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

Canada

OSSNR

2022 // Rapport Annuel

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

Le 29 septembre 2023

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 quatrième 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 2022 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 contient pas d'informations dont la communication porterait atteinte à la sécurité nationale, à la défense nationale ou aux relations internationales, ou bien des