembles de données. Les résultats de cet examen éclaireront l'examen de la *Loi sur la sécurité nationale de 2017* par le Parlement.

Ensembles de données évalués par le SCRS, approuvés ou refusés par la Cour fédérale ou le commissaire au renseignement et conservés par le SCRS (2019 à 2021)

	2019	2020	2021
Ensemble de données accessibles au public			
Évalués	8	11	4
Conservés	8	11	2[15]
Ensembles de données canadiens			
Évalués	10	0	2
Conservés	0	0	0[16]
Refusés par la CF	0	0	0

Ensembles de données étrangers			
Évalués	8	0	0
Conservés	0	1	1[17]
Refusés par le ministre	0	0	0
Refusés par le CR	0	0	0

Cadre de justification

88. La *Loi sur la sécurité nationale de 2017* a également créé un cadre de justification juridique pour les opérations de collecte de renseignements du SCRS. Le cadre établit une justification limitée pour les employés du SCRS et les personnes qui agissent selon ses directives pour mener des activités qui constitueraient autrement des infractions aux lois canadiennes. Le cadre de justification du SCRS est fondé sur ceux qui sont déjà en place pour l'application des lois canadiennes.[18] Le cadre de justification apporte au SCRS et aux Canadiens la clarté nécessaire quant à ce que le SCRS peut faire légalement dans le cadre de ses activités. Il reconnaît qu'il est dans l'intérêt du public de veiller à ce que les employés du SCRS puissent s'acquitter efficacement de leurs fonctions de collecte de renseignements, notamment à l'occasion de gestes et d'omissions qui seraient autrement illégaux, dans l'intérêt du public et conformément à la primauté du droit. Les types d'actes et d'omissions autrement illégaux qui sont autorisés par le cadre de justification sont déterminés par le ministre et approuvés par le commissaire du renseignement. Il existe des limites quant aux activités qui peuvent être réalisées et le cadre de justification ne permet pas de commettre un geste ou une omission qui porterait atteinte à un droit ou à une liberté garantie par la Charte.

89. Selon le paragraphe 20.1 (2) de la Loi sur le SCRS, les employés doivent être désignés par le ministre de la Sécurité publique pour être visés par le cadre de justification lorsqu'ils commettent ou dirigent une omission ou un acte autrement illégal. Les employés désignés sont des employés du SCRS qui ont besoin du cadre de justification pour exécuter leurs tâches et leurs fonctions. Les employés désignés sont justifiés de commettre eux-mêmes un acte ou une omission (commissions par les employés) et ils peuvent ordonner à une autre personne de commettre un acte ou une omission (directives de commettre) dans le cadre de leurs fonctions. L'OSSNR examine actuellement la mise en œuvre du cadre de justification par le SCRS. Les résultats de cet examen orienteront l'examen de la *Loi sur la sécurité nationale de 2017* par le Parlement.

Autorisations, commissions et directives en vertu du cadre de justification (2019 à 2021)

	2019	2020	2021
Autorisations	83	147	178
Commissions par les employés	17	39	51
Directives de commettre	32	84	116
Désignations en situation d'urgence	0	0	0

Conformité

90. Le programme de conformité opérationnelle interne du SCRS dirige et gère la conformité globale au sein du SCRS. L'objectif de cette unité consiste à promouvoir une culture de conformité au sein du SCRS en investissant dans la technologie de l'information pour soutenir le processus relatif aux mandats, en concevant une approche pour signaler et évaluer les incidents potentiels de non-conformité, en intégrant des experts dans les directions opérationnelles pour fournir des conseils et des directives en temps opportun et en établissant des politiques et des procédures internes pour les employés. Ce programme est le centre de traitement de tous les cas de non-conformité potentiels liés aux activités opérationnelles.

91. Les connaissances de l'OSSNR sur la non-conformité opérationnelle du SCRS et les infractions connexes à la Charte sont limitées aux renseignements figurant dans le rapport annuel du directeur du SCRS sur les opérations du ministre de la Sécurité publique. L'OSSNR constate avec intérêt que le SCRS signale des infractions à la Charte comme des cas de non-conformité. L'OSSNR continuera de surveiller de près les cas de non-conformité liés aux lois canadiennes et à la Charte et elle collaborera avec le SCRS pour améliorer la transparence quant à ces activités.

Incidents de non-conformité traités par le SCRS (2019 à 2021)

	2019	2020	2021
Incidents de non-conformité traités[19]	53	99	85
Administratifs		53	64
Opérationnels			21
Lois canadiennes	40[20]	19	1
Charte canadienne des droits et libertés			6

Conditions des mandats			6
Gouvernance du SCRS			8

Plan d'examen du SCRS de 2022

92. En 2022, l'OSSNR entreprendra ou mènera cinq examens axés exclusivement sur le SCRS : un examen axé sur la collaboration opérationnelle entre le SCRS et le CST (voir le plan d'examen de 2022 du CST ci-dessous), un examen axé sur la gestion par le SCRS et la GRC de l'extrémisme à caractère idéologique et un certain nombre d'examens interministériels qui comprennent un volet sur le SCRS.

93. En plus des trois examens obligatoires sur la *Loi sur la communication d'information ayant trait à la sécurité du Canada* (LCISC), la *Loi visant à éviter la complicité dans les cas de mauvais traitements infligés par des entités étrangères* et les MRM du SCRS, l'OSSNR a entrepris ou prévoit réaliser les examens suivants sur le SCRS :

Cadre de justification

Cet examen évaluera la mise en œuvre par le SCRS du nouveau cadre de justification pour les activités qui seraient autrement illégales, qui est autorisée en vertu de la *Loi sur la sécurité nationale de 2017*.

Ensembles de données

Cet examen portera sur la mise en œuvre du régime des ensembles de données du SCRS à la suite de l'entrée en vigueur de la *Loi sur la sécurité nationale de 2017*.

Programme de couverture du SCRS

Il s'agirait du premier examen sur les opérations de couverture du SCRS. Il portera sur l'ensemble des activités de couverture du SCRS et se concentrera sur l'acquisition de connaissances de base afin de permettre à l'OSSNR de sélectionner des activités spécifiques à examiner en profondeur au cours des prochaines années.

Extrémisme violent à caractère idéologique

Il s'agit d'un examen conjoint du SCRS et de la GRC sur leur gestion respective et conjointe de la menace de l'extrémisme violent à caractère idéologique (EVCI). L'examen portera essentiellement sur l'interaction entre le SCRS et la GRC dans le contexte de l'EVCI, l'évaluation de la conformité des activités à la loi, les directives ministérielles applicables et les politiques opérationnelles ainsi que sur la nécessité et le caractère raisonnable des activités.

94. Au-delà de 2022, l'OSSNR a l'intention d'examiner les activités du SCRS sur les sujets suivants :

- Le cycle de vie des renseignements obtenus dans le cadre des mandats;
- Le mandat du SCRS en vertu de l'article 16;
- Les politiques de conservation basée sur le critère du « strict nécessaire »;
- Le cadre de conformité interne du SCRS.

Accès aux renseignements du SCRS

95. Tout au long de l'année 2021, l'OSSNR a été confrontée à des niveaux d'accès et de réactivité différents par rapport au SCRS. Les restrictions liées à la COVID-19 ont entraîné des retards considérables dans la réception des renseignements et des séances d'information demandés et ont empêché l'OSSNR d'accéder directement aux bureaux qui lui sont réservés dans les locaux de l'administration centrale du SCRS.

96. En réponse aux demandes d'information de l'OSSNR, le SCRS a fait preuve de transparence dans sa capacité à répondre et à communiquer les retards prévus. Lorsque les niveaux d'accès et de dotation n'étaient plus restreints, les réponses du SCRS aux demandes formelles et informelles liées à l'étude des capacités techniques et à l'examen des MRM étaient complètes et opportunes et les séances d'information étaient bien organisées et fournissaient les renseignements demandés.

97. Comme susmentionné, tout au long de l'année 2021, l'OSSNR n'a pas eu accès en tout temps à ses bureaux réservés au sein de l'administration centrale du SCRS, qui sont utilisés par les employés de l'OSSNR chargés des examens, des enquêtes et des services juridiques. Par conséquent, l'OSSNR a eu un accès direct très limité aux systèmes d'information du SCRS. Pendant cette période, l'OSSNR a eu accès à divers locaux temporaires de l'administration centrale du SCRS.

98. Le SCRS a toutefois été en mesure de continuer d'offrir aux membres de l'OSSNR un accès à ses bureaux régionaux partout au Canada tout au long de 2021. Cet accès a été d'une grande aide pour les membres de l'OSSNR qui n'habitent pas dans la région de la capitale nationale et dont le travail exige souvent des installations sécurisées où ils peuvent accéder en toute sécurité à l'information pertinente aux examens et aux enquêtes. L'OSSNR apprécie grandement la volonté et les efforts du SCRS et de ses collègues régionaux à cet égard.

2.2 Examens sur le Centre de la sécurité des télécommunications

Aperçu

99. L'OSSNR a pour mandat d'examiner toute activité menée par le CST. L'OSSNR doit également présenter au ministre de la Défense nationale un rapport annuel sur les activités du CST, portant notamment sur le respect par le CST des lois et des directives ministérielles applicables ainsi que sur le caractère raisonnable et la nécessité de l'exercice des pouvoirs du CST.

100. En 2021, l'OSSNR a effectué deux examens du CST et a demandé au CST de mener une étude ministérielle, qui sont tous résumés ci-dessous. L'OSSNR a également entrepris cinq nouveaux examens axés sur les activités du CST qui devraient être achevés en 2022 (voir le plan d'examen du CST pour 2022, ci-dessous). De plus, le CST participe à d'autres examens interministériels de l'OSSNR comme les examens annuels obligatoires de la *Loi sur la communication d'information ayant trait à la sécurité du Canada* et de la *Loi visant à éviter la complicité dans les cas de mauvais traitements infligés par des entités étrangères* dont les résultats sont décrits ci-dessous (voir la section Examens interministériels).

101. Même si la pandémie et d'autres priorités ont empêché l'OSSNR de donner suite à ses engagements antérieurs concernant le caviardage, la traduction et la publication des examens de l'ancien bureau du commissaire du CST, l'OSSNR reste déterminé à publier ces documents, si les ressources le permettent.

Examen de la gouvernance des cyberopérations actives et défensives du CST

102. *La Loi sur le Centre de la sécurité des télécommunications* (Loi sur le CST) confère au CST le pouvoir de mener des cyberopérations actives (COA) et des cyberopérations défensives (COD). Au sens de la Loi sur le CST, les COA sont conçues pour « réduire, interrompre, influencer ou entraver les capacités, les intentions ou les activités d'un individu, d'un État, d'une organisation ou d'un groupe terroriste étranger en ce qui a trait aux affaires internationales, à la défense ou à la sécurité ». Les COD aident à protéger les systèmes du gouvernement fédéral canadien ou les systèmes jugés importants par le ministre de la Défense nationale pour le Canada contre les cybermenaces étrangères. Les COA et les COD sont autorisés par des autorisations ministérielles (AM) et, en raison des répercussions possibles sur la politique étrangère du Canada, exigent que le ministre des Affaires

étrangères consente à une AM qui concerne les COA ou soit consulté au sujet d'une AM qui concerne les COD.

103. Dans le cadre de l'examen, l'OSSNR a évalué le cadre de gouvernance du CST qui oriente le déroulement des cyberopérations défensives et actives et qui permet notamment de déterminer si le CST a pris en considération ses obligations juridiques et les répercussions des opérations sur la politique étrangère de manière appropriée. L'OSSNR a analysé les politiques et les procédures, les documents relatifs aux opérations et à la gouvernance et la correspondance entre le CST et Affaires Mondiales Canada (AMC). La portée de l'examen comprenait les premiers documents disponibles relatifs aux COA et aux COD et se terminait en même temps que la période de validité des premières autorisations ministérielles de COA et de COD (2019 à 2020).

104. L'OSSNR a intégré AMC dans cet examen en raison de son rôle clé dans la structure de gouvernance des COA et des COD. Par conséquent, l'OSSNR a pu comprendre les structures de gouvernance et de responsabilisation en place pour ces activités en obtenant des perspectives uniques de la part des deux ministères sur leurs rôles et leurs responsabilités respectifs.

105. La nouveauté de ces pouvoirs a obligé le CST à élaborer de nouveaux mécanismes et processus tout en tenant compte des nouvelles autorités et limites légales. L'OSSNR a constaté que le CST et AMC ont déployé des efforts considérables pour mettre en place la structure de gouvernance des COA et des COD. Dans ce contexte, l'OSSNR a constaté que certains volets de la gouvernance des COA et des COD pourraient être améliorés en les rendant plus transparents et plus clairs.

106. Plus précisément, l'OSSNR a constaté que le CST pourrait améliorer le niveau de détail fourni à toutes les parties qui participent à la prise de décisions et à la gouvernance des COA et des COD dans les documents comme les autorisations ministérielles autorisant ces activités et les plans opérationnels qui régissent leur exécution. En outre, l'OSSNR a constaté que le CST et AMC n'avaient pas pris en compte plusieurs lacunes cernées dans le cadre de cet examen et a recommandé des améliorations concernant :

- La mobilisation d'autres ministères pour assurer l'harmonisation d'une opération avec les priorités générales du gouvernement du Canada;
- La distinction entre une COA et une COD préventive;
- L'évaluation de la conformité de chaque opération au droit international;
- La communication entre les ministères de toute information nouvellement acquise qui est pertinente au niveau de risque d'une opération.

107. Les lacunes observées par l'OSSNR, si elles ne sont pas corrigées, pourraient comporter des risques. Par exemple, la nature générale des catégories d'activités, de techniques et de cibles qui composent les COA et les COD pourrait englober des activités et des cibles à risque élevé de façon involontaire. De plus, compte tenu de la différence dans l'engagement requis d'AMC dans les COA et les COD, une classification erronée de ce qui est vraiment un COA en tant que COD préventif pourrait entraîner un risque accru pour les relations internationales du Canada en raison de l'engagement insuffisant d'AMC.

108. Bien que cet examen ait porté sur les structures de gouvernance en jeu en ce qui concerne les COA et les COD, la façon dont ces structures sont mises en œuvre et suivies dans la pratique revêt une importance encore plus grande. L'OSSNR a formulé plusieurs observations au sujet des renseignements contenus dans les documents de gouvernance élaborés à ce jour et évaluera prochainement comment ils sont mis en pratique dans le cadre de l'examen de l'OSSNR axé sur les opérations elles-mêmes.

Réponse aux recommandations de l'OSSNR

109. Les recommandations de l'OSSNR et d'autres détails sur cet examen se trouvent à l'annexe D du présent rapport.

Examen sur l'échange de renseignements entre les divers volets du mandat du CST

110. Cet examen a porté sur le pouvoir juridique du CST de communiquer des renseignements obtenus dans le cadre d'un volet de son mandat afin de remplir un autre volet de son mandat. Plus précisément, l'examen était axé sur l'échange interne de renseignements au sein du CST entre le volet du renseignement étranger et le volet de la cybersécurité et de l'assurance de l'information du mandat du CST.

111. L'OSSNR a examiné si l'échange interne de renseignements du CST concernant un Canadien ou une personne au Canada est conforme à la *Loi sur la protection des renseignements personnels,* qui limite la façon dont les renseignements personnels recueillis peuvent être utilisés par une institution fédérale ainsi qu'à la Loi sur le CST, qui s'applique à la collecte et à l'utilisation fortuites d'information qui se rapporte à un Canadien ou à une personne se trouvant au Canada (IRCPC) par le CST. L'OSSNR a conclu que, d'après les descriptions des volets des articles 16 et 17 de la Loi sur le CST, les renseignements obtenus sous un volet peuvent parfois être utilisés aux mêmes fins ou à des fins similaires. Cette utilisation répondrait aux exigences de la *Loi sur la protection des renseignements personnels* en matière d'échange de renseignements à l'interne. Toutefois,

ce principe ne peut pas simplement s'appliquer de façon présumée, car les objectifs des volets diffèrent au sein de la Loi sur le CST. Le CST doit effectuer une analyse de conformité au cas par cas qui tient compte de l'objectif de la collecte et de l'échange d'information.

112. L'OSSNR estime qu'il est nécessaire que le chef du CST, dans sa demande d'autorisation ministérielle, informe pleinement le ministre de la Défense nationale de la façon dont l'IRCPC pourrait être utilisée et analysée par le CST, notamment en ce qui concerne l'échange de renseignements du IRCPC à un autre volet, et dans quelle fin. À une exception près, les demandes du chef présentées pendant la période visée par l'examen ont informé le ministre de la Défense nationale que l'IRCPC conservée pourrait être utilisée à l'appui d'un autre volet. De plus, les demandes de renseignement étranger ont informé le ministre sur la façon dont le CST a évalué le caractère « essentiel » des renseignements recueillis par l'IRCPC dans le cadre du volet sur le renseignement étranger.

113. En vertu de la politique du CST, une évaluation de la pertinence, du caractère essentiel ou de la nécessité de l'IRCPC pour chaque volet est requise pour échanger des renseignements entre les volets. La politique du CST fournit des définitions et des critères pour évaluer et appliquer ces seuils aux renseignements. L'OSSNR a constaté que le cadre stratégique du CST en ce qui concerne l'échange interne de renseignements entre les volets du mandat du renseignement étranger et de la cybersécurité est conforme à la Loi sur le CST.

Réponse aux recommandations de l'OSSNR

114. Les recommandations de l'OSSNR, la réponse de la direction du CST et d'autres détails sur cet examen se trouvent à l'annexe D du présent rapport.

Étude ministérielle du CST sur la communication de renseignements canadiens d'identification

115. À la suite d'un examen de 2020 sur la communication de renseignements canadiens d'identification (RCI)[21] par le CST, l'OSSNR a conclu que la mise en œuvre par le CST de son régime de communication en vertu de la *Loi sur la défense nationale* n'était peut-être pas conforme à la *Loi sur la protection des renseignements personnels.* Le 25 novembre 2020, à la suite de la publication de l'examen, l'OSSNR a présenté un rapport de conformité au ministre de la Défense nationale.[22] L'OSSNR était d'avis que le CST, en tant que gardien des RCI recueillis incidemment, a la responsabilité de s'assurer et de documenter qu'il existe un pouvoir de collecte et de communication avant de le partager avec des tiers destinataires. L'OSSNR a ensuite demandé au CST de mener une étude ministérielle sur la communication de RCI du 1er août 2019 au 1er mars 2021.[23]

116. L'étude ministérielle vise à s'assurer que la communication de RCI par le CST est effectuée d'une manière conforme à la Loi sur le CST et, par-dessus tout, que toutes les communications de RCI étaient essentielles aux affaires internationales, à la défense, à la sécurité ou à la cybersécurité.[24]

117. Le CST a fourni l'étude ministérielle achevée au ministre de la Défense nationale le 8 octobre 2021 et a remis un exemplaire à l'OSSNR le 1er novembre 2021. L'OSSNR est d'avis que le CST a fourni un compte rendu complet de son régime de communication pour la période d'examen demandée et a fourni un rapport qui répond aux objectifs détaillés du mandat de l'OSSNR. Ce faisant, le CST a défini son processus d'évaluation et de communication des demandes de RCI au gouvernement du Canada et aux clients étrangers en vertu de la Loi sur le CST, tout en faisant le point sur les changements pertinents qui ont été apportés au régime de communication en fonction des recommandations formulées par l'OSSNR dans le dernier examen sur les RCI.

118. La production de l'étude ministérielle a également permis au CST d'examiner le régime de communication de RCI du point de vue du CST. Ce processus permet à l'OSSNR de mieux comprendre comment le CST gère son programme et évalue ses autorisations juridiques pertinentes. En plus de contribuer à la compréhension actuelle du régime de communication du CST par l'OSSNR, l'étude aidera également à cerner des pistes d'enquête pour l'examen de suivi sur les RCI prévu pour 2023.

Statistiques

119. Pour accroître la responsabilisation à l'égard du public, l'OSSNR demande au CST de publier des statistiques et des données liées aux volets d'intérêt public et à la conformité de ses activités. L'OSSNR est d'avis que les statistiques suivantes permettront de renseigner le public sur la portée et l'ampleur des opérations du CST ainsi que sur l'évolution des activités d'une année à l'autre.

Autorisations ministérielles et arrêtés ministériels

120. Les autorisations ministérielles sont délivrées par le ministre de la Défense nationale et autorisent des activités précises menées par le CST conformément à l'un des volets de son mandat. Le tableau suivant présente les autorisations ministérielles délivrées entre 2019 et 2021.

Autorisations ministérielles du CST (2019 à 2021)

Type d'autorisation ministérielle	Article habilitant de la Loi sur le CST	Nombre d'AM délivrées en 2019	Nombre d'AM délivrées en 2020	Nombre d'AM délivrées en 2021
Renseignement étranger	26(1)	3	3	3
Cybersécurité — Infrastructures fédérales et non fédérales	27(1) et 27(2)	2	1	2
Cyberopérations défensives	29(1)	1	1	1
Cyberopérations actives	30(1)	1	1	2

Remarque : Ce tableau fait référence aux autorisations ministérielles qui ont été délivrées au cours des années civiles données et ne reflètent pas nécessairement les autorisations ministérielles qui étaient en vigueur à un moment donné. Par exemple, si une autorisation ministérielle a été délivrée à la fin de 2020 et est demeurée en vigueur pendant une partie de 2021, elle est comptée ci-dessus uniquement comme une autorisation ministérielle de 2020.

121. Les arrêtés ministériels sont émis par le ministre de la Défense nationale et désignent les personnes ou les organisations avec lesquelles le CST peut travailler et échanger des renseignements. Par exemple, un arrêté ministériel désignant les infrastructures d'information non fédérales comme étant importantes pour le gouvernement du Canada est nécessaire pour que le CST puisse s'acquitter de certains aspects de son mandat en matière de cybersécurité et de cyberopérations défensives. Un arrêté ministériel est également requis pour désigner les destinataires de RCI. Le tableau suivant énumère les trois arrêtés ministériels qui étaient vigueur en 2021.

Arrêtés ministériels du CST (2021)

Nom de l'arrêté ministériel	En vigueur en 2021	Article habilitant de la Loi sur le CST
Désignation de l'information électronique et des infrastructures de l'information comme étant d'importance pour le gouvernement du Canada.	1	21(1)
Désignation des destinataires des renseignements relatifs à un Canadien ou à une personne au Canada acquis, utilisés ou analysés dans le cadre des volets du mandat du CST liés à la cybersécurité et à l'assurance de l'information.	1	45 et 44(1)
Désignation des destinataires de renseignements canadiens d'identification utilisés, analysés ou conservés en vertu d'une autorisation de renseignement étranger en vertu de l'article 45 de la Loi sur le CST.	1	45 et 43

Rapports sur le renseignement étranger

122. Conformément à l'article 16 de la Loi sur le CST, ce dernier a pour mandat d'acquérir de l'information à partir de l'infrastructure mondiale de l'information (IMI)[25] ou par son entremise et d'utiliser, d'analyser et de diffuser l'information dans le but de fournir des renseignements étrangers, en conformité avec les priorités du gouvernement fédéral en matière de renseignement.

123. Selon le CST, 3050 rapports sur les produits finaux du renseignement étranger ont été transmis en 2021 à 1627 clients dans 28 ministères et organismes du gouvernement du Canada.

Information qui se rapporte à un Canadien ou à une personne se trouvant au Canada (IRCPC)

124. Comme indiqué dans l'examen sur l'échange de renseignements entre les divers volets du mandat du CST réalisé par l'OSSNR (voir ci-dessus), l'IRCPC constitue de l'information se rapportant à des Canadiens ou à des personnes se trouvant au Canada qui pourrait être recueillie incidemment par le CST lorsqu'il mène des activités liées au renseignement étranger ou à la cybersécurité en vertu d'une AM.[26] Selon la politique du CST, l'IRCPC constitue toute information reconnue comme faisant référence à un Canadien ou à une personne se trouvant au Canada, peu importe si cette information peut être utilisée pour identifier un Canadien ou une personne se trouvant au Canada ou non.

125. On a demandé au CST de publier des statistiques ou des données sur la régularité avec laquelle de l'IRCPC ou l'information recueillie au Canada est incluse dans les rapports sur les produits finaux du CST. Le CST a répondu que [traduction] « comme ce type d'information n'a pas été diffusé publiquement auparavant, le CST procède à une évaluation du préjudice pour déterminer si l'information peut être fournie en vue de sa publication. » Le CST a ajouté que [traduction] « l'évaluation des répercussions pour la communication de l'information demandée constitue un effort à plus long terme, qui ne sera probablement pas résolu à temps pour le rapport annuel public de 2021 de l'OSSNR. Veuillez considérer que la réponse du CST est qu'il n'y a pas d'information communicable aux fins du rapport de cette année. »

Renseignements canadiens d'identification (RCI)

126. Il est interdit au CST de cibler des Canadiens ou des personnes se trouvant au Canada dans le cadre de ses activités. Toutefois, compte tenu de la nature de l'infrastructure

internationale de l'information et des méthodes de collecte du CST, de tels renseignements peuvent être recueillis incidemment par le CST. Lorsqu'ils sont utilisés dans un rapport du renseignement étranger du CST, les renseignements recueillis incidemment susceptibles d'identifier un Canadien ou une personne se trouvant au Canada sont supprimés afin de protéger la vie privée des personnes en question. Le CST peut communiquer les RCI non supprimés à des destinataires désignés lorsqu'ils disposent d'un pouvoir juridique et d'une justification opérationnelle de la recevoir et lorsque l'information est essentielle aux affaires internationales, à la défense ou à la sécurité (y compris la cybersécurité).

127. Le tableau suivant indique le nombre de demandes de communication de RCI reçues par le CST en 2021.

Nombre de demandes de communication de RCI (2021)

Types de demandes	
Demandes du gouvernement du Canada	741
Demandes du Groupe des cinq[27]	90
Demandes d'organismes ne faisant pas partie du Groupe des cinq	0
Total	831

128. On a également demandé au CST de publier le nombre de cas où des RCI ont été supprimés de rapports sur la cybersécurité et le renseignement étranger du CST. Le CST a répondu que [traduction] « comme ce type d'information n'a pas été diffusé publiquement auparavant, le CST procède à une évaluation du préjudice pour déterminer si l'information peut être fournie en vue de sa publication. » Le CST a ajouté que [traduction] « l'évaluation des répercussions pour la communication de l'information demandée constitue un effort à plus long terme, qui ne sera probablement pas résolu à temps pour le rapport annuel public de 2021 de l'OSSNR. Veuillez considérer que la réponse du CST est qu'il n'y a pas d'information communicable aux fins du rapport de cette année.»

Incidents liés à la protection des renseignements personnels et erreurs de procédure

129. Un incident lié à la protection des renseignements personnels se produit lorsque la vie privée d'un Canadien ou d'une personne se trouvant au Canada est mise à risque d'une manière qui va à l'encontre des politiques du CST ou qui n'est pas prévue par celles-ci. Le CST assure le suivi de ces incidents au moyen de son dossier des incidents liés à la protection des renseignements personnels[28], de son dossier des incidents liés à la

protection des renseignements personnels de seconde partie[29] et de son dossier d'erreurs de procédure mineures[30], respectivement.

130. Le tableau suivant indique le nombre d'incidents liés à la protection des renseignements personnels et d'erreurs de procédure dont le CST a fait le suivi en 2021.

Incidents liés à la protection des renseignements personnels et erreurs de procédure (2021)

Type d'incident	Nombre
Incidents liés à la protection des renseignements personnels	96
Incidents liés à la protection des renseignements personnels de seconde partie	33
Erreurs de procédure mineures	18

Cybersécurité et assurance de l'information

131. Conformément à l'article 17 de la Loi sur le CST, le CST a pour mandat de fournir des avis, des conseils et des services afin d'aider à protéger l'information électronique et les infrastructures de l'information des institutions fédérales, de même que des entités non fédérales désignées par le ministre comme étant d'importance pour le gouvernement du Canada.

132. On a demandé au CST de publier des statistiques ou des données décrivant les activités du CST liées aux volets de la cybersécurité et de l'assurance de l'information de son mandat. Le CST a répondu que :

> *[traduction] De manière générale, le Centre canadien pour la cybersécurité ne fait pas de commentaires sur des incidents de cybersécurité précis, ne confirme pas les entreprises ou les partenaires d'infrastructure essentiels avec lesquels il collabore et ne fournit pas de statistiques sur le nombre d'incidents signalés. Les statistiques sur les cyberincidents, notamment la cybercriminalité, sont fondées sur les victimes qui se manifestent, ce qui n'est pas un reflet exact de l'environnement canadien.*
>
> *Le CST et le Centre canadien pour la cybersécurité travaillent chaque jour pour défendre les systèmes du gouvernement du Canada contre les cyberattaques. Chaque jour, les capacités de défense dynamique du CST bloquent jusqu'à sept milliards de balayages de reconnaissance sur ces systèmes.*

Cyberopérations actives et défensives

133. Conformément à l'article 18 de la Loi sur le CST, le CST a pour mandat de mener des cyberopérations défensives afin d'aider à protéger l'information électronique et les

infrastructures de l'information des institutions fédérales, de même que des entités non fédérales désignées par le ministre comme étant d'importance pour le gouvernement du Canada contre les cyberattaques hostiles.

134. Conformément à l'article 19 de la Loi sur le CST, le CST a pour mandat de mener des cyberopérations actives contre des étrangers, des États, des organismes ou des groupes terroristes étrangers dans la mesure où elles se rapportent aux affaires internationales, à la défense ou à la sécurité.

135. L'OSSNR a demandé au CST de publier le nombre de COD et de COA approuvés en 2021. Le CST a répondu qu'il n'était pas en mesure de fournir cette information aux fins de publication par l'OSSNR, car « [traduction] cela pourrait porter atteinte aux relations internationales, à la défense nationale et à la sécurité nationale du Canada. »

Assistance technique et opérationnelle

136. Dans le cadre du volet du mandat du CST de l'assistance technique et opérationnelle, le CST a reçu des demandes d'assistance d'organismes de l'application de la loi et de la sécurité du Canada, de même que de la part du ministère de la Défense nationale et des Forces armées canadiennes.

137. Le tableau suivant indique le nombre de demandes d'assistance que le CST a reçues et auxquelles il a donné suite en 2020 et en 2021.

Demandes d'assistance	2020	2021
Nombre de demandes reçues	24	35
Nombre de demandes auxquelles le CST a donné suite	23	32

Plan d'examen du CST de 2022

138. En plus des deux examens obligatoires sur la *Loi sur la communication d'information ayant trait à la sécurité du Canada* et la *Loi visant à éviter la complicité dans les cas de mauvais traitements infligés par des entités étrangères*, dont le CST fait l'objet, l'OSSNR a entrepris ou prévoit réaliser les cinq examens suivants sur le CST :

Examen du programme de sécurité interne du CST (mesures de protection)

Cet examen portera sur la façon dont le CST protège ses employés, ses renseignements et ses biens. Il explorera les façons dont le CST atténue les risques internes liés à la sécurité au moyen d'enquêtes et, en particulier, l'utilisation du polygraphe comme outil dans le processus de filtrage de sécurité. L'examen évaluera également la conformité du CST aux politiques et aux directives en matière de sécurité du Conseil du Trésor ainsi que la pertinence, la conformité et l'efficacité des processus internes du CST servant à traiter les incidents de sécurité, les violations et les infractions à la sécurité réels et potentiels.

Examen sur la cybersécurité — Solutions axées sur les réseaux

Il s'agit du premier examen de l'OSSNR axé sur les volets du mandat du CST de la cybersécurité et de l'assurance de l'information. Il étudiera l'utilisation d'un outil précis : les solutions axées sur les réseaux, telles que décrites dans l'autorisation ministérielle sur la cybersécurité.

Examen des cyberopérations actives et défensives — Partie 2 (opérations)

Il s'agit de la suite de l'examen de l'OSSNR sur les cyberopérations actives et défensives effectuées avant le 30 juillet 2021. Le premier examen portait sur les procédures et les politiques internes régissant l'utilisation par le CST de cyberopérations actives et défensives. L'examen s'appuie sur les travaux précédents de l'OSSNR et sera axé sur la mise en œuvre de ces structures de gouvernance dans les opérations réelles.

Examen d'un programme relevant du mandat du renseignement étranger

Il s'agit d'un examen sur un programme classifié relevant du volet du mandat du CST du renseignement étranger. Ce programme est autorisé par une autorisation ministérielle, qui en établira également les paramètres.

Examen sur la collaboration opérationnelle entre le CST et le SCRS

L'examen portera sur la collaboration opérationnelle entre le CST et le SCRS, à la fois sous le volet du mandat du CST, mais également en ce qui concerne les activités opérationnelles conjointes et coordonnées entre les mandats respectifs des deux organismes.

139. Au-delà de 2022, l'OSSNR a l'intention d'examiner les sujets suivants, sans toutefois s'y limiter :

- Un examen annuel sur la conformité des activités du CST;
- Les pratiques de conservation des renseignements électromagnétiques (SIGINT) du CST;
- Un programme de collecte du CST mené en vertu d'une autorisation ministérielle;
- Le cadre de gestion des actifs du CST.

Accès à l'information du CST

140. Dans son rapport annuel public de 2020, l'OSSNR a indiqué qu'il cherchait à officialiser la fourniture par le CST de catégories précises de renseignements sur une base régulière comme les autorisations, les arrêtés et les directives ministériels qui serviraient à assurer la conformité des activités et à éclairer les conclusions que l'OSSNR formule dans le rapport annuel classifié à l'intention du ministre de la Défense nationale. L'OSSNR commencera cet examen nommé « examen annuel de la conformité du CST » en 2022. L'OSSNR est heureux d'annoncer que le CST a déjà commencé à fournir les renseignements demandés.

141. L'OSSNR a également signalé précédemment que le manque d'accès complet et vérifiable aux dépôts d'information du CST posait un défi important à la capacité de l'OSSNR d'examiner les activités du CST. En 2021, ce défi persistait.

142. En 2021, l'OSSNR a cherché à obtenir un accès direct aux répertoires d'information du CST, conformément au modèle d'examen « Faites confiance, mais vérifiez » de l'OSSNR.[31] À l'exception d'un espace de bureau dédié que l'OSSNR continue d'utiliser à l'administration centrale du CST, l'OSSNR et le CST n'ont été en mesure de mettre en place un modèle viable du principe « Faites confiance, mais vérifiez » pour aucun des examens du CST jusqu'à présent, malgré plusieurs propositions de cas types présentées par l'OSSNR tout au long de l'année. L'OSSNR demeure résolu à obtenir un meilleur accès vérifiable à l'information du CST afin de soutenir la force de ses conclusions et en ses recommandations et, par le fait même, d'assurer une plus grande transparence des activités du CST envers le Parlement et le public canadien.

143. Plutôt que d'accéder directement aux répertoires d'information du CST, l'OSSNR doit s'en remettre au personnel des examens externes du CST pour recueillir l'information pertinente que possède le CST en son nom. Le personnel des examens externes du CST organise des séances d'information avec des experts en la matière, sollicite des réponses à des questions précises et coordonne les recherches effectuées par les employés du CST dans les répertoires d'information pour trouver des documents et d'autre matériel pertinent pour les examens. L'OSSNR reconnaît le travail du personnel chargé des examens externes du CST et le remercie pour sa contribution au travail d'examen.

144. Toutefois, le fait de s'en remettre au CST pour trouver, rassembler et conserver l'information destinée à l'OSSNR ne constitue pas une solution de rechange viable à l'accès direct à long terme. Actuellement, lorsqu'il reçoit une demande d'information, le CST mène un long processus de recherche et de collecte d'information, suivi d'un examen interne de cette information pour en déterminer la pertinence avant de la communiquer à l'OSSNR. Le fait que le CST détermine préalablement la pertinence de l'information nuit au pouvoir de

l'OSSNR de déterminer si l'information est liée à ses examens et contribue à retarder considérablement la communication de l'information à l'OSSNR. En outre, le processus entraîne une charge de travail accrue pour le personnel du CST qui doit coordonner les réponses aux demandes d'information de l'OSSNR. Cette charge de travail pourrait être considérablement réduite en permettant à l'OSSNR d'effectuer ses propres recherches dans les répertoires d'information du CST. Par ailleurs, cette méthode de vérification permettrait de renforcer la confiance de l'OSSNR en l'exhaustivité de l'information examinée.

145. Au-delà des problèmes liés aux limites de la capacité de l'OSSNR à suivre le modèle d'examen « Faites confiance, mais vérifiez », il y a des préoccupations continues liées à la réactivité du CST. Comme il a été mentionné précédemment, les retards importants dans la communication de l'information ont continué d'être problématique pour tous les examens de l'OSSNR sur les activités du CST en 2021.[32] Bien que la pandémie de COVID-19 ait interrompu la vie partout, elle ne pouvait à elle seule expliquer l'ampleur des retards subis en 2021. La communication en temps opportun de l'information requise pour un examen facilite non seulement le travail de l'OSSNR, mais constitue une exigence légale que l'OSSNR s'attend à ce que le CST respecte.

146. La seule exception au droit d'accès de l'OSSNR aux renseignements sous le contrôle du CST sont les documents confidentiels du Conseil privé de la Reine pour le Canada, également connu sous le nom de documents confidentiels du Cabinet. Les renseignements assujettis à la *Loi sur la protection des renseignements personnels* ou à toute autre loi du Parlement ainsi que les renseignements hautement classifiés ou faisant l'objet d'un contrôle exceptionnel doivent être mis à la disposition de l'OSSNR en temps opportun, lorsqu'ils sont liés à un examen. Cela n'a pas toujours été le cas en 2021.

147. À la lumière des difficultés constantes auxquelles l'OSSNR fait face dans le cadre de ses examens sur le CST, l'OSSNR continue d'être d'avis que le seul mécanisme qui permettrait d'assurer un niveau élevé de confiance, de fiabilité et d'indépendance dans son travail serait d'obtenir un accès direct à l'information pertinente pour ses examens. Un moyen important pour le CST de continuer d'accroître le niveau de transparence de ses activités est de faciliter l'accès direct aux examens externes. Pour que l'OSSNR puisse mener ses travaux avec un niveau de confiance élevé, il doit simplement être en mesure de vérifier que l'information sur laquelle il fonde ses conclusions et ses recommandations est exacte et complète. L'OSSNR continuera de collaborer avec le CST pour cerner des moyens par lesquels il peut commencer à mettre en œuvre d'autres éléments du modèle d'examen « Faites confiance, mais vérifiez » d'une manière plus complète et pertinente.

2.3 Autres ministères

Aperçu

148. En plus du SCRS et du CST, l'OSSNR a entrepris des examens sur les ministères et organismes suivants en 2021 :

- Le ministère de la Défense nationale (MDN) et les Forces armées canadiennes (FAC);
- La Gendarmerie royale du Canada (GRC);
- Immigration, Réfugiés et Citoyenneté Canada (IRCC);
- L'Agence des services frontaliers du Canada (ASFC);
- Transports Canada (TC).

149. En outre, dans le cadre des examens annuels de la *Loi sur la communication d'information ayant trait à la sécurité du Canada* et de la *Loi visant à éviter la complicité dans les cas de mauvais traitements infligés par des entités étrangères*, l'OSSNR a collaboré avec tous les ministères et organismes qui font partie de l'appareil de la sécurité nationale et du renseignement.

150. Les sections suivantes décrivent les examens terminés ou amorcés en 2021, par ministère ou organisme, ainsi que certains examens prévus pour les années à venir.

Ministère de la Défense nationale et Forces armées canadiennes

Étude de l'entreprise du renseignement de défense du ministère de la Défense nationale et des Forces armées canadiennes

151. L'étude avait trois objectifs : le premier consistait à comprendre le concept de l'entreprise du renseignement de défense (ERD), qui est le cadre dans lequel le MDN et les FAC mènent leurs activités en matière de renseignement. Le second objectif consistait à établir et à comprendre les fonctions de surveillance au sein de l'ERD, de même que le signalement des cas des non-conformité. Enfin, l'information recueillie par le biais des deux premiers objectifs de l'examen a permis à l'OSSNR d'acquérir des connaissances préalables pour l'aider à concevoir ses prochains examens.

152. Bien qu'elle ne représente qu'un faible pourcentage du travail du MDN et des FAC, la fonction du renseignement prend de l'ampleur tant dans la façon dont le MDN et les FAC perçoivent son importance que dans l'affectation des ressources. Toutes les structures et

les activités liées au renseignement du MDN et des FAC relèvent de l'ERD alors, si l'OSSNR ne comprend pas cette entreprise, son plan d'examen manquerait de cohérence et d'organisation. L'ERD représente une structure vaste et complexe avec des activités et des fonctions très variées. Les examens successifs s'appuieront sur les connaissances et l'expérience de l'OSSNR, tout en développant l'expertise requise pour cerner de manière proactive les sujets des prochains examens. De plus, une compréhension plus exhaustive de l'ERD permettra de mieux situer le MDN et les FAC dans la communauté de la sécurité nationale et du renseignement, ce qui permettra de cerner davantage d'activités d'examen horizontales.

153. L'étude a également contribué à mettre en évidence et à déterminer certaines des difficultés auxquelles l'OSSNR pourrait faire face lors d'examens sur le MDN et les FAC. Notamment, le MDN et les FAC représentent une structure vaste et complexe, avec des activités et des fonctions très variées. Les structures hiérarchiques sont complexes. Par exemple, les structures de la haute direction du MDN relèvent directement du sous-ministre, les commandements des Forces armées canadiennes relèvent du chef d'état-major de la défense et certaines structures hiérarchiques nécessitent de rendre des comptes aux deux. L'OSSNR a également constaté que les procédures de stockage et de collecte d'information varient au sein de l'organisation et qu'il existe plus de 180 répertoires d'information indépendants. La combinaison de ces éléments souligne l'importance de maintenir de solides relations de travail avec le MDN et les FAC pour faciliter l'accès à l'information et aux biens opportuns. L'OSSNR travaille en étroite collaboration avec le MDN et les FAC sur la façon de surmonter toutes ces difficultés. Une possibilité est de fournir des chaînes de recherche détaillées et des séances d'information de suivi pour confirmer la fiabilité, l'exhaustivité et la spécificité des documents fournis.

Examen de l'Unité nationale de contre-ingérence des Forces canadiennes — Collecte opérationnelle et pratiques en matière de protection des renseignements personnels

154. Cet examen donne suite à l'examen de l'année dernière sur l'Unité nationale de contre-ingérence des Forces canadiennes (UNCIFC). L'examen était axé sur la façon dont les recherches en technologie de l'information (TI) étaient utilisées à l'appui des enquêtes de contre-ingérence. L'examen a permis de déterminer si les recherches en TI et la collecte de renseignements à l'appui des enquêtes de contre-ingérence portaient atteinte aux attentes raisonnables des personnes en matière de protection des renseignements personnels dans ces circonstances.

155. Au cours de l'examen, l'OSSNR a cerné trois sujets de préoccupation liés aux demandes de contre-ingérence dans les réseaux internes de TI et à leur exécution. Ces sujets sont classés

selon les catégories suivantes : (1) la recherche par l'UNCIFC des activités liées aux courriels, à Internet et aux appareils mobiles d'un sujet; (2) la liste de vérification de l'UNCIFC utilisée pour déterminer et restreindre les paramètres de recherche et la façon dont les intervenants applicables définissent les paramètres de recherche; (3) la façon dont l'acquisition de l'information est utilisée pour élargir les recherches supplémentaires.

156. L'OSSNR estime que les employés du MDN et que les membres des FAC ont des attentes raisonnables en matière de protection des renseignements personnels lorsqu'ils utilisent les ordinateurs de travail à des fins personnelles. L'UNCIFC a besoin de l'aide des services de police ou des organismes de sécurité pour obtenir des mandats de perquisition ou des services d'interception technique dans le cadre d'enquêtes de niveau II et III. L'OSSNR a conclu que l'UNCIFC pourrait possiblement s'appuyer de façon inappropriée aux politiques du MDN et des FAC comme autorité légitime pour nuire à l'attente raisonnable d'un sujet en matière de protection des renseignements personnels.

157. L'OSSNR a observé que les renseignements obtenus par l'UNCIFC au moyen de la liste de vérification peuvent potentiellement permettre de saisir des renseignements personnels et intimes qui ont trait aux renseignements biographiques d'un sujet. L'OSSNR a constaté que la liste de vérification risque de recueillir des renseignements qui sont protégés en vertu de l'article 8 de la Charte. L'OSSNR a également constaté que le MDN et les FAC appliquent une définition des métadonnées qui comprend des renseignements pouvant faire l'objet d'une attente raisonnable en matière de protection des renseignements personnels.

158. L'OSSNR a observé que l'UNCIFC utilise de vastes paramètres de recherche dans le cadre de recherches en TI, ce qui pourrait comprendre des renseignements qui ne sont pas pertinents aux fins de l'enquête. Ces paramètres étaient appliqués sous forme d'approbations générales, sans contrôles internes spécifiques ou surveillance, tant sur le plan opérationnel que sur le plan professionnel. Les techniques de collecte, attribuables en partie aux limites des outils d'audit informatiques et aux vastes paramètres de recherche, ont permis de ratisser large. L'OSSNR a conclu que les pratiques d'enquête du système de TI observées dans le contexte des enquêtes de contre-ingérence de l'UNCIFC n'ont pas une surveillance juridique suffisante pour s'assurer qu'elles sont le moins invasives possible.

159. À la suite de ces conclusions, l'OSSNR a recommandé que le MDN et les FAC suspendent les pratiques du système d'enquête de TI dans le contexte des enquêtes de contre-ingérence de l'UNCIFC jusqu'à ce qu'une autorisation légale raisonnable ait été établie. Une fois qu'une autorité légale raisonnable a été établie, le MDN et les FAC devront créer un nouveau cadre stratégique qui reflète les conclusions notées.

Réponse aux recommandations de l'OSSNR

160. Les recommandations de l'OSSNR, la réponse de la direction du MDN et les FAC et d'autres détails concernant cet examen figurent à l'annexe D du présent rapport.

Examens prévus ou en cours

161. L'OSSNR a prévu plusieurs examens sur le MDN et les FAC et poursuivra deux d'entre eux en 2022. Le premier examen se penchera sur le programme de renseignement humain (HUMINT) du MDN et des FAC. Cet examen portera sur l'ensemble du programme de gestion des sources humaines utilisé par le MDN et les FAC.

162. Le deuxième examen se penche actuellement sur les activités nationales de collecte à source ouverte du MDN et des FAC. Plus précisément, cet examen examinera de plus près les autorisations légales et le cadre stratégique, le soutien aux programmes et la formation en vue de ceux-ci, les systèmes de gestion de l'information et de la technologie, les activités de collecte, la production et la diffusion de renseignements ainsi que les mécanismes de surveillance et de responsabilisation.

Accès aux renseignements du MDN et des FAC

163. Le MDN (avec les FAC) est le plus grand ministère fédéral, tant sur le plan du personnel (127 000 employés, y compris les forces régulières et de la réserve) que sur le plan des installations (42 unités opérationnelles dans la région de la capitale nationale seulement). Étant donné sa portée, au pays comme à l'étranger, la collecte et l'entreposage des données varient au sein de l'organisation, qui possède plus de 180 dépôts électroniques indépendants. L'OSSNR accède principalement à l'information par l'entremise de l'organe de liaison du MDN et des FAC : le Secrétariat de la coordination de l'examen et de la surveillance de la sécurité nationale et du renseignement (SCESSNR).

164. Afin d'accorder à l'OSSNR un accès complet et en temps opportun à l'information demandée, le MDN et les FAC ont officialisé les processus de réponses aux demandes de renseignements nécessitant une approbation ou une attestation de niveau 1 de la part du sous-ministre adjoint (SMA) ou de son équivalent. Ainsi, lorsque le SCESSNR reçoit une demande de renseignements, il communique avec les intervenants internes pour obtenir l'information demandée et la soumettre à l'approbation du SMA. Ensuite, le SMA (ou son équivalent) fournit une attestation de la direction, qui garantit que l'information fournie est complète et exacte.

165. L'OSSNR a aussi établi un accès direct à des systèmes de TI du MDN et des FAC, dans le cadre d'un examen en cours et s'affaire à élaborer un modèle d'accès à distance en vue

d'examens ultérieurs. En fin de compte, c'est la nature et la portée de l'examen qui dicteront le modèle à privilégier, pour ce qui est de l'accès aux renseignements et de la vérification. L'OSSNR s'engage toujours à travailler avec le SCESSNR pour veiller à ce que les processus liés à l'accès aux renseignements et à la vérification répondent aux exigences de l'examen.

Gendarmerie royale du Canada (GRC)

Examens prévus ou en cours

166. L'OSSNR travaille actuellement à trois examens portant exclusivement sur la GRC. Le premier examen évalue l'utilisation de sources humaines par la GRC dans le cadre d'enquêtes criminelles liées à la sécurité nationale. Le deuxième examen porte sur la façon dont la GRC contourne le chiffrement lorsqu'elle intercepte des communications privées dans le cadre d'enquêtes criminelles liées à la sécurité nationale. Enfin, le troisième examen, qui porte sur l'Unité de recherche opérationnelle (RO) de la GRC, examinera l'accès et l'utilisation des renseignements de sécurité par l'Unité. La GRC participe également à un examen interministériel dont il est question ci-dessous.

Accès aux renseignements de la GRC

167. L'OSSNR a commencé à examiner les activités de la GRC en 2020 et il n'a toujours pas un accès direct à ses systèmes de technologies de l'information (TI). Le caractère décentralisé des fonds de renseignements de la GRC, les restrictions liées à la COVID-19 et les contraintes liées à d'autres urgences ont fait en sorte que la GRC tarde à fournir à l'OSSNR l'information demandée. L'OSSNR s'est engagé à collaborer avec l'équipe des examens externes de la conformité en matière de sécurité nationale (EECSN) afin d'établir des approches permettant l'obtention de renseignements en temps opportun.

168. Au lieu d'avoir directement accès aux systèmes de TI de la GRC, l'OSSNR compte présentement sur l'équipe du CRSNG de la GRC pour recueillir les renseignements pertinents. L'OSSNR remercie l'équipe du CRSNG de sa contribution aux travaux d'examen mais se réjouit à la perspective d'obtenir un accès direct aux systèmes de TI de la GRC ou à d'autres processus de vérification indépendants qui procurent à l'OSSNR une confiance indépendante dans la fiabilité et l'exhaustivité des l'information à laquelle il a accès.

Agence des services frontaliers du Canada

169. En 2021, l'OSSNR a achevé son examen de l'utilisation de la biométrie par le gouvernement du Canada dans le continuum frontalier. Si cet examen visait aussi IRCC et TC, l'examen des activités de l'ASFC en était une composante importante. Le résumé de cet examen se trouve plus loin dans la section *Examens multiministériels*.

170. L'OSSNR a par ailleurs réalisé des progrès considérables concernant deux examens visant l'ASFC. Le premier porte sur le ciblage des passagers aériens, plus précisément sur l'utilisation de l'analyse prévisionnelle par l'ASFC pour cibler les passagers aériens devant faire l'objet d'une surveillance accrue à leur entrée au pays dans le contexte de menaces à la sécurité nationale. Le second vise à évaluer l'utilisation par l'ASFC de sources humaines confidentielles et s'appuie sur le travail réalisé dans ce domaine par le CPSNR[33].

Centre d'analyse des opérations et déclarations financières du Canada

171. L'OSSNR travaille actuellement à son premier examen du Centre d'analyse des opérations et déclarations financières du Canada (CANAFE). L'OSSNR se penchera sur le régime actuel d'échange de renseignements du CANAFE avec ses partenaires nationaux et internationaux en examinant les demandes de renseignements et les communications aux unités étrangères du renseignement financier.

2.4 Examens multiministériels

Examen de l'utilisation de la biométrie par le gouvernement du Canada dans le continuum frontalier

172. La biométrie joue un rôle fondamental dans le continuum frontalier[34]. Elle sert notamment au filtrage des ressortissants étrangers cherchant à entrer au Canada et au ciblage de passagers aériens internationaux. Au cours de son examen, l'OSSNR s'est penché sur les activités menées par l'ASFC, IRCC et TC. L'examen s'est étendu aux activités de la GRC, qui joue un rôle de soutien dans l'un des principaux programmes utilisant la biométrie dirigés par IRCC.

173. Les données biométriques sont des renseignements personnels de nature sensible. En effet, l'identification des personnes en fonction de leurs caractéristiques biologiques soulève des préoccupations sur le plan de la confidentialité et des droits de la personne. Le public a exprimé des craintes en ce qui a trait à l'utilisation des données biométriques par le

gouvernement, notamment l'utilisation de la technologie de reconnaissance faciale et la question des répercussions que celle-ci pourrait avoir sur les groupes marginalisés. D'autre part, le ciblage des personnes entrant au pays (et le fait de déterminer si elles ont ou non le droit d'entrer ou si elles peuvent poser des risques en matière de sécurité nationale) est une fonction qui se rapporte à la sécurité nationale. Ainsi, l'équilibre entre la confidentialité et la sécurité s'impose lorsqu'il est question d'utiliser la biométrie.

174. L'objectif immédiat de cet examen consistait à définir la nature et la portée des activités biométriques ayant cours dans l'espace en question. Pour ce faire, il a fallu notamment examiner la collecte, la conservation, l'utilisation et la communication des données biométriques ainsi que les autorisations légales en vertu desquelles ces activités ont cours. L'examen a aussi tenu compte de la raisonnabilité et de la nécessité de telles activités en étudiant l'exactitude et la fiabilité des données biométriques recueillies.

175. L'examen présente un ensemble d'observations liées à neuf thèmes majeurs :

- *Biométrie et sécurité nationale :* Au fil du temps, on a cessé d'invoquer la sécurité nationale comme principale raison pour justifier l'utilisation de la biométrie. D'autres objectifs sont maintenant pris en compte tels que la gestion de l'identité et les mesures de facilitation pour les voyageurs. Par conséquent, il est difficile d'examiner les activités liées à la biométrie de manière générale en tant qu'activités liées à la sécurité nationale. Dans le cadre d'examens ultérieurs, l'OSSNR se concentrera davantage sur l'examen d'activités liées à la biométrie qui entretiennent un lien étroit et direct avec la sécurité nationale.
- *Activités permanentes*[35]. De manière générale, les activités permanentes de biométrie dans le continuum frontalier sont bien appuyées par les autorisations légales actuelles et sont menées conformément à la pratique internationale.
- *Utilisation élargie de la biométrie au fil du temps.* Au cours des trente dernières années, la biométrie dans le continuum frontalier a connu un essor considérable et il est probable que son expansion continue. Les nouvelles activités liées à la biométrie doivent être justifiées dans le respect des exigences de nécessité et de proportionnalité en ce qui a trait à la collecte et à l'utilisation des données biométriques à des fins particulières et bien précises.
- *Projets pilotes.* Les projets pilotes et les initiatives soulèvent davantage de préoccupations que les activités permanentes étant donné qu'ils risquent d'être mis en œuvre de manière expérimentale sans l'appui d'analyses juridiques et de politiques suffisantes. Malgré la nature temporaire ou expérimentale d'un projet, l'OSSNR s'attend à ce que les ministères et organismes mènent les analyses nécessaires afin de vérifier les autorisations légales et

les politiques qui régissent la collecte, l'utilisation, la conservation et la communication des renseignements personnels.

- *Évolution des normes juridiques et sociétales*. Le débat public entourant les pouvoirs juridiques soulève la question de savoir si les normes et les protections existantes sont suffisantes pour réglementer les activités biométriques ou si de nouvelles normes et protections sont nécessaires. La frontière est, comparativement, un espace dans lequel une plus grande intrusion est considérée comme raisonnable, mais des limites à ces justifications existent et nécessiteront un calibrage minutieux à l'avenir.
- *Double utilisation de la biométrie.* L'OSSNR a relevé plusieurs cas où il était possible de faire une double utilisation des données biométriques dans le cadre des activités examinées dans le présent rapport. Même lorsque les avantages sont vérifiables, les nouvelles manières d'utiliser les données biométriques doivent être examinées avec soin pour veiller à leur raisonnabilité et à leur proportionnalité. De plus, toute nouvelle utilisation de la biométrie doit être justifiée et autorisée en vertu de la loi. Le principe de « limitation de la finalité » peut servir à contrôler la double utilisation dans le contexte des activités liées à la biométrie[36].
- *Systèmes techniques.* Un chevauchement important a été constaté entre les systèmes techniques et les bases de données utilisés pour l'ensemble des activités permanentes de biométrie. Si l'architecture globale des systèmes est complexe, elle n'est pas nécessairement problématique pour autant.
- *Visibilité des algorithmes.* Les ministères et organismes ont une visibilité limitée relativement au fonctionnement des algorithmes qu'ils utilisent aux fins d'analyses biométriques. Cependant, chaque ministère et organisme a démontré que les mesures de rendement sont connues et testées et que des seuils personnalisés sont utilisés au besoin.
- *Prévention des préjugés et de la discrimination*. IRCC et l'ASFC ont effectué des analyses préliminaires pour explorer la façon dont leurs activités biométriques peuvent avoir une incidence sur divers groupes de personnes, bien que la mise en œuvre de stratégies d'atténuation possibles n'ait pas toujours été apparente. Dans certains contextes, les progrès technologiques ont contribué à réduire, mais non à éliminer, les impacts différentiels. Il reste encore du travail à faire pour atténuer les impacts différentiels sur certains segments de la population. Parallèlement, les ministères et organismes examinés ont démontré qu'ils sont conscients des inégalités systémiques possibles et qu'ils sont déterminés à y remédier.

176. Le débat public sur l'application de la biométrie par le gouvernement continuera d'évoluer et d'entraîner des modifications aux cadres juridiques et réglementaires associés aux activités de biométrie. Ainsi, la surveillance continue de l'OSSNR est justifiée, en particulier dans les cas où l'on invoque explicitement la sécurité nationale comme motif pour la collecte et l'utilisation des données biométriques.

Examen sur la communication de renseignements par les institutions fédérales en vertu de la *Loi sur la communication d'information ayant trait à la sécurité du Canada* en 2020

177. En novembre 2021, l'OSSNR et le Commissariat à la protection de la vie privée (CPVP) ont achevé un examen conjoint visant 215 communications émises en 2020 en vertu de *la Loi sur la communication d'information ayant trait à la sécurité du Canada* (LCISC). Il s'agit du premier examen réalisé par l'OSSNR conjointement avec un autre organisme d'examen.

178. La LCISC encourage et facilite la communication d'information au sein du gouvernement fédéral afin d'assurer la protection contre les activités qui minent ou menacent la sécurité nationale, à certaines conditions[37]. La LCISC permet les communications d'information lorsque l'institution fédérale divulgatrice a la conviction que l'information contribuera à l'exercice de la compétence ou de l'attribution de l'institution destinataire à l'égard d'activités portant atteinte à la sécurité du Canada et que l'incidence de la communication sur le droit à la vie privée d'une personne sera limitée à ce qui est raisonnablement nécessaire[38]. Il s'agit du critère de communication.

179. L'examen a permis de constater que 212 des 215 communications (environ 99 %) répondaient aux deux volets du critère de communication. En ce qui concerne les trois communications préoccupantes, elles semblaient spéculatives et leur rapport aux activités minant la sécurité du Canada était nébuleux. Il s'agissait, dans ces trois cas, de communications proactives de la GRC. L'une de celles-ci, qui présente un intérêt particulier, est la communication de l'identité et des données biométriques d'environ 2 900 personnes aux Forces armées canadiennes (FAC). Ainsi, l'OSSNR et le CPVP recommandent que la GRC mette à jour ses politiques et ses pratiques en vue de se conformer au critère de communication, que les institutions qui ont reçu ces communications préoccupantes de la GRC suppriment l'information ou la renvoient à la GRC à moins qu'elles soient en mesure de fournir une raison valable de la conserver[39] et que toute institution qui communique des renseignements personnels liés à un grand nombre de personnes (ou communication en bloc) fasse preuve d'une diligence raisonnable accrue.

180. Les dossiers examinés ont également mis en évidence un cas de communication verbale faite au SCRS des mois avant une communication officielle en vertu de la LCISC et sans une source apparente d'autorisation légale. L'OSSNR et le CPVP ont recommandé que les institutions ayant une expertise en matière de sécurité nationale s'assurent que, lorsqu'elles demandent des renseignements personnels à des fins de sécurité nationale à d'autres institutions fédérales, elles indiquent clairement que leur demande ne constitue pas ou ne confère pas à l'autre institution le pouvoir de communiquer des renseignements personnels.

181. Selon les tendances observées en matière de communication d'information en vertu de la LCISC, l'OSSNR et le CPVP recommandent que le CST et IRCC concluent une entente sur l'échange d'information et qu'AMC et le SCRS mettent à jour leur entente sur l'échange d'information, conformément aux principes de la LCISC[40].

182. Enfin, les politiques du gouvernement du Canada liées à la LCISC ont été passées en revue. L'examen a permis de constater que SP a mis au point un guide sur la LCISC à l'intention des institutions fédérales, a dirigé un groupe de travail interministériel et a fourni une formation à l'ensemble des 17 institutions visées par la LCISC. Il a par ailleurs été conclu que 16 des 17 institutions visées par la LCISC, l'Agence canadienne d'inspection des aliments (ACIA) étant l'exception, possèdent des politiques à l'appui de la conformité à la LCISC. L'OSSNR et le CPVP recommandent à l'ACIA d'élaborer un cadre semblable afin de mettre en œuvre une politique relative à la LCISC.

Réponse aux recommandations de l'OSSNR

183. Les recommandations de l'OSSNR, la réponse formulée par la direction des entités visées par l'examen et d'autres détails de l'examen se trouvent à l'annexe D du présent rapport.

Examen de la mise en œuvre ministérielle de la *Loi visant à éviter la complicité dans les cas de mauvais traitements infligés par des entités étrangères* pour 2020

184. La *Loi visant à éviter la complicité dans les cas de mauvais traitements infligés par des entités étrangères* (la LÉC) et les instructions connexes visent à empêcher que quiconque subisse de mauvais traitements suivant l'échange de renseignements entre un ministère du gouvernement du Canada et une entité étrangère. Au cœur des directives se trouve la prise en compte du risque important et la question de savoir si ce risque, le cas échéant, peut être atténué. Pour ce faire, la LÉC et les directives énoncent une série d'exigences qui doivent être respectées ou mises en œuvre lors du traitement de l'information.

185. L'examen porte sur la mise en œuvre des directives données à 12 ministères et organismes[41] depuis la date où celles-ci leur ont été communiquées (1er janvier 2020) jusqu'à la fin de l'année civile (31 décembre 2020). Cet examen a été mené en vertu du paragraphe 8(2.2) de la Loi sur l'OSSNR, qui exige que l'OSSNR examine, chaque année civile, la mise en œuvre de toutes les directives données en vertu de la LÉC.

186. Il s'agit du premier examen relatif à la LÉC portant sur une année civile complète. Bon nombre des ministères visés par l'examen ont soulevé que la pandémie de COVID-19 a eu une incidence sur leurs activités relatives à l'échange de renseignements, notamment sur le nombre de cas nécessitant un examen approfondi en vertu de la LÉC. En effet, l'OSSNR a constaté qu'aucun cas visé par la LÉC n'a été transmis aux administrateurs généraux entre le 1er janvier et le 31 décembre 2020, tous ministères confondus.

187. Si l'OSSNR était satisfait des efforts considérables déployés par de nombreux ministères pour élaborer leurs premiers cadres stratégiques relatifs à la LÉC, il a constaté que l'ASFC et SP n'avaient pas encore achevé les leurs selon les directives reçues en vertu de la LÉC au cours de la période visée par l'examen.

188. Les mesures d'atténuation mises en place par les ministères ont également été examinées dans le cadre du présent examen étant donné qu'elles constituent un volet fondamental du processus d'échange de renseignements des ministères..

189. L'OSSNR estime qu'il est maintenant en mesure de mener des évaluations approfondies des études de cas liées à la conformité de chacun des ministères à la LÉC et aux instructions connexes, que les ministères aient ou non transmis des cas à leur administrateur général. Enfin, la mise en œuvre des recommandations antérieures de l'OSSNR sera vérifiée dans le cadre d'examens ultérieurs.

Examens prévus ou en cours

190. À l'avenir, l'OSSNR prévoit de tirer parti de son mandat « d'examiner toute activité menée par un ministère qui a trait à la sécurité nationale ou au renseignement »[42] en menant davantage d'examens multiministériels et en évitant les examens cloisonnés. Outre ses examens annuels relatifs à la LCISC et à la *Loi visant à éviter la complicité dans les cas de mauvais traitements infligés par des entités étrangères* prévus dans le cadre de son mandat, l'OSSNR compte travailler à deux autres examens visant de nombreux ministères. Le premier porte sur la manière dont le SCRS et la GRC gèrent les menaces posées par l'extrémisme violent à caractère idéologique. Le second se penchera sur la relation qu'entretiennent le CST et le SCRS dans le contexte de leurs activités opérationnelles.

2.5 Rôle de la technologie dans les examens

Intégration de la technologie aux examens

191. On associe habituellement la technologie de l'information, ou TI, aux systèmes et aux logiciels fournissant un appui administratif aux organisations. Or, les TI jouent un rôle de plus en plus important dans les activités opérationnelles liées à la sécurité nationale du Canada et à la communauté du renseignement. La communauté canadienne de la sécurité et du renseignement tire profit de l'essor fulgurant des technologies de pointe en les rendant opérationnelles, et ce, comme jamais auparavant. Aujourd'hui, non seulement les organismes œuvrant à la sécurité nationale et au renseignement peuvent utiliser les nouvelles technologies à l'appui de leurs mandats, mais ils doivent le faire, pour demeurer à l'affût des occasions tout comme des menaces émergentes.

192. De telles avancées se produisent rapidement. Elles sont complexes et souvent propres à chaque institution. En outre, bien que les technologies émergentes soient mises au point dans un but précis, elles entraînent souvent des répercussions imprévues sur les libertés civiles et le respect de la vie privée, en particulier lorsqu'on les utilise dans le contexte du renseignement et de la sécurité. Ainsi, il est crucial qu'une entité de surveillance telle que l'OSSNR assure le suivi de l'utilisation de ces nouvelles technologies au sein de la communauté canadienne de la sécurité nationale et du renseignement pour veiller à ce que les organisations visées par son mandat de surveillance s'acquittent de leurs mandats de manière légale, raisonnable et appropriée.

193. La Direction de la technologie de l'OSSNR vise à améliorer la portée de son examen en se penchant davantage sur l'utilisation et la mise en œuvre des technologies par les organismes responsables de la sécurité et du renseignement au Canada. En élargissant son champ d'examen pour y inclure les applications pratiques des technologies et en confiant cette nouvelle sphère d'intérêt à une équipe interne d'ingénieurs, d'informaticiens et d'examinateurs chevronnés, l'OSSNR sera en mesure de garantir que les ministères et organismes sont tenus responsables de leurs décisions relatives aux divers volets des technologies émergentes.

194. Le développement d'une telle capacité à l'OSSNR fournira également une occasion unique de créer un modèle d'examen qui mettra l'organisme de surveillance sur un pied d'égalité avec le Groupe des cinq et l'appareil international d'examen. Une telle expertise à l'interne est essentielle pour permettre à l'OSSNR d'examiner les risques et les questions d'ordre juridique et liés à la conformité émergeant dans le contexte de la sécurité nationale. Sans celle-ci, l'OSSNR ne pourra conserver sa pertinence.

195. Dans cette optique, la Direction de la technologie de l'OSSNR :

- Dirigera l'examen sur les systèmes de TI et les dernières avancées technologiques;
- Mènera des enquêtes techniques indépendantes;
- Appuiera les membres de l'OSSNR affectés aux enquêtes sur les plaintes contre le SCRS, le CST ou la GRC lorsque l'examen des preuves requiert une expertise technologique;
- Produira des rapports pour vulgariser des sujets techniques sophistiqués;
- Évaluera le risque posé par les entités examinées sur le plan de la conformité aux TI en lien avec les lois et les politiques applicables;
- Recommandera des mesures de protection concernant les systèmes de TI et les données pour minimiser le risque de non-conformité sur le plan juridique;
- Fera en sorte que les thèmes liés à la technologie soient intégrés dans les plans d'examens annuels de l'OSSNR;
- Tirera parti d'une expertise externe afin de mieux comprendre et évaluer les risques touchant les TI.

Avenir de la technologie dans les examens

196. L'OSSNR continuera d'accroître son nombre d'employés travaillant au sein de la Direction de la technologie étant donné que celle-ci joue un rôle de plus en plus actif et important. Par ailleurs, l'OSSNR mènera les premiers examens axés sur la technologie visant le cycle de vie de l'information recueillie par des moyens technologiques en vertu d'un mandat de la Cour fédérale en 2022. L'année suivante, il prévoit examiner les pratiques du CST en matière de conservation des données SIGINT.

197. En ce qui a trait aux considérations importantes liées aux examens en cours, la Direction de la technologie de l'OSSNR a déterminé trois thèmes concernant la technologie à aborder en priorité :

- Technologies à double usage;
- Entreposage de données, quantités massives de données et analyses de données;
- Décisions automatisées.

198. Tandis que la communauté canadienne de la sécurité et du renseignement continue d'étendre sa capacité technique de collecte et d'analyse, l'OSSNR doit poursuivre en parallèle le perfectionnement de son expertise en matière d'examen. Au cours de la prochaine année, afin que ses approches tiennent compte des enjeux de technologie clés,

l'OSSNR compte établir des partenariats au pays et à l'étranger et compte nouer des relations de travail avec le milieu universitaire, la société civile et des leaders commerciaux. La Direction de la technologie de l'OSSNR appuiera aussi l'équipe d'enquête sur les plaintes de l'OSSNR afin de comprendre où et quand les avancées technologiques pourraient être mises en application dans le cadre des enquêtes de l'OSSNR.

2.6 Politiques et processus employés dans les examens

Méthode pour évaluer la rapidité des réponses

Lignes directrices pour évaluer la rapidité des réponses dans le cadre des examens

199. Pour favoriser la responsabilisation et la prévisibilité, l'OSSNR aura recours aux lignes directrices suivantes afin d'évaluer le délai de réponse des entités visées par un examen lorsque des demandes de renseignements leur sont présentées et commentera les résultats de manière confidentielle et publique. L'OSSNR examinera notamment la rapidité des réponses dans chacun de ses rapports annuels. Les lignes directrices en question établissent des attentes claires et normalisées sur ce volet important du processus d'examen.

Délais standard pour les demandes de renseignements

200. Une grande partie de l'information demandée par l'OSSNR s'inscrit dans l'une des deux catégories suivantes : les documents « prêt à l'emploi » et les documents nécessitant un travail supplémentaire de compilation. Parmi les documents « prêts à l'emploi », on trouve des politiques, des directives ministérielles, des politiques opérationnelles, des avis juridiques et des procédures opérationnelles normalisées. Quant aux documents nécessitant un travail supplémentaire de compilation, ils requièrent des manipulations de données ou des explications ou alors ils se trouvent dans les bases de données spécialisées ou dans les courriels. Le type de documents requis et les délais de réponse à respecter sont précisés dans les demandes de renseignements (15 jours pour le premier type de document, 30 jours pour le second).

Délais non standard pour les demandes de renseignements

201. L'OSSNR peut accorder un délai prolongé pour donner suite aux demandes de renseignements lorsqu'il le juge nécessaire. Voici certaines raisons pouvant justifier la décision de prolonger le délai : l'examen porte sur de la nouvelle matière, une importante quantité d'information ou de documents a été demandée ou l'entité en question fait l'objet

d'autres examens au même moment où elle doit respecter d'autres considérations opérationnelles. L'OSSNR attribuera des échéanciers non normalisés à sa discrétion et selon le jugement de l'équipe responsable de l'examen.

202. L'OSSNR reconnaît que des facteurs extraordinaires et des circonstances atténuantes peuvent avoir une incidence sur le délai de réponse aux demandes de renseignements et de documentation. Dans de telles situations, les entités qui font l'objet d'un examen peuvent proposer une échéance autre que celle attribuée initialement, accompagnée d'une justification substantielle. Elles doivent, si possible, le faire dès qu'elles reçoivent la demande et en prennent connaissance. C'est à l'équipe d'examen de l'OSSNR que reviendra la décision d'accorder ou non une extension. D'autres dispositions peuvent être envisagées telles que fournir l'information demandée en tranches. Toutes les demandes de renseignements seront tout de même accompagnées d'un délai pour la réponse. Celui-ci servira à déterminer si des mesures correctives s'imposeront.

Mesures correctives

203. L'OSSNR mettra en œuvre une approche à trois étapes pour mobiliser les entités examinées lorsque celles-ci ne donnent pas suite à une demande de renseignements dans le respect du délai accordé. Si l'échéance est passée et qu'aucune réponse satisfaisante n'a été fournie, l'OSSNR fera part de ses préoccupations aux échelons supérieurs de manière progressive. Une série de lettres sera envoyée au sous-ministre adjoint, au sous-ministre puis, en dernier recours, au ministre.

204. Les lettres seront jointes en annexe au rapport associé et orienteront l'évaluation globale de la rapidité d'exécution des entités examinées dans le cadre du rapport public annuel de l'OSSNR. Les lignes directrices ci-dessus seront également passées en revue chaque année et pourraient être révisées au fur et à mesure qu'elles sont mises en œuvre pour veiller à ce qu'elles remplissent leurs objectifs.

Mise en œuvre des recommandations

205. De manière générale, l'OSSNR formule ses recommandations à la lumière des principales conclusions découlant de son travail d'examen. Dans la plupart des examens réalisés depuis sa création, l'OSSNR a émis des recommandations aux ministères et aux organismes examinés. En réponse à celles-ci, les entités visées ont donné suite à ces recommandations, notamment en présentant un plan de mise en œuvre des recommandations en question. Étant donné qu'un peu plus de deux ans se sont écoulés depuis que l'OSSNR a présenté les recommandations contnus dans ses premiers examens, il estime que le temps est venu de

constater les résultats découlant de leur application dans les activités et les politiques des entités examinées. Ainsi, l'OSSNR envisagera des moyens appropriés d'assurer le suivi et l'évaluation de la mise en œuvre des recommandations formulées dans le cadre d'examens antérieurs.

206. L'OSSNR discutera avec les ministères et les organismes ayant fait l'objet d'un examen afin de déterminer la marche à suivre pour évaluer la mise en œuvre des recommandations antérieures. Par exemple, si certains problèmes ou difficultés ont été ignorés, l'OSSNR pourrait amorcer des examens de suivi. Le rapport annuel public de l'OSSNR pourrait aussi soulever des questions relatives à la mise en œuvre des recommandations au besoin.

Vérification

207. Comme susmentionné, la vérification est une composante fondamentale de tout travail d'examen indépendant, crédible et professionnel. Dans le cadre de chacun de ses examens, l'OSSNR doit être en mesure de vérifier que l'information reçue est complète et exacte. Il s'agit d'une condition essentielle afin que l'OSSNR puisse garantir à ses intervenants qu'il peut se fier à l'information obtenue dans le cadre de ses examens pour formuler ses conclusions.

208. Dans le cadre de ses examens, l'OSSNR a le droit d'obtenir toute information jugée pertinente, à l'exception des documents confidentiels du Cabinet. L'OSSNR ne pourrait s'acquitter de son mandat sans ce volet clé de la Loi sur l'OSSNR. Les ministères et les organismes visés par un examen doivent, à cette fin, faire en sorte que l'OSSNR puisse garantir au Parlement et aux Canadiens qu'il accorde une grande confiance à l'information reçue. À cet égard, il est attendu que les ministères et les organismes visés par un examen appuient les processus qui satisfont l'exigence selon laquelle l'OSSNR doit vérifier, de manière indépendante, que l'information fournie est complète et exacte. Par exemple, les ministères et les organismes visés par un examen doivent :

- fournir à l'OSSNR, pour chaque examen, un index des documents transmis et préciser si de l'information a été modifiée ou retirée et à quelle fin;
- inclure un compte rendu décrivant comment les recherches d'information ont été menées et mentionner les termes utilisés dans les recherches ainsi que les bases de données interrogées.

209. Les entités examinées doivent toujours s'attendre à ce que les examens comportent une part de vérification. Afin de respecter son engagement concernant la transparence et la rigueur méthodologique, les examens de l'OSSNR contiennent désormais un énoncé sur le niveau de confiance. Cet énoncé reflète la capacité de l'OSSNR de vérifier l'information

requise dans le cadre de ses examens. L'énoncé sur le niveau de confiance fournit également un contexte supplémentaire important à l'examen, en indiquant aux lecteurs dans quelle mesure l'OSSNR a été en mesure de vérifier les renseignements nécessaires ou pertinents pendant l'examen, et si cet exercice a eu une incidence sur la confiance portée à l'entité examinée.

03 //

Enquêtes sur les plaintes

3.1 Aperçu

210. Au cours de l'année, l'OSSNR a continué de s'adapter dans le cadre de ses enquêtes en adoptant des approches novatrices. Celles-ci comprennent l'utilisation de la technologie de vidéoconférence pour mener ses audiences et ses entrevues d'enquête ainsi que la tenue de certaines enquêtes par écrit pour maximiser l'efficacité sur le plan procédural. L'OSSNR a accusé des retards dans ses enquêtes, en partie à cause des défis occasionnés par la pandémie de COVID-19. En effet, L'OSSNR a connu des retards dans ses enquêtes en raison de sa capacité réduite d'accéder à l'information et aux éléments probants en raison des délais de réponse accrus. L'annexe E contient les statistiques des enquêtes sur les plaintes de l'OSSNR en 2021.

211. Pour l'OSSNR comme pour les entités du gouvernement fédéral obligées de lui fournir de l'information, la progression des enquêtes et l'obtention des éléments probants ont posé des défis. Dans plusieurs affaires en cours, l'OSSNR a accordé des reports et des extensions en ce qui concerne les étapes procédurales, notamment le dépôt des soumissions et des documents probants. Outre les retards liés à la pandémie, l'OSSNR constate que les entités du gouvernement fédéral visées par une enquête ont invoqué d'autres raisons pour justifier le report de leur échéance pour la soumission de documents, notamment des problèmes liés à la disponibilité des témoins et une pénurie de ressources. Par ailleurs, l'OSSNR a dû prendre des mesures pour obtenir de l'information supplémentaire du gouvernement suivant la réception de communications incomplètes relativement à plus d'une de ses enquêtes, ce qui a occasionné d'autres retards.

212. En ce qui a trait au volume de cas en 2021, l'OSSNR a géré une hausse substantielle et continue de son inventaire des cas, en raison de 58 plaintes que lui a renvoyées la Commission canadienne des droits de la personne, en vertu du paragraphe 45(2) de la *Loi canadienne sur les droits de la personne*, aux fins d'enquête, en avril 2021. Ce fort volume de cas a eu une incidence sur la gestion globale des cas de l'OSSNR.

213. L'OSSNR s'est aussi affairé à améliorer sa prestation de programme en travaillant à des stratégies de collecte, d'analyse et d'utilisation de données démographiques et fondées sur la race dans le contexte du processus d'enquête sur les plaintes. L'OSSNR a collaboré

étroitement avec son partenaire, la Commission civile d'examen et de traitement des plaintes relatives à la GRC afin d'élaborer des stratégies d'intérêt commun et d'améliorer les procédures dans l'optique des considérations concernant la diversité et l'inclusion. Les objectifs précis d'une telle initiative consistent à améliorer l'accès à la justice en favorisant la compréhension du processus d'enquête. Celle-ci vise aussi à répertorier les divers groupes raciaux desquels émanent ces plaintes civiles pour déterminer :

- si des écarts considérables existent sur le plan racial;
- si les types de plaintes portées contre des membres de l'organisme de sécurité nationale varient selon les groupes raciaux;
- la fréquence des plaintes qui comprennent des allégations de préjugés fondées sur la race ou d'autres formes de préjugés;
- si les résultats de l'enquête sur les plaintes varient selon le groupe racial.

214. Au cours de l'année à venir, l'OSSNR entamera une analyse des données procédurales concernant la rapidité de ses enquêtes afin d'orienter la mise en place de nouvelles normes de service, ce qui s'inscrit dans ses efforts pour assurer l'efficacité et la transparence de son processus. L'OSSNR est conscient du fait que les normes de service sont basées sur des échéances réalistes en temps normal. Puisque la situation sanitaire concernant la pandémie de COVID-19 continue de s'améliorer, l'OSSNR s'attend à ce que les entités du gouvernement coopèrent en répondant plus promptement aux demandes afin de faire progresser les enquêtes. À la lumière de ses objectifs visant à élaborer des normes de service, l'OSSNR adoptera une approche mesurée relativement aux demandes de report et d'extension des échéances, lesquelles seront permises en cas de circonstances exceptionnelles. De plus, au cours de l'année à venir, l'OSSNR continuera de travailler à améliorer son site Internet de manière à favoriser l'accessibilité aux processus d'enquête sur les plaintes et la pertinence de ceux-ci.

3.2 État d'avancement de la réforme du processus d'enquête sur les plaintes

215. En 2021, l'OSSNR a terminé sa réforme du processus d'enquête sur les plaintes après une consultation complexe avec de nombreux intervenants. En juillet 2021, il a mis en œuvre le processus, qui comprend un nouvel ensemble de règles de procédure visant à offrir une accessibilité et une efficacité améliorées en ce qui a trait à son mandat d'enquête. L'OSSNR constate que les enquêtes menées dans le cadre de ce nouveau modèle dévoilent, déjà à

ce stade précoce, des signes d'efficacité. En effet, les dates des entrevues d'enquête ont pu être fixées en temps plus opportun.

3.3 Enquêtes

Résumé du rapport définitif

Enquête concernant les allégations contre le Service canadien du renseignement de sécurité (1500-516)

Contexte

216. Le plaignant a déposé une plainte contre le SCRS concernant divers incidents avec les autorités aéroportuaires alors qu'il voyageait.

217. En outre, le plaignant accuse le SCRS de harcèlement, d'une possible entrave à ses occasions d'emploi, d'une entrave à une demande de passeport, d'avoir intercepté et examiné son courrier ainsi que d'avoir perturbé ses relations personnelles.

Enquête

218. Lors de l'enquête, le plaignant a soulevé plusieurs incidents distincts qui l'ont mené à déposer sa plainte. L'OSSNR a examiné les éléments probants afin de déterminer si le SCRS avait agi de manière raisonnable et appropriée dans les circonstances, s'il y avait eu ou non du harcèlement et si les agissements du SCRS étaient conformes à la loi.

219. L'OSSNR s'est penché sur les preuves fournies par des témoins, la documentation des parties ainsi que d'autre matériel pertinent transmis au cours de l'enquête. L'OSSNR a aussi écouté le témoignage du plaignant.

220. En ce qui concerne un incident en particulier en lien avec les agissements des autorités aéroportuaires, l'OSSNR a tenu compte des preuves fournies par des témoins concernant l'article 8 de la *Charte canadienne des droits et libertés* (la Charte). L'article 8 prévoit que chacun a droit à la protection contre les fouilles et les saisies abusives.

Conclusion

221. En ce qui concerne l'ensemble des allégations, l'OSSNR a déterminé que la plainte était infondée. Toutefois, pour ce qui est de la participation du SCRS à une fouille menée par

l'ASFC du téléphone cellulaire du plaignant à un aéroport, à une occasion, l'OSSNR a conclu que le SCRS avait enfreint l'article 8 de la Charte.

222. L'OSSNR a cependant déterminé que le SCRS n'a pas pris à la légère les intérêts du plaignant relativement à sa vie privée et n'a pas délibérément omis de tenir compte de ceux-ci lors de la fouille. Le non-respect de l'article 8 ne constitue pas un manquement grave. Il s'agissait plutôt d'une erreur de jugement.

Réouverture de l'enquête sur les allégations contre le Service canadien du renseignement de sécurité (1500-471)

Contexte

223. L'OSSNR a produit un rapport définitif supplémentaire à la suite de la réouverture d'une enquête menée par son prédécesseur, le Comité de surveillance des activités de renseignement de sécurité (CSARS).

224. Le plaignant accuse le SCRS d'avoir violé ses droits constitutionnels en ce qui concerne sa race et sa religion ainsi que son refus de travailler en tant que source humaine. Il a par ailleurs soutenu que des agents du SCRS l'ont harcelé en l'interceptant dans les aéroports et en le suivant dans ses déplacements. Enfin, le plaignant affirme que le SCRS a communiqué de faux renseignements à une entité étrangère, qui ont mené à sa détention pendant 8 heures dans l'aéroport d'un pays étranger, sans nourriture.

225. Dans son rapport définitif, le CSARS avait conclu que les allégations du plaignant concernant la discrimination et le harcèlement étaient infondées. Le CSARS avait aussi conclu que les agissements des représentants du SCRS allaient à l'encontre de l'article 12 de la Loi sur le SCRS, des directives ministérielles, des politiques et des procédures opérationnelles et que le plaignant avait souffert des conséquences de tels agissements.

226. L'enquête rouverte par l'OSSNR se limitait strictement à deux questions d'ordre juridique, à savoir : 1) si le critère concernant les motifs raisonnables de soupçonner aux termes de l'article 12 de la Loi sur le SCRS doit être rempli pour que le Service mène de premières recherches dans ses fonds de renseignements opérationnels; 2) si le Service aurait dû obtenir une autorisation de ciblage individuel contre le plaignant.

Enquête

227. Il a été décidé que l'enquête devait être rouverte par l'OSSNR en vertu du paragraphe 11(1) de la *Loi sur la sécurité nationale*. L'OSSNR a examiné les documents présentés par les

parties, y compris les soumissions et les documents classifiés déposés par le SCRS. Par ailleurs, il a examiné les soumissions du plaignant ainsi que tout autre matériel pertinent auquel il a eu accès dans le cadre de la réouverture de l'enquête.

228. Pour ce qui est de savoir si le critère concernant les motifs raisonnables de soupçonner aux termes de l'article 12 de la Loi sur le SCRS doit être rempli lorsque le Service mène de premières recherches dans ses fonds de renseignements opérationnels, le SCRS a admis au cours de l'enquête qu'il devait en effet avoir des motifs raisonnables de soupçonner que des activités constituent une menace à la sécurité du Canada pour mener de telles recherches dans ses fonds de renseignements comme décrit dans l'article 2 de la Loi sur le SCRS.

229. À la lumière des faits de cette affaire, l'OSSNR a déterminé que le CSARS avait conclu à juste titre que le SCRS ne disposait pas de faits objectifs au sujet d'activités qui satisfaisaient le critère des motifs raisonnables de soupçonner.

230. Pour ce qui est de savoir si le SCRS était tenu d'obtenir une autorisation de ciblage individuel contre le plaignant, l'OSSNR a déterminé que les conclusions du CSARS concernant la portée et la façon dont le SCRS a enquêté sur le plaignant ne seraient pas réexaminées par l'OSSNR. L'OSSNR a déterminé que la conclusion du CSARS selon laquelle il y a un moment dans l'enquête du SCRS où les agents du SCRS enquêtaient spécifiquement sur les activités du plaignant était sans équivoque et, par conséquent, il était clair que le SCRS aurait dû obtenir une autoriation de ciblage individuel contre lui, pourtant il ne l'a pas fait.

Conclusion

231. L'OSSNR confirme les constats formulés par le CSARS dans son rapport.

04 //

Conclusion

232. En 2021, l'OSSNR a continué à remplir son mandat en réalisant plusieurs examens sur un grand nombre de ministères et d'organismes fédéraux engagés dans des activités liées à la sécurité nationale et au renseignement. De même, malgré les défis inhérents à la pandémie de COVID-19 sur les procédures d'enquêtes sur les plaintes ainsi qu'une forte augmentation de sa charge de travail, l'OSSNR a adapté ses méthodes et a poursuivi ses efforts visant à améliorer l'exécution de ses programmes.

233. Au fur et à mesure de sa croissance, l'OSSNR vise à accroître sa capacité à examiner la technologie et son utilisation pratique dans les activités en matière de sécurité nationale et de renseignement. La croissance continue de l'effectif de l'Office permettra également à l'organisation d'examiner une plus grande variété d'activités liées à la sécurité nationale et au renseignement et de continuer à progresser dans ses enquêtes sur un grand nombre de plaintes.

234. L'OSSNR demeure engagé à collaborer avec les intervenants non gouvernementaux. L'OSSNR a pris note des commentaires sur son précédent rapport annuel et continuera à s'efforcer d'en améliorer l'utilité.

235. Encore une fois, les membres de l'OSSNR sont très reconnaissants de l'excellent travail accompli par le personnel du Secrétariat et du dévouement dont il fait preuve à l'égard de la mission de l'organisation, qui consiste à promouvoir une plus grande responsabilité au sein de la communauté canadienne de la sécurité nationale et du renseignement.

05 //

Annexes

Annexe A : Abréviations

Abréviation	Nom complet
AI	Avocat indépendant
AMC	Affaires mondiales Canada
ASFC	Agence des services frontaliers du Canada
BCP	Bureau du Conseil privé
CANAFE	Centre d'analyse des opérations et déclarations financières du Canada
CI	Contre-ingérence
COA	Cyberopération active
COD	Cyberopération défensive
CPSNR	Comité de parlementaires sur la sécurité nationale et le renseignement
CPVP	Commissariat à la protection de la vie privée du Canada
CSARS	Comité de surveillance des activités de renseignement de sécurité
CST	Centre de la sécurité des télécommunications
ÉFVP	Évaluation des facteurs relatifs à la vie privée
ERD	Entreprise du renseignement de défense
FAC	Forces armées canadiennes
GLCSN	Groupe litiges et conseils en sécurité nationale (ministère de la Justice)
GRC	Gendarmerie royale du Canada
GSN	Groupe sur la sécurité nationale (ministère de la Justice)
HUMINT	Renseignement humain

IRCC	Immigration, Réfugiés et Citoyenneté Canada
IRCPC	Information qui se rapporte à un Canadien ou à une personne se trouvant au Canada
LÉC	*Loi visant à éviter la complicité dans les cas de mauvais traitements infligés par des entités étrangères*
LCISC	*Loi sur la communication d'information ayant trait à la sécurité du Canada*
MDN	Ministère de la Défense nationale
MRM	Mesure de réduction de la menace
OSSNR	Office de surveillance des activités en matière de sécurité nationale et de renseignement
RCI	Renseignements canadiens d'identification
RO	Recherche opérationnelle (GRC)
SCRS	Service canadien du renseignement de sécurité
SIGINT	Renseignement d'origine électromagnétique
SP	Sécurité publique Canada
SSD	Sous-section des déposants (SCRS)
TC	Transports Canada
UNCIFC	Unité nationale de contre-ingérence des Forces canadiennes

Annexe B : Aperçu administratif et financier

Aperçu financier

1. L'OSSNR est organisé selon trois principaux secteurs d'activité : les services juridiques, les examens et les services internes. Le tableau ci-dessous présente une comparaison des dépenses effectuées en 2020 et en 2021 pour chacun des trois secteurs d'activité susmentionnés.

Dépenses par secteur d'activité (2020 et 2021)

(en dollars)	Dépenses (2020)	Dépenses (2021)
Services juridiques et enquêtes sur les plaintes	1 859 924	3 051 611
Examens	3 094 323	4 471 941
Services internes	4 625 860	8 926 178
Total	**9 580 107**	**16 449 730**

2. Au cours de l'année civile 2021, les dépenses de l'OSSNR se sont élevées à 16,4 millions de dollars, ce qui représente une augmentation de 6,8 millions de dollars (72 %) par rapport à 2020. Cette augmentation des dépenses est principalement attribuable à la croissance de l'effectif de l'OSSNR, à l'aménagement d'installations sécurisées pour accueillir les employés et à des investissements dans les infrastructures de gestion de l'information et de technologie de l'information, notamment afin de permettre l'accès aux réseaux classifiés, aux vidéoconférences sécurisées ainsi qu'à l'équipement permettant au personnel de l'OSSNR de travailler à distance.

Dotation

3. Au cours de l'année, le personnel de l'OSSNR est passé de 58 à 73, soit une augmentation nette de 15 employés. L'incidence des mesures de confinement liées à la pandémie sur les activités de filtrage de sécurité, combinée à un marché du travail plus concurrentiel et à la nécessité, du moins en partie, pour les employés de l'OSSNR de travailler à partir d'un site sécurisé, a entraîné des retards dans la dotation, une augmentation de l'attrition et un nombre net global d'employés inférieur par rapport à l'année précédente.

4. Bien que l'OSSNR continue d'utiliser des stratégies, des procédures et des pratiques de dotation modernes et flexibles, elle travaille également avec les employés pour mettre en œuvre un modèle de travail post-pandémie hybride et flexible afin d'attirer et de retenir les talents et de concurrencer les autres employeurs fédéraux offrant aux employés la possibilité de travailler à domicile.

5. En 2021, l'OSSNR a entrepris la première étape de la mise en œuvre d'un programme personnalisé d'intégration des employés, notamment la mise en place de feuilles de route pour la formation. En fonction des commentaires des employés, l'OSSNR fera, en 2022, de nouveaux investissements pour définir les exigences en matière de compétences de base des postes et continuera à renforcer, documenter et perfectionner les méthodologies et les pratiques d'examen dans le but de soutenir l'intégration efficace des employés. Ces activités sont essentielles pour attirer et retenir les talents dans un marché du travail concurrentiel.

Pandémie

6. Comme indiqué tout au long du présent rapport, la pandémie a continué à avoir des conséquences importantes sur les opérations et les activités de l'OSSNR en 2021. La priorité absolue du Secrétariat de l'OSSNR était la sécurité de ses employés et, par conséquent, il a réagi rapidement aux mesures de confinement, en communiquant les protocoles de travail relatifs à la COVID-19 et en mettant en œuvre sa propre politique en matière de vaccination à la suite de l'appel du gouvernement du Canada concernant la vaccination obligatoire de ses employés de la fonction publique.

7. En 2021, l'OSSNR a reconnu qu'une approche moderne et flexible au travail était nécessaire pour mener à bien les activités de son mandat pendant la pandémie. L'OSSNR a élaboré un guide évolutif sur la COVID-19 que les employés et les gestionnaires peuvent consulter pour obtenir des renseignements à jour sur la COVID-19 et les modalités de travail flexibles.

8. L'OSSNR a continué de mettre l'accent sur l'augmentation des communications numériques et des contacts virtuels avec le personnel par la publication régulière de bulletins, des mises à jour sur la pandémie, l'organisation de rencontres virtuelles et la promotion des programmes d'aide aux employés.

Cyberincident

9. Comme mentionné dans le rapport de l'année dernière, en mars 2021, l'OSSNR a été victime d'un cyberincident sur le réseau qu'il utilise pour héberger des renseignements non classifiés et jusqu'à Protégé B seulement. Ce réseau n'était pas utilisé pour stocker des renseignements de niveau SECRET ou TRÈS SECRET.

10. Grâce à l'aide de ses partenaires fédéraux et, en particulier, aux efforts du Bureau du Conseil privé (BCP), du Centre canadien pour la cybersécurité et de Services partagés Canada, l'OSSNR a pu régler le problème et reprendre rapidement ses activités normales. Toutefois, cet incident a accentué les retards existants dans le travail de l'OSSNR causés par la pandémie.

11. L'OSSNR a travaillé en collaboration avec le Commissariat à la protection de la vie privée du Canada (CPVP) et le Secrétariat du Conseil du Trésor du Canada afin de régler un cas de violation de la vie privée ayant découlé du cyberincident. L'OSSNR a informé ses partenaires, a avisé le public par l'intermédiaire de son site Web et de ses comptes de médias sociaux et a publié des avis directs conformément aux exigences et aux recommandations du CPVP. L'OSSNR a pour principales priorités d'assurer la protection de la vie privée des Canadiens et de protéger l'information en sa possession.

Initiatives fondamentales

12. Fort d'avoir nommé un champion et établi un Comité pour prendre des mesures contre les problèmes systémiques d'équité en matière d'emploi, de diversité et d'inclusion en 2020, l'OSSNR a continué de travailler fort pour créer une culture d'inclusion en tenant des discussions avec le personnel sur la lutte contre le racisme et les thèmes liés à la diversité. En réponse à l'appel à l'action du greffier du Conseil privé[43], l'Office a réalisé une évaluation de la maturité de ses politiques, de ses programmes et de ses pratiques en matière de droits de la personne, d'accessibilité, d'équité en matière d'emploi, de diversité et d'inclusion. L'OSSNR a également élaboré un plan d'action triennal pour orienter ses efforts.

13. L'OSSNR prend également des mesures pour analyser les données sur les plaintes des années précédentes afin d'examiner les tendances démographiques, y compris la race. À cet égard, il travaille conjointement avec un autre organisme d'examen pour tirer parti de l'expertise universitaire pertinente afin d'aider l'OSSNR à recueillir le bon type de données dans le cadre d'enquêtes futures sur les plaintes dans le but de faciliter cette analyse. L'objectif est de mieux comprendre les collectivités les plus touchées par les activités de

sécurité nationale, ce qui peut aider l'OSSNR à orienter ses priorités en matière de sensibilisation et de mobilisation.

14. Compte tenu de la croissance actuelle et prévue des effectifs et des exigences en matière de distanciation physique en vigueur durant la pandémie, il est crucial d'avoir accès à des locaux sécurisés pour effectuer des travaux de nature classifiée pour que l'organisation connaisse du succès. En 2021, l'OSSNR a été en mesure d'accroître sa présence en ouvrant un lieu de travail temporaire. Parallèlement, les plans pour un lieu permanent ont également été achevés et la construction de locaux à bureaux sécurisés supplémentaires a commencé en avril 2022.

15. L'OSSNR a terminé la mise en œuvre d'une stratégie de services ministériels en officialisant les ententes de service avec le Bureau du Conseil privé et Services publics et Approvisionnement Canada en ce qui concerne les services de réseautage des TI, les activités de filtrage de sécurité ainsi que le soutien aux services de finances et de rémunération.

16. En 2021, l'OSSNR s'est concentrée sur l'évaluation des lacunes dans ses pratiques de sécurité et de gestion de l'information. La réalisation d'une évaluation de la gouvernance et des contrôles de sécurité de l'organisation a conduit à l'approbation et à la mise en œuvre des recommandations du plan de sécurité de l'Office en septembre 2021.

17. L'OSSNR a également publié une politique sur la gestion de l'information pour veiller à ce que les rôles, les responsabilités et les attentes en matière de gestion de l'information soient définis, communiqués, compris et respectés dans l'ensemble de l'organisation. Puisque l'information et sa gestion sont essentielles à la réalisation du mandat de l'OSSNR, un nouveau plan de classification a été élaboré, des plans de conservation de l'information ont été établis et des stratégies de destruction, de stockage, de numérisation, de transport et de transfert de l'information ont été mises en place.

18. L'OSSNR l'organisation continue de promouvoir la transparence en consacrant des ressources au caviardage, à la déclassification et à la publication des rapports précédents du CSARS, en plus de la publication proactive de ses propres examens. Au cours de 2021, l'OSSNR a effectué une évaluation des facteurs relatifs à la vie privée (ÉFVP) pour la plupart de ses activités de programme et procède actuellement à la mise en œuvre de recommandations visant à assurer la protection de la vie privée tout en communiquant de manière transparente et ouverte.

Annexe C : Retour sur les examens de 2021

La présente annexe dresse une liste succincte des examens que l'OSSNR a achevés, lancés ou menés en 2021. Dans le tableau ci-dessous, la « date de début » renvoie au mois où l'OSSNR a envoyé une lettre de notification pour un examen donné tandis que la « date d'achèvement » renvoie au mois où le rapport définitif d'un examen a été approuvé par les membres de l'OSSNR.[44]

Examens achevés en 2021

Nom de l'examen	Date de début	Date d'achèvement
Examens sur le Service canadien du renseignement de sécurité (SCRS)		
Rétablir la confiance : Réforme des processus de prestation de conseils juridiques du ministère de la Justice et d'obtention de mandats du SCRS	Juin 2020	Janvier 2022
Examen des activités de réduction de la menace du SCRS : Accent sur la communication de renseignements à des parties externes	Février 2021	Décembre 2021
Étude sur les capacités techniques du SCRS	Septembre 2020	Octobre 2021
Examens sur le Centre de la sécurité des télécommunications (CST)		
Examen sur la gouvernance des cyberopérations actives et défensives	Août 2020	Octobre 2021
Examen sur l'échange de renseignements dans tous les volets du mandat du CST	Janvier 2020	Septembre 2021
Ministère de la Défense nationale et Forces armées canadiennes		
Étude de l'entreprise du renseignement de défense du ministère de la Défense nationale et des Forces armées canadiennes	Juin 2021	Octobre 2021
Examen de l'Unité nationale de contre-ingérence des Forces canadiennes — Collecte opérationnelle et pratiques en matière de protection des renseignements personnels	Avril 2021	Décembre 2021
Examens interministériels		
Examen de l'utilisation de la biométrie par le gouvernement du Canada dans le continuum frontalier	Juillet 2020	Décembre 2021

Examen sur la communication de renseignements par les institutions fédérales en vertu de la *Loi sur la communication d'information ayant trait à la sécurité du Canada* en 2020	Mai 2021	Novembre 2021
Examen sur la mise en œuvre par les ministères de la *Loi visant à éviter la complicité dans les cas de mauvais traitements infligés par des entités étrangères* en 2020	Juillet 2021	Décembre 2021

Annexe D : Conclusions et recommandations formulées dans le cadre des examens

Cette annexe énumère les conclusions et les recommandations de l'OSSNR pour les examens dont il est question dans le présent rapport annuel ainsi que les réponses de la direction des entités examinées aux recommandations de l'OSSNR.[45] L'OSSNR a l'intention de publier cette information et d'en faire le suivi pour tous les examens se trouvant sur son site Web.

Examens sur le Service canadien du renseignement de sécurité (SCRS)

Examen de l'OSSNR découlant de la décision 2020 CF 616 de la Cour fédérale, Rétablir la confiance : Réforme des processus de prestation de conseils juridiques du ministère de la Justice et d'obtention de mandats du SCRS

Conclusions de l'OSSNR

1. L'OSSNR constate que le processus de demande et de prestation de conseils juridiques et les limites du GLCSN en matière de ressources contribuent à des retards importants, [description de la durée].
2. L'OSSNR constate que les avis juridiques du ministère de la Justice sont parfois préparés sans qu'une attention suffisante ne soit portée aux destinataires qui doivent les comprendre et prendre des mesures en conséquence. Les avis concernaient principalement l'évaluation des risques juridiques, souvent tard dans le cycle d'élaboration d'une activité du SCRS, et les efforts visant à proposer d'autres moyens légaux pour arriver à l'objectif fixé étaient limités.
3. L'OSSNR constate que le cadre de gestion des risques juridiques du ministère de la Justice n'est pas bien compris au niveau opérationnel du SCRS et qu'il n'offre pas un cadre approprié pour la communication sans ambiguïté du comportement illicite au SCRS.
4. L'OSSNR constate que les difficultés de l'obtention rapide de conseils juridiques pertinents ont contribué à [Discussion sur les effets nuisibles et les risques dans le contexte des opérations] pouvant nécessiter des conseils juridiques. Par conséquent, la façon dont le ministère de la Justice a fourni des conseils juridiques au SCRS ne répond pas toujours aux besoins des opérations du SCRS.
5. L'OSSNR constate que le ministère de la Justice ne produit pas l'analytique organisationnelle nécessaire pour faire un suivi de son rendement en matière de prestation de services au SCRS.

6. L'OSSNR constate que le ministère de la Justice a reconnu que les cloisonnements internes au sein du GLCSN entre les équipes des conseils et des litiges ont parfois fait en sorte que l'avocat responsable des mandats n'est pas au courant de questions juridiques émergentes, et que le ministère de la Justice a pris des mesures pour régler ces problèmes.

7. L'OSSNR constate que le ministère de la Justice s'est engagé à améliorer sa prestation de conseils au SCRS, notamment par l'adoption de la feuille de route pour présenter ses conseils juridiques, qui demande une collaboration continue avec le SCRS pour atteindre les objectifs opérationnels dans les limites du droit.

8. L'OSSNR constate que le SCRS n'a pas toujours fourni l'information pertinente au GLCSN, entraînant une méfiance et limitant la capacité du ministère de la Justice de fournir des conseils juridiques adaptés à la situation.

9. L'OSSNR est d'avis que l'histoire du SCRS est ponctuée de plusieurs réformes sommaires, suivant lesquelles on a observé des cas de négligence, un roulement important de personnel ayant donné lieu à une dilution des connaissances organisationnelles, ainsi qu'un renouvellement des ressources qui, en l'occurrence, ne répondait pas aux priorités énoncées. Le SCRS ne dispose d'aucun mécanisme permettant de faire le suivi des réformes ou d'en mesurer les résultats.

10. L'OSSNR est d'avis que les politiques du SCRS sont en retard sur la réalité opérationnelle : elles sont souvent floues et désuètes, et elles comportent des dédoublements, quand elles ne sont pas carrément en contradiction les unes avec les autres. L'absence de politiques transparentes sème le doute, voire l'inquiétude et donne lieu à des interprétations divergentes quant aux normes juridiques et opérationnelles.

11. L'OSSNR est d'avis qu'il y a des lacunes sur le plan de la compréhension des processus et des critères permettant d'évaluer le niveau de priorité d'un mandat. Les fréquents changements apportés au mécanisme de priorisation ont accru le niveau d'incertitude quant au déroulement des opérations. Le processus de priorisation fait en sorte qu'il a été particulièrement difficile de porter, à l'attention de la Cour, de nouvelles questions visant à résoudre les ambiguïtés juridiques par des décisions de la Cour.

12. L'OSSNR est d'avis que les intervenants prenant part au processus relatif aux mandats sont susceptibles d'interpréter/de percevoir différemment les motifs justifiants chacune des [multiple] étapes qui composent le processus global devant mener à l'obtention d'un mandat, et ne sont pas toujours certains de l'objet de chacune de ces étapes.

13. L'OSSNR est d'avis que la surmultiplication des procédures devant mener à l'obtention de mandats a considérablement affaibli le degré de responsabilisation d'un système

désormais considéré comme étant lent et désorganisé, mais aussi caractérisé par les retards causés par la multiplicité des niveaux d'approbation.

14. L'OSSNR note qu'il n'y a aucun système formel de rétroaction qui puisse faire en sorte que les motifs des décisions prises à un niveau donné soient connus des intervenants des autres niveaux. Le défaut de rétroaction est particulièrement évident du côté des enquêteurs régionaux.

15. L'OSSNR constate que souvent, le seul moyen de résoudre les doutes en matière juridique est de porter les questions litigieuses devant la Cour fédérale par l'intermédiaire de demandes de mandats. En l'occurrence, le lourd processus relatif aux mandats complique inutilement les mesures de résolution des doutes juridiques.

16. L'OSSNR constate que le SCRS a éprouvé des difficultés lorsqu'il s'est agi de veiller à ce que toutes les informations substantielles permettant d'établir la crédibilité des sources soient adéquatement consignées dans les demandes de mandat. Le problème des « omissions récurrentes » est principalement attribuable à la méconnaissance du rôle tenu par la Cour fédérale dans l'évaluation de la crédibilité des sources ainsi qu'à l'éparpillement des informations dans plusieurs systèmes de gestion distincts. L'OSSNR reconnait que le SCRS a apporté d'importants changements, mais il reste beaucoup à faire avant de pouvoir mettre en œuvre une solution à long terme qui soit viable.

17. L'OSSNR estime que la création de la Sous-section des déposants (SSD) constitue une réforme louable, voire vitale pour le SCRS. Toutefois, la SSD est arrivée au point où elle risque de s'effondrer. Le SCRS n'a offert ni les ressources ni le soutien nécessaire à la viabilité de cette Sous-section qui, pourtant, exerce des fonctions essentielles pour la mission du SCRS. Les avantages dont le SCRS peut jouir grâce au travail de la SSD risquent de disparaître en raison de lacunes sur le plan de la gouvernance, des ressources humaines et du perfectionnement de l'effectif.

18. L'OSSNR estime qu'en relevant de la Direction des [Nom], la Sous-section des déposants occupe, dans l'organigramme, une place qui ne témoigne pas suffisamment de l'importance des fonctions que la Sous-section exerce. Cette anomalie en matière de gouvernance engendre probablement plusieurs des obstacles administratifs rencontrés par la SSD et des problèmes observés sur le plan des ressources humaines.

19. L'OSSNR estime que sans une SSD fonctionnelle et capable de préparer, en temps opportun, des demandes de mandats qui soient complètes et précises, le SCRS risque de ne pas obtenir les mandats demandés, ce qui le priverait des informations qu'il pourrait collecter grâce au mandat.

20. L'OSSNR est d'avis de que le rôle « d'avocat indépendant » (AI) tel qu'il est tenu par l'avocat du GSN n'est pas en mesure d'exercer une fonction de contrôle suffisamment rigoureuse.

21. L'OSSNR est d'avis que les coordonnateurs régionaux des demandes de mandat du SCRS n'ont pas reçu de formation qui les rende suffisamment aptes à traduire la teneur des mandats en mesures concrètes d'exécution de ces mêmes mandats.

22. L'OSSNR est d'avis que le SCRS affiche des lacunes pour ce qui a trait aux programmes de formation à long terme destinés aux agents du renseignement.

23. L'OSSNR est d'avis que le SCRS n'a pas été en mesure d'offrir des programmes formels de formation aux intervenants « autres que les agents du renseignement ».

24. L'OSSNR est d'avis que la Division de l'apprentissage et du perfectionnement du SCRS n'a pas disposé des ressources requises pour élaborer et administrer des programmes de formation complets, particulièrement dans les domaines spécialisés qui ne sont pas couverts par la formation que les agents du renseignement reçoivent en début de carrière.

25. L'OSSNR est d'avis que le SCRS et le ministère de la Justice risquent de ne pas être en mesure d'exercer leurs missions respectives. Ni l'une ni l'autre des réformes proposées n'arrivera seule à résoudre les problèmes; une mise en œuvre concertée de l'ensemble des réformes s'impose. Or, cette mise en œuvre de l'ensemble des réformes ne fonctionnera que si elle constitue une priorité majeure pour la haute direction et si elle dispose de ressources suffisantes et stables, c'est-à-dire si elle peut compter sur l'effectif et les connaissances institutionnelles permettant une instauration adéquate desdites réformes. De plus, toute initiative de réforme doit être accompagnée d'une série d'indicateurs de rendement clairement énoncés ainsi que de mécanismes de mesure et d'analyse permettant de faire le suivi des progrès réalisés.

Recommandations de l'OSSNR et réponses ministérielles

Recommandation	Réponse ministérielle (29 mars 2022)
Recommandation 1 : Que le ministère de la Justice poursuive son engagement à réformer la prestation de conseils juridiques au SCRS et à adopter comme pratique exemplaire la feuille de route pour fournir des conseils. En appui de cet objectif et de la prestation de conseils opportuns et pertinents pour les opérations, l'OSSNR recommande également que le ministère de la Justice assure la mise en place de ce qui suit :	**D'accord.** Avant même le dépôt du rapport de l'OSSNR, Justice Canada travaillait sur un certain nombre de mesures liées aux politiques et aux pratiques en matière de prestation de services juridiques au SCRS. Ces mesures touchent aux activités liées à l'obligation de franchise et au processus d'obtention des mandats, aux pratiques exemplaires en matière de prestation de services juridiques, à la prestation de conseils au SCRS sur les risques juridiques associés à ses opérations,

Recommandation	Réponse ministérielle (29 mars 2022)
• Soit au moyen d'un programme offrant des heures de bureau étendues avec des avocats responsables de la liaison ou autre, le GLCSN doit mettre sur pied un service de soutien juridique accessible en tout temps par les agents du SCRS de tous les niveaux et de tous les bureaux régionaux et doté d'avocats d'expérience habilités à fournir des conseils opérationnels en temps réel se fondant sur les positions établies du ministère de la Justice au sujet de questions juridiques récurrentes et sur lesquels les agents du SCRS peuvent s'appuyer. • Le GLCSN conçoit un outil de référence concis donnant sa position sur les enjeux récurrents et les autorisations légales invoquées les plus courantes et rend cet outil accessible aux avocats pour soutenir la prestation de conseils en temps réel. • Afin de minimiser le besoin de recourir au processus officiel de demandes de conseils juridiques, le GLCSN (de concert avec le SCRS) doit associer un avocat aux agents du SCRS dès le début de la planification d'opérations clés ou inhabituelles et tout au long du cycle opérationnel afin de gérer les cas du processus itératif d'orientation juridique.	aux échanges d'informations dans le contexte de la sécurité nationale, ainsi qu'au suivi des principaux indicateurs de rendement liés à la prestation de services juridiques et aux réponses à y donner. Justice Canada s'est engagée à améliorer la prestation de services juridiques et à assurer des services juridiques pratiques et opportuns. Les mesures prises jusqu'ici et celles qui le seront bientôt soutiennent une approche coordonnée des services juridiques et l'atteinte d'un juste équilibre entre les ressources affectées aux priorités organisationnelles et opérationnelles. Il est ici question de fournir des services juridiques de façon plus accessible, régulière, et de soutenir les avocats au moyen d'une formation interactive et de soutenir leur travail en amont. Dans un modèle intégré de collaboration entre Justice Canada et le SCRS, l'avocat intervient dans tout le cycle de vie d'une opération, y compris aux premières étapes. Une intégration rapide dans la planification opérationnelle favorise la prestation de conseils juridiques pertinents et opportuns à mesure que l'opération progresse. Justice Canada a déjà modifié son modèle d'avocat de liaison. Les avocats de liaison sont des avocats chevronnés désignés pour soutenir les agents du SCRS dans tous les bureaux régionaux et dans certaines opérations. Les améliorations apportées à leur rôle font que les avocats de liaison fournissent des conseils opportuns et cibles, appuient les impératifs opérationnels et cernent les tendances et les sujets de préoccupation afin d'élaborer des documents d'orientation et d'autres outils pratiques. Justice Canada met au point une série d'outils pratiques et de mécanismes de prestation de

Recommandation	Réponse ministérielle (29 mars 2022)
	services juridiques pour soutenir le SCRS. Parmi ceux-ci, citons : • un blogue convivial qui décrit en langage simple les concepts et les enjeux juridiques et leur application pratique au travail du SCRS; • un guide sur l'application pratique de questions juridiques aux opérations du SCRS, que les agents peuvent utiliser sur le terrain et en temps réel; • des documents d'interprétation et d'orientation; • des outils de gestion des connaissances permettant aux avocats de consulter les précédents et interprétations juridiques.
Recommandation 2 : Que le GLCSN (de concert avec le SCRS) définisse des indicateurs de rendement clés pour mesurer la prestation des services juridiques au SCRS.	**D'accord.** Justice Canada a élaboré des paramètres opérationnels pour mesurer le rendement de la prestation de services. Il continuera de travailler avec le SCRS pour investir des ressources dans la réalisation d'analyses détaillées de ses activités afin d'améliorer la prestation des services juridiques et d'apporter des modifications au système existant. Des sondages auprès des clients sont effectués régulièrement.
Recommandation 3 : Que le SCRS et le ministère de la Justice ajoutent à leurs programmes de formation une formation interactive fondée sur les scénarios améliorant l'expertise sur les opérations de renseignement des avocats du GLCSN et les connaissances juridiques du personnel des opérations du SCRS.	**D'accord.** Justice Canada travaille avec le SCRS pour élaborer et offrir une formation interactive fondée sur des mises en situation et est déterminé à poursuivre cette collaboration. Renvoi aux recommandations nº 14 et nº 18.
Recommandation 4 : Afin le ministère de la Justice puisse fournir des conseils juridiques utiles et adaptés au sens de la recommandation nº 1, que le SCRS invite l'avocat du ministère de la Justice à toutes les étapes du cycle de vie des opérations clés et inhabituelles, et qu'il l'informe	**D'accord.** Comme il a déjà été mentionné, Justice Canada travaille avec le SCRS pour intervenir plus tôt et de façon plus régulière au cours du cycle de vie des opérations afin de fournir des services juridiques opportuns, ciblés et réguliers.

Recommandation	Réponse ministérielle (29 mars 2022)
complètement et sincèrement des objectifs, intentions et détails de l'opération.	
Recommandation 5 : Que la prestation de conseils par le ministère de la Justice communique clairement et sans équivoque un conseil sur l'illégalité de la conduite d'un client, qu'il s'agisse d'une infraction criminelle ou autre.	**D'accord.** Justice Canada entreprend actuellement un examen de son cadre de gestion des risques juridiques afin d'améliorer tant sa façon d'évaluer les risques juridiques que sa façon de les communiquer aux clients.
Recommandation 6 : Que le SCRS énonce clairement, adopte et diffuse en interne les critères régissant le processus de priorisation des mandats.	**D'accord.** Le SCRS améliorera encore le processus de priorisation des demandes de mandats et travaillera à établir des critères clairs.
Recommandation 7 : Que le SCRS mette en place un nouveau processus relatif aux mandats qui élimine les étapes ne contribuant pas indispensablement à l'optimisation des demandes. Le processus devrait énoncer clairement les règles de responsabilisation qui contribueront à l'optimisation des demandes. Une fois rationnalisé, le système devrait réduire au minimum les retards engendrés par les approbations de la direction et réinvestir le temps économisé dans les étapes d'optimisation des demandes.	**D'accord.** Le travail de mise en œuvre est en cours. Le SCRS et Justice Canada sont résolus à simplifier les modèles et les demandes de mandats, dans le cadre d'objectifs de modernisation plus vastes.
Recommandation 8 : Que le SCRS consulte les intervenants régionaux (notamment, les enquêteurs concernés) à chacun des jalons du processus relatif aux mandats.	**D'accord.** Le SCRS a déjà commencé à apporter des améliorations pour répondre à cette recommandation. Il a notamment mis à jour le modèle opérationnel d'obtention de mandats de la Sous-section des déposants, qui inclut maintenant les intervenants régionaux.
Recommandation 9 : Que le SCRS adopte des politiques et des procédures qui régissent le processus rationnalisé s'appliquant aux mandats; qu'il énonce clairement les rôles et les responsabilités qui incombent à chacun des participants et définisse précisément l'objet de chacune des étapes du processus s'appliquant aux mandats; que les politiques adoptées soient tenues à jour suivant l'évolution du processus.	**D'accord.** La version révisée de la politique commune du SCRS et de Justice Canada sur l'obligation de franchise et le document d'orientation connexe décrivent le rôle de tous les employés du SCRS (pas juste des déposants) dans le respect des obligations de communication à la Cour. De plus, le SCRS a élaboré une politique sur les mandats relatifs à l'article 21 et est en train de rédiger les procédures connexes. En 2020 et 2021, le SCRS a offert une formation sur

Recommandation	Réponse ministérielle (29 mars 2022)
	l'obligation de franchise à tous ses employés des secteurs opérationnels dans le cadre d'un projet spécial.
Recommandation 10 : Pour résoudre la question apparemment inéluctable des « omissions récurrentes », l'OSSNR recommande que le SCRS regroupe toutes les tâches de gestion des informations relatives aux sources humaines en [un système amélioré.] Le SCRS devrait également continuer de mettre en œuvre des initiatives ayant pour objet de veiller à ce que les responsables des sources se montrent rigoureux lorsqu'il s'agit de documenter les informations faisant foi de la crédibilité des sources et d'en inscrire l'intégralité dans les précis de sources humaines. Parallèlement à ces initiatives, la Sous-section des déposants devrait adopter et suivre des procédures de vérification des informations ayant été préparées par les régions.	**D'accord.** La recommandation appuie un projet du SCRS déjà en cours. Le Comité de direction a approuvé en janvier 2021 un plan d'action décrivant les besoins, et les intervenants au SCRS font avancer ce projet. Le SCRS a dressé une liste exhaustive de ses besoins et défini une solution technique possible. Étant donné la complexité du processus de développement technique, ce sera un long processus.
Recommandation 11 : Que le SCRS reconnaisse l'ampleur du rôle tenu par la Sous-section des déposants en attribuant aux déposants et aux analystes une classification professionnelle qui corresponde à l'importance des responsabilités qui leur incombent.	**D'accord.** Le SCRS a répondu à cette recommandation en classifiant les déposants un niveau au-dessus des agents de renseignement au niveau de travail afin de reconnaître la complexité de leur travail, d'attirer des candidats et de les maintenir en poste. Un processus de dotation par voie de concours de postes de déposants est en cours et devrait être terminé d'ici la fin de mars 2022.
Recommandation 12 : Que le SCRS crée une Direction des déposants relevant directement du directeur du SCRS.	**En désaccord.** Le SCRS note les préoccupations du comité concernant l'emplacement dans la hiérarchie organisationnelle de la Sous- section des déposants. Cela dit, au cours de cet examen, le SCRS a investi considérablement dans la Sous-section des déposants et ses employés ont apporté des changements importants au processus d'obtention de mandats et à sa gouvernance. Le SCRS est certain que ces changements seront suffisants pour répondre aux

Recommandation	Réponse ministérielle (29 mars 2022)
	préoccupations qui ont mené à cette constatation et cette recommandation, particulièrement en ce qui concerne les observations liées aux obstacles administratifs et aux problèmes de ressources humaines. De plus, l'emplacement actuel de la Sous-section des déposants, aux côtés d'autres sous-sections ayant des responsabilités correspondantes dans le processus de demande de mandats, facilite la prestation de conseils continue pendant la durée du cycle de vie du mandat et assure que les obligations en matière de conformité et de franchise soient remplies. Étant donné son importance, le SCRS s'engage à surveiller et évaluer la Sous-section des déposants sur une base continue pour s'assurer que les préoccupations soulevées dans ce rapport ne se reproduisent pas.
Recommandation 13 : Que le SCRS dote la Sous-section des déposants dans les plus brefs délais de sorte qu'elle soit viable et qu'elle puisse exercer adéquatement les fonctions qui lui incombent. En établissant la taille que devrait avoir la SSD, le SCRS devra évaluer le nombre de mandats qu'une équipe de déposants est raisonnablement en mesure de traiter chaque année.	**D'accord.** Conformément à la recommandation, le SCRS a déjà augmenté les ressources affectées à la Sous-section des déposants et approuve l'apport de changements à son organigramme en mars 2021. Comme il a déjà été mentionné, une mesure de dotation est en cours en vue de créer un bassin de candidats qualifiés qui pourraient être mis à contribution pour accroître la capacité de la Sous-section des déposants.
Recommandation 14 : Que le SCRS, suivant une consultation auprès du ministère de la Justice, élabore une formation complète devant être suivie par les déposants et les analystes et énonce les pratiques exemplaires ainsi que les modalités de travail que les membres de la SSD seront appelés à suivre.	**D'accord.** Le SCRS a l'intention d'offrir une formation complète aux employés de la Sous-section des déposants, comme il est recommandé. À la fin de 2021, de premières consultations ont été tenues afin de définir la formation adéquate. Malheureusement, la pandémie a perturbé les activités de formation. Justice Canada appuie le SCRS dans l'élaboration et la prestation d'une formation complète et pratique à tous ceux qui travaillent sur les demandes de mandats. Renvoi aux recommandations n° 5 et n° 18.

Recommandation	Réponse ministérielle (29 mars 2022)
Recommandation 15 : L'OSSNR recommande que le GLCSN embauche de nouveaux avocats ainsi que du personnel de soutien, et ce, en nombre suffisant pour garantir que les opérations du SCRS ne seront pas compromises par un éventuel manque de ressources au sein du GLCSN.	**D'accord.** Justice Canada et le SCRS continueront de collaborer dans les dossiers des ressources et de la dotation.
Recommandation 16 : Que le rôle d'avocat indépendant tel qu'il est tenu par l'avocat du GSN, au ministère de la Justice, doit être aboli au profit d'une nouvelle fonction de contrôle s'apparentant à celle qu'un avocat de la défense exercerait, comme si les demandes de mandat s'exposaient à des processus accusatoires. Cette fonction de contrôle relevant de Sécurité publique serait appuyée par l'équipe de vérification de Sécurité publique et exercée par un avocat spécialisé provenant du Service des poursuites pénales du Canada, du secteur privé ou d'un autre organisme; il agirait en toute indépendance par rapport au ministère de la Justice et ne serait pas impliqué dans le processus s'appliquant aux demandes de mandat du SCRS.	**D'accord.** Sécurité Publique Canada (SPC) créera une fonction de vérification renforcée, qui relèvera d'elle et qui tiendra compte des principes et des objectifs établis par l'OSSNR. Plus particulièrement, SPC déterminera les solutions possibles pour pouvoir compter sur un soutien juridique indépendant dans l'exercice de cette fonction de vérification améliorée. De plus, SPC veillera à ce que cette fonction de contestation vigoureuse dans le cadre du processus de demande de mandats du SCRS ne complique pas et ne retarde pas déraisonnablement le processus. Pendant que ce travail est en cours, SPC prendra des mesures pour renforcer provisoirement la vérification des mandats.
Recommandation 17 : Que les titulaires du poste de coordonnateur de mandats dans les régions reçoivent une formation adéquate; que le SCRS professionnalise ce poste et donne à ces coordonnateurs les moyens de traduire la teneur des mandats en conseils favorisant leur adéquate exécution.	**D'accord.** Le SCRS reconnaît l'importance de la formation et des centres d'expertise. Il a entrepris de définir les besoins en matière de formation.
Recommandation 18 : Que le SCRS accorde des ressources suffisantes à la création et à la prestation continue de formations évolutives axées sur les scénarios à l'intention de tous les employés du SCRS. Ces formations comprendront notamment :	**D'accord.** Le SCRS est résolu à améliorer la formation offerte à tous ses employés, comme il est recommandé. Les formations fondées sur des mises en situation, qui aident les employés à comprendre l'application des politiques et procédures, font maintenant partie intégrante de la formation opérationnelle, qui prévoit la mise sur pied d'un atelier opérationnel annuel. Une analyse de rentabilisation approuvée récemment

Recommandation	Réponse ministérielle (29 mars 2022)
- une formation annuelle complète sur le traitement des mandats destinée à tous les employés opérationnels; - une formation d'accueil spécialement conçue pour les employés autres que les agents du renseignement; - un programme de perfectionnement à long terme pour les membres du personnel spécialisé.	augmentera considérablement le nombre de postes à l'AP, ce qui permettra d'offrir plus de formations aux employés du SCRS. L'analyse de rentabilisation prévoit la création d'un nouveau poste dont le titulaire sera chargé d'élaborer un programme d'accueil et d'intégration amélioré pour tous les employés nouvellement recrutés, ainsi que la création de nouveaux postes dont les titulaires seront chargés de créer et d'offrir des occasions d'apprentissage additionnelles pour tous les employés des secteurs opérationnels. Renvoi aux recommandations nº 3 et nº 14.
Recommandation 19 : Que les recommandations énoncées dans le présent rapport d'examen soient intégralement mises en œuvre de façon coordonnée et que les progrès ainsi que les résultats de cette mise en œuvre soient documentés pour permettre à la direction du SCRS, au ministre de la Sécurité publique, au ministre de la Justice et à l'OSSNR d'évaluer l'efficacité des réformes et, s'il y a lieu, d'apporter les ajustements qui s'imposent.	**D'accord.** SPC, le SCRS et Justice Canada sont déterminés à adopter une approche globale pour la mise en œuvre des recommandations, en assureront le suivi et rectifieront le tir au besoin dans ce contexte opérationnel complexe.
Recommandation 20 : Que la version intégrale classifiée du présent rapport soit mise à la disposition des juges désignés de la Cour fédérale.	**Partiellement d'accord**. Le procureur général du Canada communiquera le rapport complet, caviardé en raison du secret professionnel de l'avocat, aux juges désignés de la Cour fédérale du Canada.

Examen des activités de réduction de la menace du SCRS : Accent sur la communication de renseignements à des parties externes

Conclusions de l'OSSNR

1. L'OSSNR a constaté que la documentation du SCRS sur les renseignements communiqués à des parties externes dans le cadre des MRM n'était pas uniforme et, parfois, manquait de clarté et de précision.

2. L'OSSNR a constaté que le SCRS ne recense pas ou ne documente pas systématiquement l'autorité et la capacité des parties externes à prendre des mesures ou les effets négatifs plausibles de la mesure.
3. L'OSSNR a constaté que le SCRS n'a pas systématiquement documenté les résultats des MRM et que les rapports après action aux mesures excluent souvent les mesures prises par des parties externes.

Recommandations de l'OSSNR et réponse ministérielle

Recommandation	Réponse du SCRS (Juin 2022)
Recommandation 1. L'OSSNR recommande que, lorsqu'une MRM suppose que le SCRS communique des renseignements à des parties externes, le SCRS doit clairement indiquer et documenter la portée et l'ampleur des renseignements qui seront communiqués dans le cadre de la mesure proposée.	**D'accord.** Le SCRS est d'accord avec cette recommandation. En tant qu'organisation engagée à être complètement transparente avec les Canadiens, le SCRS bénéficie des examens externes et valorise leurs recommandations en mettant à jour, si possible, ses politiques, pratiques et procédures afin de s'assurer que toutes mesures qu'il entreprend, y compris la divulgation de renseignements aux tierces personnes, soient documentées en totalité.
Recommandation 2. L'OSSNR recommande que le SCRS indique, documente et considère de manière exhaustive l'autorité et la capacité de la partie externe à prendre des mesures ainsi que les répercussions négatives possibles de la mesure.	**Partiellement d'accord.** Le SCRS est partiellement d'accord avec cette recommandation. Bien que le Service accepte complètement la recommandation de documenter l'autorité et l'habileté des tierces personnes à agir, ainsi que ses possibles effets néfastes, cette information ne provient pas du SCRS et n'est donc pas toujours disponible ou accessible de manière constante parmi les partis impliqués.
Recommandation 3. L'OSSNR recommande que le SCRS modifie sa politique sur les MRM de manière à y inclure l'obligation d'indiquer systématiquement les mesures prises par les parties externes. Cette pratique devrait guider les évaluations après action et la prise de décisions futures.	**Partiellement d'accord.** Le SCRS est partiellement d'accord avec cette proposition. Les politiques du Service incluent des exigences en matière de rapports comme la documentation des MRM. Les actions prises par de tierces personnes sont documentées lorsqu'elles sont disponibles. Toutefois, ces actions sont volontaires, tout

	comme sont volontaires les discussions et les échanges avec le Service.
Recommandation 4. L'OSSNR recommande que le SCRS se conforme à ses politiques de tenue de dossiers concernant la documentation des résultats des MRM.	**D'accord**. Le SCRS est d'accord avec cette recommandation. Toutefois, la recommandation est basée sur un examen de rapports désuets et n'est donc pas tout à fait exacte. En effet, depuis le début de 2019, le SCRS a entièrement documenté les résultats des MRM de manière à respecter ses politiques en matière de tenue de dossiers.
Recommandation 5. L'OSSNR recommande que le SCRS prenne en compte de manière appropriée les répercussions résultant des mesures prises par des parties externes lorsqu'ils déterminent si un mandat est nécessaire.	**En désaccord**. Le SCRS n'est pas d'accord avec la position de l'OSSNR quant à l'utilisation des tiers partis en appuis aux MRM. Le SCRS travaille en étroite collaboration avec le Ministère de la Justice pour évaluer si un mandat est requis pour chacune de ses mesures, incluant celles qui s'appliquent aux tiers partis, le tout, en conformité avec le cadre législatif en place.

Examens sur le Centre de la sécurité des télécommunications (CST)

Examen de la gouvernance des cyberopérations actives et défensives du CST

Conclusions de l'OSSNR

1. Les demandes d'autorisation ministérielle des cyberopérations défensives et actives ne fournissent pas suffisamment de détails pour que le ou les ministres puissent saisir la portée des catégories d'activités demandées dans l'autorisation. De même, l'autorisation ministérielle ne précise pas suffisamment les catégories d'activités, les techniques connexes et les ensembles de cibles à utiliser dans la conduite des opérations.
2. L'évaluation des risques sur le plan de la politique étrangère exigée par deux conditions de l'autorisation dépend trop des risques d'attribution technique plutôt que des caractéristiques qui reflètent la politique étrangère du gouvernement du Canada.
3. Le cadre de gouvernance actuel ne comprend pas de mécanisme pour confirmer l'harmonisation d'une cyberopération active (COA) avec les priorités stratégiques plus vastes du gouvernement du Canada (GC), comme l'exigent la Loi sur le CST et l'autorisation ministérielle. Bien que ces objectifs et priorités ne relèvent pas uniquement du CST et

d'AMC, les deux ministères gouvernent les COA sans la participation de l'ensemble de la collectivité du GC contribuant à la gestion des objectifs généraux du Canada.

4. Le CST et AMC n'ont pas établi de seuil pour déterminer comment identifier et distinguer une cyberopération défensive préventive d'une cyberopération active, ce qui peut mener à une participation insuffisante d'AMC si l'opération erronément classée comme étant défensive.

5. Les politiques internes du CST concernant la collecte de renseignements pendant les cyberopérations ne sont pas décrites avec précision dans les autorisations ministérielles des cyberopérations actives et défensives.

6. Le processus de présentation des cibles, qui a lieu après l'approbation des documents de planification, contient des renseignements pertinents pour les plans opérationnels généraux du CST. La présentation de l'objectif contenait parfois des renseignements pertinents qui ne figuraient pas dans ces autres documents, même s'ils sont approuvés à un niveau de gestion inférieur.

7. Le CST a offert à ses employés des occasions d'apprentissage de haut niveau pour en apprendre davantage sur ses nouveaux pouvoirs de mener des cyberopérations actives et défensives (COA/COD). Toutefois, il se peut que les employés qui travaillent directement sur les COA ou les COD ne comprennent pas les détails des nouveaux pouvoirs juridiques du CST et les nouveaux paramètres entourant leur utilisation.

8. Le CST et AMC n'ont pas suffisamment élaboré de cadre clair et objectif pour évaluer les obligations du Canada en vertu du droit international relativement aux cyberopérations actives et défensives.

9. Le CST s'attend à ce qu'AMC l'informe de tout changement aux risques liés à la politique étrangère, mais il n'a pas suffisamment tenu compte de la nécessité de communiquer à AMC les autres risques qui peuvent survenir au cours d'une opération. De plus, les renseignements essentiels à l'évaluation des risques en matière de politique étrangère par AMC ont également été exclus des documents que le CST utilise pour faire participer AMC dans une opération. Par conséquent, dans le cadre de consultation actuel, le CST pourrait ne pas communiquer suffisamment de renseignements pertinents à AMC pour appuyer son évaluation de la politique étrangère et pour gérer les changements continus dans le risque associé à une cyberopération.

Recommandations de l'OSSNR

Recommandation

Recommandation 1. L'OSSNR recommande que le CST définisse plus précisément les catégories d'activités, les techniques connexes et les ensembles d'objectifs prévus pour les cyberopérations actives et défensives ainsi que pour leur justification et leurs objectifs sous-jacents, tant dans les demandes que dans les autorisations ministérielles connexes pour ces activités.

Recommandation 2. L'OSSNR recommande à AMC d'inclure un mécanisme pour évaluer tous les paramètres de risque pertinents liés à la politique étrangère des cyberopérations actives et défensives dans le cadre des autorisations ministérielles connexes.

Recommandation 3. L'OSSNR recommande que le CST et AMC établissent un cadre de consultation des principaux intervenants, comme le conseiller en matière de sécurité nationale et de renseignement auprès du premier ministre et d'autres ministères fédéraux dont les mandats recoupent les cyberopérations actives proposées, pour veiller à ce qu'ils s'harmonisent avec les priorités stratégiques générales du gouvernement du Canada et à ce que les exigences de la Loi sur le CST soient satisfaites.

Recommandation 4. L'OSSNR recommande que le CST et AMC établissent un seuil qui permet de faire la distinction entre une cyberopération active et une cyberopération défensive préventive. Ce seuil devrait être décrit au ministre de la Défense nationale dans les autorisations ministérielles applicables.

Recommandation 5. L'OSSNR recommande que, dans ses demandes au ministre de la Défense nationale, le CST décrive de manière précise la possibilité que des activités de collecte se produisent dans le cadre d'autorisations distinctes au cours des cyberopérations actives et défensives.

Recommandation 6. L'OSSNR recommande au CST d'inclure tous les renseignements pertinents, notamment les renseignements concernant le ciblage et le contexte, dans tous les plans opérationnels en place pour une cyberopération ainsi que dans les documents qu'il présente à AMC.

Recommandation 7. L'OSSNR recommande que le CST offre un programme de formation structuré à ses employés qui participent à l'exécution des cyberopérations actives et défensives (COA et COD) afin de s'assurer qu'ils ont la connaissance requise des pouvoirs, des exigences et des interdictions juridiques du CST, conformément aux autorisations ministérielles connexes.

Recommandation 8. L'OSSNR recommande que le CST et AMC fournissent une évaluation du régime juridique international applicable à la conduite des cyberopérations actives et défensives. De plus, le CST devrait exiger qu'AMC effectue et documente une évaluation juridique approfondie de la conformité de chaque opération au droit international.

Recommandation 9. L'OSSNR recommande que le CST et AMC communiquent entre eux tous les renseignements et tous les nouveaux développements pertinents à l'évaluation des risques associés à une cyberopération, tant au cours des phases de planification que pendant l'exécution.

Examen sur l'échange de renseignements dans tous les volets du mandat du CST

Conclusions de l'OSSNR

1. L'échange interne de renseignements entre les volets du renseignement étranger et de la cybersécurité du mandat du CST n'a pas fait l'objet d'un examen suffisant pour assurer la conformité à la *Loi sur la protection des renseignements personnels*.
2. À une exception près, les demandes d'autorisation ministérielle présentées par le chef du CST en 2020 informaient adéquatement le ministre de la Défense nationale que les renseignements conservés pourraient servir à appuyer un autre volet.
3. Les demandes d'autorisations de renseignement étranger faites par le chef du CST pendant la période visée par l'examen ont correctement informé le ministre de la Défense de la façon dont le caractère essentiel énoncé à l'alinéa 34(2)c) était respecté pour l'IRCPC recueillie dans le cadre du volet du renseignement étranger.
4. Le cadre stratégique du CST concernant l'échange interne de renseignements entre les volets du renseignement étranger et de la cybersécurité du mandat respecte la Loi sur le CST.

Recommandation de l'OSSNR et réponse du CST

Recommandation	Réponse du CST (Mai 2022)
Recommandation 1. L'OSSNR recommande que le CST obtienne des avis juridiques supplémentaires sur l'échange interne de renseignements entre les volets du renseignement étranger et de la cybersécurité de son mandat, notamment en ce qui a trait au respect de la *Loi sur la protection des renseignements personnels*, qui traite en détail des deux questions suivantes : 1) Si le partage interne de renseignements entre les aspects du renseignement étranger et de la cybersécurité du mandat constitue une utilisation ou une communication de renseignements aux fins de la *Loi sur la protection des renseignements personnels*; *2)* Si les utilisations et les communications sont effectuées conformément aux articles 7 et 8	Le CST refuse la recommandation nº 1. Le CST a déjà reçu des conseils juridiques exhaustifs et clairs à ce sujet de la part du ministère de la Justice et se fie à ces conseils dans le cadre de ses activités (dont l'OSSNR a conclu qu'elles se déroulent dans le respect de la loi).

de la *Loi sur la protection des renseignements personnels*.	
Recommendation 2. Toutes les applications de renseignement étranger et de cybersécurité provenant de la chef du CST devraient adéquatement mettre la ministre de la Défense nationale au courant de l'utilisation potentielle d'informations conservées à l'appui d'autres aspects du mandat du CST.	Le CST a déjà mis en œuvre cette recommandation. L'organisme informe déjà la ministre, et continuera de le faire, au sujet de l'utilisation des informations dans le cadre des autres aspects de son mandat. Les applications pour toutes les autorisations ministérielles liées au renseignement étranger et à la cybersécurité en 2021-2022 comprenaient un libellé expliquant clairement comment les informations recueillies en vertu de l'un des aspects du mandat du CST pourraient être utilisées pour appuyer d'autres aspects du mandat.

Ministère de la Défense nationale et Forces armées canadiennes

Examen de l'Unité nationale de contre-ingérence des Forces canadiennes — Collecte opérationnelle et pratiques en matière de protection des renseignements personnels

Conclusions de l'OSSNR

1. L'OSSNR a constaté que l'UNCIFC s'appuie de manière inappropriée sur des politiques du MDN et des FAC à titre d'autorité légale pour porter atteinte aux attentes raisonnables d'un sujet en matière de protection des renseignements personnels.
2. L'OSSNR a constaté que la liste de vérification du MDN et des FAC utilisée à titre d'instruction permanente d'opération en matière d'enquête risque de recueillir des renseignements qui sont protégés en vertu de l'article 8 de la Charte.
3. L'OSSNR a constaté que le MDN et les FAC appliquent une définition des métadonnées qui comprend les renseignements pouvant faire l'objet d'une attente raisonnable en matière de protection des renseignements personnels.
4. L'OSSNR a constaté que l'UNCIFC risque de violer les droits à la protection des renseignements personnels en n'ayant pas d'orientation stratégique claire fondée sur l'autorité légitime pour les recherches en TI en élargissant les recherches en TI au-delà des paramètres de recherche approuvés.
5. L'OSSNR a constaté que les pratiques d'enquête relatives au système de TI qu'il a observées dans le contexte des enquêtes de contre-ingérence de l'UNCIFC ne font pas

l'objet d'une surveillance juridique suffisante pour veiller à ce qu'elles soient les moins invasives possible.

Recommandations de l'OSSNR et réponse du MDN et des FAC

Recommandation	Réponse (25 mai 2022)
Recommandation 1. L'OSSNR recommande que le MDN et les FAC suspendent les pratiques d'enquête sur les systèmes de TI dans le contexte des enquêtes de contre-ingérence de l'UNCIFC jusqu'à ce qu'une autorisation juridique raisonnable ait été établie.	Le ministère de la Défense nationale et les Forces armées canadiennes (MDN et FAC) reconnaissent et accueillent favorablement le rapport annuel de 2021 produit par l'Office de surveillance des activités de renseignement de sécurité nationale (OSSNR). Le MDN et les FAC reconnaissent l'importance d'un examen externe indépendant des activités de sécurité nationale et de renseignement du gouvernement du Canada pour s'assurer qu'elles sont légales, raisonnables et nécessaires. De plus, le MDN et les FAC demeurent déterminés à tenir des discussions ouvertes et transparentes au sujet de ces activités de sécurité nationale et de renseignement, car les examens externes améliorent la façon dont le Ministère mène ses activités au nom des Canadiens. Le MDN et les FAC continueront de tenir compte de toutes les recommandations formulées par l'OSSNR dans leurs examens externes et attendent avec impatience de recevoir d'autres rapports de leur part.
Recommandation 2. L'OSSNR recommande qu'une fois qu'une autorité juridique raisonnable aura été établie, le MDN et les FAC créent un nouveau cadre stratégique qui reflète les conclusions notées, à savoir une liste de vérification multipoints, la catégorisation des métadonnées et le fait que les recherches en TI soient les moins invasives que possible.	

Examens multiministériels

Examen sur la communication de renseignements par les institutions fédérales en vertu de la *Loi sur la communication d'information ayant trait à la sécurité du Canada* en 2020, un examen conjoint avec le Commissariat à la protection de la vie privée

Conclusions

1. Des renseignements personnels relatifs à la sécurité nationale peuvent être communiqués dans les situations où les institutions fédérales ne sont pas conscientes des exigences relatives à l'autorisation légale de le faire.
2. Selon les renseignements examinés, la quasi-totalité (environ 99 %) des communications de renseignements faites en vertu de la *Loi sur la communication d'information ayant trait à la sécurité du Canada* (LCISC) en 2020 ont satisfait au critère de communication prévu à l'alinéa 5(1)a).
3. Selon les renseignements examinés, la quasi-totalité (environ 99 %) des divulgations de renseignements effectuées en vertu de la LCISC en 2020 ne semblent pas avoir d'incidence sur les intérêts en matière de protection de la vie privée d'une personne plus qu'il n'était raisonnablement nécessaire dans les circonstances. Toutefois, la seule communication non conforme par la GRC représente la grande majorité de tous les renseignements personnels confirmés qui ont été communiqués en vertu de la LCISC en 2020.
4. Presque toutes les communications (près de 98 %) comprenaient des déclarations d'exactitude et de fiabilité, bien qu'il y ait eu des incohérences quant à la suffisance et à la spécificité des déclarations.
5. La tenue de dossiers d'une institution qui a utilisé la LCISC pour la première fois ne répondait pas aux exigences de la LCISC.
6. La plupart des dossiers étaient bien organisés et ne comportaient aucune anomalie, bien que certains aient été fournis d'une manière difficile à comprendre et à examiner.
7. L'examen a permis de relever des cas où les dossiers conservés à des fins de communication ne contenaient pas une description suffisante, comme l'exige l'alinéa 9(1)e), des renseignements sur lesquels l'institution fédérale s'était basée pour conclure que la communication était autorisée en vertu de la LCISC.
8. Presque toutes les divulgations (plus de 97 %) comprenaient des mises en garde appuyant le droit de regard de la source et le partage responsable de l'information.

9. En vertu de la LCISC, IRCC et le CST ainsi qu'AMC et le SCRS s'échangent régulièrement des renseignements d'une nature et d'une manière qui justifient des ententes d'échange de renseignements, comme l'encourage l'alinéa 4c) de la LCISC.

10. Sécurité publique Canada coordonne la mise en œuvre de la LCISC parmi les institutions fédérales et les 17 institutions fédérales énumérées dans la LCISC possèdent du personnel qui a suivi la formation de la LCISC de Sécurité publique Canada.

11. L'Agence canadienne d'inspection des aliments (ACIA) ne disposait pas des politiques ou des procédures nécessaires pour appuyer la conformité à la LCISC.

Recommandations de l'OSSNR et réponses ministérielles

Recommandation	Réponse (février 2022)
Recommandation 1. Compte tenu des restrictions énoncées à l'article 8 de la *Loi sur la protection des renseignements personnels* pour les communications de tels renseignements, l'OSSNR et le CPVP recommandent aux institutions expertes en sécurité nationale de s'assurer que, quand elles demandent des renseignements personnels à d'autres institutions fédérales pour des motifs qui intéressent la sécurité nationale, elles soient claires sur le fait que leurs demandes en tant que telles ne confèrent pas le pouvoir de communiquer des renseignements personnels.	**D'accord**. Étant donné que les demandes de renseignements n'autorisent pas en soi les institutions fédérales à communiquer des renseignements personnels, plusieurs ministères et organismes du gouvernement du Canada ont déjà élaboré et mis en œuvre des politiques internes pour établir des attentes claires, des lignes directrices cohérentes et des [...] pour conserver les pratiques relatives à la divulgation de renseignements personnels à des fins de sécurité nationale, conformément aux autorisations légales. Fait important, il incombe à chaque institution fédérale de connaître et de mettre en œuvre ses obligations et à chaque administrateur général de veiller à ce que des directives et des ressources soient mises en place pour s'acquitter de ces obligations. Sécurité publique Canada continuera de collaborer avec les ministères et organismes partenaires pour offrir aux institutions fédérales un accès à la formation, des conseils et d'autres ressources utiles sur l'échange de renseignements relatifs à la sécurité nationale qui aident à expliquer les exigences relatives à la communication de ce type de renseignements de façon légale. Sécurité publique Canada mettra

	également à jour son guide de la LCISC et les modèles connexes de demande et communication de renseignements en vertu de la LCISC afin d'aider les institutions fédérales à comprendre leurs pouvoirs en matière de demande et de divulgation de renseignements sur la sécurité nationale.
Recommandation 2. L'OSSNR et le CPVP recommandent que la GRC termine la mise à jour de sa politique relative à la LCISC afin d'appuyer la conformité au critère de communication de la LCISC, de fournir des conseils à ses décideurs habilités à faire des communications en vertu de la LCISC sur l'analyse requise pour s'assurer que le critère de divulgation est respecté et de s'assurer que ces décisions sont bien documentées.	**D'accord**. La GRC a fait des progrès importants vers la modernisation de sa politique de la LCISC depuis avril 2021. Cette politique actualisée de la LCISC fournira un complément propre à la GRC des directives générales de Sécurité publique Canada à l'intention des partenaires fédéraux sur les communications de la LCISC. La politique actualisée de la GRC adapte les lignes directrices de la LCISC à un environnement d'application de la loi et permettra aux décideurs de la GRC de communiquer en toute confiance des renseignements sur la sécurité nationale de façon conforme et de veiller à ce que les décisions sur la communication de renseignements personnels soient adéquatement documentées.
Recommandation 3. Premièrement, l'OSSNR et le CPVP recommandent que la GRC fournisse au MDN et aux FAC des renseignements complets et exacts sur la communication non conforme. Deuxièmement, l'OSSNR et le CPVP recommandent que, conformément à l'article 5.1 de la LCISC, le MDN et les FAC évaluent la nécessité de conserver les renseignements personnels reçus à la lumière de ces nouveaux renseignements, de nos conclusions, des directives connexes du MDN et des FAC et des autres politiques applicables.	**Partiellement d'accord**. La GRC ne considère pas comme incomplète ni inexacte l'information qu'elle a fournie au MDN et aux FAC. La GRC a communiqué l'information qui, selon elle, contribuerait à la responsabilisation du ministère de la Défense nationale et des Forces armées canadiennes de cerner les menaces potentielles pour le personnel militaire et de fournir un avertissement stratégique des menaces émergentes, à l'appui de leur mandat de lutte contre le terrorisme. Au moment de la communication, la GRC était convaincue que la communication ne porterait pas atteinte à la protection des renseignements personnels plus qu'il n'était raisonnablement nécessaire dans les circonstances.

	Le MDN et les FAC évalueront s'il est nécessaire de conserver les renseignements personnels reçus compte tenu de l'information fournie par la GRC, des conclusions de l'OSSNR et du CPVP ainsi que de leurs propres directives et politiques. Comme l'indique le rapport sur la LCISC, le MDN et les FAC ont reçu les renseignements de la GRC, en fonction de son mandat de lutte contre le terrorisme.
Recommandation 4. L'OSSNR et le CPVP recommandent que les institutions fédérales répertoriées dans la LCISC évitent d'utiliser des formules figées dans les énoncés d'exactitude et de fiabilité lorsque la nature et la source de l'information divulguée ne sont pas dérivées d'un processus de routine.	**D'accord**. Plusieurs ministères et organismes ont des politiques internes en vigueur qui exigent que les énoncés d'exactitude et de fiabilité soient adaptés à la communication en question et évitent l'utilisation de formules figées. Afin d'appuyer davantage cette recommandation dans l'ensemble des institutions fédérales qui utilisent la LSCIC pour échanger de l'information, Sécurité publique mettra à jour son guide de la LSCIC, la formation et les documents d'orientation connexes afin de tenir compte du fait que les institutions fédérales devraient fournir des énoncés précis et clairs de l'exactitude et de la fiabilité dans les cas où les renseignements communiqués sont obtenus autrement que par un processus de routine. Sécurité publique encouragera également les partenaires fédéraux à inclure ce guide sur les énoncés d'exactitude et de fiabilité dans leurs propres politiques internes, le cas échéant.
Recommandation 5. L'OSSNR et le CPVP recommandent que les institutions répertoriées à l'annexe 3 de la LCISC demandant des renseignements à une institution non inscrite au titre de la LCISC informent cette dernière de ses obligations légales à l'égard de la communication de renseignements en vertu de la LCISC, y compris les exigences en matière de tenue de dossiers, et l'encourage à demander conseil au ministère de la Justice et à Sécurité publique Canada.	**D'accord**. Dans l'intérêt de favoriser la conformité à la LCISC parmi les institutions fédérales, il est considéré comme une pratique exemplaire de demander aux institutions énumérées à l'annexe 3 de la Loi d'informer les institutions fédérales qui ne figurent pas dans la LCISC de leurs obligations légales à l'égard de toute divulgation faite en vertu de la LCISC, y compris les exigences en matière de tenue de dossiers. Il est également considéré comme une pratique exemplaire pour les institutions fédérales d'encourager les partenaires qui ne connaissent pas aussi bien les pouvoirs de

	communication en vertu de la LCISC à utiliser les ressources disponibles auprès du ministère de la Justice et de la Sécurité publique. Tout en reconnaissant qu'il s'agit de pratiques exemplaires et non d'obligations légales des bénéficiaires, Sécurité publique encouragera les partenaires à mettre en œuvre ces pratiques exemplaires en incluant des directives connexes dans son guide mis à jour de la LCISC.
Recommandation 6. L'OSSNR et le CPVP recommandent que les institutions fédérales qui communiquent ou reçoivent régulièrement de l'information au titre de la LCISC normalisent leurs pratiques de conservation de documents selon les dernières instructions de Sécurité publique Canada.	**D'accord**. Plusieurs institutions ont déjà normalisé leurs politiques en matière de tenue de dossiers, ou sont en train de le faire, pour tenir compte des plus récentes directives de Sécurité publique. La poursuite des travaux dans le cadre des groupes de travail dirigés par Sécurité publique aidera à harmoniser les pratiques de tenue de dossiers avec les lignes directrices normalisées pour les institutions qui ne l'ont pas encore fait. Plusieurs partenaires ont aussi des conventions de désignation ou des systèmes de référencement de dossiers internes qui favorisent la normalisation de la conservation de documents. Là où ceux-ci n'existent pas, Sécurité publique Canada met de l'avant un système commun de numéros de référence de dossiers qui doit servir pour les réceptions et les communications d'information afin de normaliser les pratiques de conservation de documents.
Recommandation 7. L'OSSNR et le CPVP recommandent que les institutions veillent à ce que les dossiers conservés pour les communications en bloc comprennent une description suffisamment solide des renseignements sur lesquels elles s'appuient pour s'assurer que la communication de tous les éléments de l'ensemble de données respecte l'article 5 de la LCISC et que le niveau de surveillance interne est proportionnel au risque d'atteinte à la vie privée.	**D'accord.** Les dossiers conservés pour les communications en bloc doivent contenir suffisamment de renseignements pour démontrer que la communication de tous les éléments de l'ensemble de données respecte les seuils de contribution et de proportionnalité contenus dans le critère de communication de l'article 5 de la Loi et le niveau de surveillance interne doit être proportionnel au risque d'atteinte à la vie privée. Dans certains cas, toutefois, les exigences

	opérationnelles peuvent nécessiter une intervention immédiate et une surveillance de suivi proportionnelle au niveau de risque lié à une menace qui mine la sécurité du Canada. Pour aider les ministères et les organismes à mettre en œuvre cette recommandation, une clarification supplémentaire de l'OSSNR et le CPVP serait grandement apprécié sur ce qui constitue une « description suffisamment solide » de cette information. De même, des précisions supplémentaires de la part de l'OSSNR et du Commissariat à la protection de la vie privée du Canada sur ce qui constitue une « communication en bloc » seraient également appréciées, car il n'existe actuellement aucune définition normalisée pour ce terme dans les bases de données du Gouvernement du Canada. Une fois ces éléments clarifiés, Sécurité publique mettra à jour les documents d'orientation de la LCISC en conséquence et partagera cette information par l'entremise de ses groupes de travail interministériels connexes.
Recommandation 8. L'OSSNR et le CPVP recommandent que les institutions fédérales incluent des renseignements sur la façon dont la communication contribuera à leur compétence ou à leurs responsabilités à l'égard d'activités portant atteinte à la sécurité du Canada ainsi que d'autres renseignements pertinents au critère de communication dans leurs demandes écrites de renseignements en vertu de la LCISC, et ce, même si ces renseignements ont été communiqués verbalement avant la demande afin de permettre la tenue de dossiers appropriée par les institutions fédérales communiquant des renseignements en vertu de la LCISC.	**D'accord**. Plusieurs institutions incluent déjà ou demandent que les renseignements décrivant comment la communication contribuera à la compétence ou aux responsabilités des institutions destinataires à l'égard d'activités portant atteinte à la sécurité du Canada soient fournis par écrit. Afin de faciliter la mise en œuvre de cette recommandation dans toutes les institutions, Sécurité publique mettra à jour ses modèles de demande et de communication de renseignements en vertu de la LCISC afin de souligner l'importance d'inclure ces renseignements dans la demande écrite ou la lettre de communication. Les institutions qui n'ont actuellement pas de pratique en place pour inclure ces informations acceptent de revoir leurs politiques internes conformément aux documents

	d'orientation actualisée de la LCISC une fois publiés.
Recommandation 9. L'OSSNR et le CPVP recommandent qu'IRCC et le CST concluent une entente pour structurer leurs échanges d'information au titre de la LCISC.	**D'accord**. IRCC et le CST entameront des discussions afin d'explorer les meilleures solutions pour la création d'une entente d'échange de renseignements entre les deux institutions structurant la communication de renseignements en vertu de la LCISC.
Recommandation 10. L'OSSNR et le CPVP recommandent que le SCRS et AMC mettent à jour leur entente d'échange de renseignements, qui a été précédemment convenue dans le cadre de la LCISC (ancienne loi en vigueur du 1er août 2015 au 20 juin 2019), afin de tenir compte de la LCISC (loi en vigueur).	**D'accord**. Le SCRS et AMC examineront la meilleure façon de mettre à jour leur entente d'échange de renseignements, qui a été précédemment convenue dans le cadre de la LCISC (ancienne loi en vigueur du 1er août 2015 au 20 juin 2019), afin de tenir compte de la LCISC (loi en vigueur). Les deux institutions s'efforceront d'amorcer le processus d'actualisation de l'entente d'échange de renseignements dans un délai raisonnable et de terminer les mises à jour dès que possible en respectant les contraintes des priorités existantes, des urgences opérationnelles émergentes ainsi que d'autres complications qui ont une incidence sur les délais.
Recommandation 11. L'OSSNR et le CPVP recommandent à l'Agence canadienne d'inspection des aliments de consulter Sécurité publique Canada, puis d'élaborer et de mettre en œuvre des politiques et des procédures pour favoriser la conformité à la LCISC.	**D'accord**. Bien que l'Agence canadienne d'inspection des aliments (ACIA) n'ait pas encore communiqué ou reçu de renseignements en vertu de la LCISC, elle collaborera avec Sécurité publique pour élaborer et mettre en œuvre des politiques et des procédures à l'appui de la conformité de la LCISC. Le personnel de l'ACIA se sentira donc habilité à communiquer ou à recevoir des renseignements sur la sécurité nationale en vertu de la LCISC si le besoin s'en fait sentir.
Recommandation 12. L'OSSNR recommande qu'Immigration, Réfugiés et Citoyenneté Canada, et les autres institutions qui reçoivent régulièrement des demandes d'information en vertu de la LCISC, mettent par écrit la pratique consistant à séparer les informations contenues dans les demandes	**D'accord.** IRCC a pour pratique opérationnelle de séparer les demandes de renseignements des autres banques de données et des listes de surveillance. Bien que cette pratique soit incluse dans son document sur les procédures opérationnelles normalisées, pour plus de clarté,

d'informations du reste de ses banques de données et de ses listes de surveillance.	IRCC ajoutera également cette politique dans son guide de politiques sur de renseignements. Sécurité publique Canada inclura également ce guide dans ses documents d'orientation actualisés de la LCISC afin d'encourager d'autres institutions qui reçoivent régulièrement des demandes d'information en vertu de la LCISC à adopter cette pratique exemplaire.

Examen de la mise en œuvre par les ministères de la *Loi visant à éviter la complicité dans les cas de mauvais traitements infligés par des entités étrangères* en 2020

Conclusions de l'OSSNR

1. L'OSSNR a constaté que l'ASFC et Sécurité publique n'ont pas encore mis la dernière main à leurs cadres stratégiques à l'appui des directives reçues en vertu de la LÉC.
2. L'OSSNR a constaté qu'entre le 1er janvier 2020 et le 31 décembre 2020, aucun cas visé par la LÉC n'a été transmis aux administrateurs généraux d'un ministère.
3. L'OSSNR a constaté que, même lorsque les ministères utilisaient des méthodes et des sources d'information semblables pour déterminer si un cas concernant le même pays préoccupant devait ou non être transmis à un échelon supérieur, des divergences importantes dans l'évaluation du risque et le niveau d'approbation requis émergent.
4. L'OSSNR a constaté que, dans une étude de cas portant sur la divulgation de renseignements, le risque de mauvais traitement était important et que la décision aurait dû être renvoyée au sous-ministre des Affaires étrangères, le sous-ministre responsable de cette demande.

Annexe E : Statistiques concernant les enquêtes sur les plaintes

1er janvier 2021 au 31 décembre 2021

Demandes de traitement des plaintes reçues	**67**		
Nombre de nouvelles plaintes déposées	**86**		
Article 16 de la Loi sur l'OSSNR (plaintes visant le SCRS)	14		
Article 17 de la Loi sur l'OSSNR (plaintes visant le CST)	3		
Article 18 de la Loi sur l'OSSNR (habilitations de sécurité)	4		
Article 19 de la Loi sur l'OSSNR (plaintes renvoyées par la GRC)	5		
Article 19 de la Loi sur l'OSSNR (*Loi sur la citoyenneté*)	0		
Article 45 de la Loi sur l'OSSNR (renvois par la CCDP)	60		
Décision sur la compétence d'enquêter	**7**		
	Acceptée	**Rejetée**	**Retirée**
Article 16 de la Loi sur l'OSSNR (plaintes visant le SCRS)	3	14	2
Article 17 de la Loi sur l'OSSNR (plaintes visant le CST)	0	2	0
Article 18 de la Loi sur l'OSSNR (habilitations de sécurité)	4	5	1
Article 19 de la Loi sur l'OSSNR (plaintes renvoyées par la GRC)	0	1	0
Total	7	22	3
Enquêtes actives	**81**		
Article 16 de la Loi sur l'OSSNR (plaintes visant le SCRS)	12		
Article 17 de la Loi sur l'OSSNR (plaintes visant le CST)	0		
Article 18 de la Loi sur l'OSSNR (habilitations de sécurité)	5		
Article 19 de la Loi sur l'OSSNR (plaintes renvoyées par la GRC)	4		
Article 45 de la Loi sur l'OSSNR (renvois par la CCDP)	60		
Règlement à l'amiable	**3**		
Article 16 de la Loi sur l'OSSNR (plaintes visant le SCRS)	2		
Article 18 de la Loi sur l'OSSNR (habilitations de sécurité)	1		

Article 19 de la Loi sur l'OSSNR (plaintes renvoyées par la GRC)	0		
Article 45 de la Loi sur l'OSSNR (renvois par la CCDP)	0		
Enquêtes sur des plaintes dont le dossier est clos	**3**		
	Rapport final	Plainte réglée à l'amiable	Retirée
Article 16 de la Loi sur l'OSSNR (plaintes visant le SCRS)	1	0	0
Article 18 de la Loi sur l'OSSNR (habilitations de sécurité)	0	0	0
Article 19 de la Loi sur l'OSSNR (plaintes renvoyées par la GRC)	0	0	0
Article 45 de la Loi sur l'OSSNR (renvois par la CCDP)	0	0	2
Total	1	0	2
Enquêtes reportées à l'année civile suivante	**78**		
Article 16 de la Loi sur l'OSSNR (plaintes visant le SCRS)	11		
Article 18 de la Loi sur l'OSSNR (habilitations de sécurité)	5		
Article 19 de la Loi sur l'OSSNR (plaintes renvoyées par la GRC)	4		
Article 45 de la Loi sur l'OSSNR (renvois par la CCDP)	58		

Note : Les abréviations figurent à l'Annexe A.

Notes de fin

[1]Office de surveillance des activités en matière de sécurité nationale et de renseignement (OSSNR), *Rapport annuel de 2019 :* https://www.nsira-ossnr.gc.ca/wp-content/uploads/2020/12/AR-NSIRA-Fr-Final.pdf.
[2] *Loi sur l'Office de surveillance des activités en matière de sécurité nationale et de renseignement* (L.C. 2019, ch. 13, art. 2) (Loi sur l'OSSNR) https://laws-lois.justice.gc.ca/fra/lois/n-16.62/page-1.html

[3] Site Web de la Commission civile d'examen et de traitement des plaintes de la GRC : https://www.crcc-ccetp.gc.ca/fr

[4] Examens de l'OSSNR, https://nsira-ossnr.gc.ca/fr/reviews

[5]**Termes et définitions *:*** *Capacité* — Tout ce qui permet au SCRS de mener des opérations. Les capacités peuvent être technologiques ou techniques. Dans certains cas, plus d'une technologie ou technique peut produire une capacité. *Technique* — Une façon d'exécuter une tâche ou une opération particulière. *Technologie* — Équipement (matériel et logiciel) développé à partir de l'application de connaissances scientifiques.

[6] En mars 2022, le SCRS a indiqué que l'ensemble des politiques actualisées avait été publié le 17 décembre 2021.

[7] Loi sur l'OSSNR, paragraphe 8(2).

[8] La Loi sur le SCRS exige que le SCRS fournisse à l'OSSNR certains renseignements concernant les activités suivantes : mesures de réduction de la menace (article 12.1 (3.5)), ensembles de données (article 11.25), justification d'actes ou d'omissions qui constitueraient autrement une infraction (paragraphe 20.1 (26))), les activités illégales (paragraphe 20 (4)), les ententes de coopération (article 17), les directives ministérielles (paragraphe 6(2)) et le rapport du directeur du SCRS (paragraphe 6(4)).

[9] Dans la mesure du possible, les observations seront également incluses dans le rapport annuel public de l'OSSNR au Parlement.

[10] *Loi antiterroriste*, L.C. 2015, ch. 20.

[11] Les menaces à la sécurité nationale sont décrites à l'article 2 de la Loi sur le SCRS.

[12]. Rapport sur les événements liés à Maher Arar, Dossier factuel, vol. I, note 10. http://www.sirc-csars.gc.ca/pdfs/cm_arar_bgv1-fra.pdf

[13] Modifications apportées à la Loi sur le SCRS – Analytique des données, SCRS, 18 juillet 2020. https://www.canada.ca/fr/service-renseignement-securite/nouvelles/2020/06/modifications-apportees-a-la-loi-sur-le-scrs--analytique-des-donnees.html

[14] Pour de plus amples renseignements sur les exigences législatives du SCRS visant à fournir à l'OSSNR des renseignements sur les principales activités du SCRS, veuillez consulter la note de fin nº 8.

[15] En 2021, le SCRS a évalué quatre ensembles de données accessibles au public et en a retenu deux. Parmi les deux autres ensembles de données, il a été constaté que l'un d'entre eux avait été envoyé aux fins d'évaluation trop tard, alors il a été supprimé sans qu'aucun renseignement ne soit retenu. Il a été déterminé que l'ensemble de données restant était de nature administrative, ce qui fait en sorte qu'il n'était pas visé par l'article 11 de la Loi sur le SCRS.

[16] Les demandes visant à conserver les deux ensembles de données canadiens évalués par le SCRS en 2021 sont en attente de décisions de la Cour fédérale.

[17] En 2019, le SCRS a demandé l'autorisation ministérielle de conserver huit ensembles de données étrangères. Bien qu'aucun ensemble de données étrangères n'ait été évalué en 2021, un ensemble de données étrangères a été conservé après l'autorisation ministérielle (par le directeur désigné) et la ratification par le commissaire au renseignement, à la suite d'une demande présentée en 2019.

[18] Cadre de justification du SCRS. https://www.canada.ca/fr/service-renseignement-securite/nouvelles/2020/06/modifications-apportees-a-la-loi-sur-le-scrs--cadre-de-justification.html

[19] Le nombre de cas de non-conformité traités par le SCRS comprend les cas non conformes ainsi que les cas qui ont été jugés conformes après un examen par le SCRS.

[20] Le nombre total d'incidents de non-conformité n'a pas été ventilé en 2019 et en 2020. Ce nombre représente le nombre d'incidents de non-conformité aux exigences comme celles de la Loi sur le SCRS, de la Charte, des conditions des mandats ou des procédures et des politiques internes du SCRS.

[21] Examen sur la communication de renseignements canadiens d'identification (RCI) par le Centre de la sécurité des télécommunications (CST) (Examen de l'OSSNR 08-501-3).

[22] Conformément à l'article 35 de la Loi sur l'OSSNR, si, selon l'Office, une activité de sécurité nationale ou de renseignement menée par un ministère pourrait ne pas être conforme à la loi, l'OSSNR doit présenter un rapport de conformité au ministre responsable, avec une copie qui sera envoyée à l'administrateur général concerné. Le CST soutient qu'il a agi conformément à la loi.

[23] Conformément à l'article 31 de la Loi sur l'OSSNR, l'OSSNR peut ordonner à un ministère de mener une étude sur une activité afin de s'assurer que les activités d'un ministère sont conformes à la loi et aux directives ministérielles applicables et qu'elles sont raisonnables et nécessaires.

[24] L'article 43 de la Loi sur le CST exige que le CST veille à ce que les communications de RCI soient « essentielles aux affaires internationales, à la défense, à la sécurité ou à la cybersécurité ». Dans le cadre de cette étude ministérielle, le CST a examiné les communications à des ministères du gouvernement du Canada autres que le SCRS, la Gendarmerie royale du Canada (GRC) et l'Agence des services frontaliers du Canada (ASFC). Cette étude a également examiné toutes les communications à des partenaires étrangers.

[25]. L'infrastructure mondiale de l'information est définie dans la Loi sur le CST comme incluant les émissions électromagnétiques, tout équipement produisant de telles émissions, les systèmes de communication, les systèmes et les réseaux de technologie de l'information et toute donnée ou information technique transportée, contenus dans ces émissions, cet équipement, ces systèmes ou ces réseaux ou se rapportant à ces émissions.

[26] Dans le contexte de l'acquisition de renseignements par le CST, la collecte fortuite renvoie à de l'information qui n'a pas été délibérément recherchée et au fait que l'activité qui a permis l'acquisition de cette information ne visait pas un Canadien ou une personne se trouvant au Canada.

[27] Le « Groupe des cinq » renvoie aux ententes de coopération officielles entre les organismes du SIGINT des gouvernements du Canada, des États-Unis, du Royaume-Uni, de l'Australie et de la Nouvelle-Zélande.

[28] Le dossier des incidents liés à la protection des renseignements personnels est un registre des incidents attribuables au CST qui concernent des renseignements, au sujet d'un Canadien ou d'une personne se trouvant au Canada, qui ont été traités d'une manière qui va à l'encontre de la politique en vigueur ou qui n'y est pas prévue. Ce type d'erreur de traitement est qualifié d'« incident lié à la protection des renseignements personnels ».

[29] Le dossier des incidents de seconde partie est un registre des incidents liés à la protection des renseignements personnels ou à la conformité qui mettent en cause un Canadien ou une personne au Canada et qui sont attribuables à un partenaire secondaire ou à un partenaire domestique. Ces incidents peuvent être repérés par des partenaires ou par le CST. Ce type d'erreur de traitement est également qualifié d'« incident relatif à la protection de la vie privée ». Les partenaires secondaires sont les agences nationales de cryptologie d'Australie (Australian Signals Directorate), du Royaume-Uni (Government Communications Headquarters), de la Nouvelle-Zélande (Government Communications Security Bureau) et des États-Unis (National Security Agency).

[30] Le dossier d'erreurs de procédure mineures est un registre des incidents de conformité opérationnelle où le CST a traité de façon inappropriée des renseignements concernant un Canadien ou une personne se trouvant au Canada, mais où ces renseignements se trouvaient dans les bases de données du CST. Ce type d'erreur de traitement est qualifié d' « erreur de procédure ».

[31] Rapport annuel 2020 de l'OSSNR, section 1.5 « Faites confiance, mais vérifiez ».

[32] Les retards du CST dans le traitement des demandes de renseignements de l'OSSNR précèdent la pandémie de COVID-19. L'OSSNR a suivi les délais de réponse aux demandes d'information au moyen de notes de service internes, de feuilles de calcul et de notes d'information depuis sa création en août 2019.

[33] Comité des parlementaires sur la sécurité nationale et le renseignement, *Rapport annuel de 2019,* Shapitre 3 : Agence des services frontaliers du Canada. https://www.nsicop-cpsnr.ca/reports-rapports-fr.html

[34] Le terme « continuum frontalier » est utilisé ici pour désigner les activités et les processus associés au mouvement international des personnes, y compris les ressortissants étrangers qui viennent au Canada (demandeurs d'immigration, réfugiés et demandeurs d'asile) ainsi que les citoyens canadiens et les résidents permanents voyageant à l'étranger avec des documents de voyage délivrés par le Canada (p. ex., des passeports).

[35] Le syntagme « activité permanente » est utilisé pour désigner les activités entreprises dans le cadre de politiques et de programmes établis et permanents, par opposition aux activités entreprises dans le cadre de projets pilotes ou de développement avec des échéances définies.

[36] La limitation de la finalité consiste à énoncer explicitement l'objectif précis d'utilisation de données biométriques recueillies, tout en s'engageant à ne jamais les utiliser à d'autres fins ultérieurement.

[37] *Loi sur la communication d'information ayant trait à la sécurité du Canada* (LCISC), L.C. 2015, ch. 20, art. 2. https://laws.justice.gc.ca/fra/lois/s-6.9/. La LCISC est entrée en vigueur le 21 juin 2019. L'ancienne loi en la matière était en vigueur du 1er août 2015 au 20 juin 2019.

[38] LCISC, par. 5(1)

[39] LCISC, art. 5.1

[40] LCISC, al. 4c)

[41] En ce qui concerne la période d'examen de 2019, les 12 ministères et organismes ayant reçu des directives en vertu de la *Loi visant à éviter la complicité dans les cas de mauvais traitements infligés par des entités étrangères* étaient les suivants : l'Agence des services frontaliers du Canada, l'Agence du revenu du Canada, le Service canadien du renseignement de sécurité, le Centre de la sécurité des télécommunications, Pêches et Océans Canada, le ministère de la Défense nationale et les Forces armées canadiennes, le Centre d'analyse des opérations et déclarations financières du Canada, Affaires mondiales Canada, Immigration, Réfugiés et Citoyenneté Canada, Sécurité publique Canada, la Gendarmerie royale du Canada et Transports Canada.

[42] Loi sur l'OSSNR, alinéa 8(1)b)

[43] Appel à l'action en faveur de la lutte contre le racisme, de l'équité et de l'inclusion dans la fonction publique fédérale. https://www.canada.ca/fr/conseil-prive/organisation/greffier/appel-action-faveur-lutte-contre-racisme-equite-inclusion-fonction-publique-federale.html

[44] Il est à noter que, parfois, le travail sur les examens, y compris les demandes de renseignements, a commencé avant la finalisation du mandat.

[45] Dans le cas de certains examens, l'OSSNR n'a pas été en mesure de publier une partie ou la totalité de ces informations dans le rapport annuel de cette année. Les résumés complets de la plupart des examens dont il est question dans ce rapport annuel sont disponibles sur demande, s'ils ne sont pas déjà publiés sur le site Web de l'OSSNR (https://nsira-ossnr.gc.ca/fr/reviews) au moment de la publication du présent rapport.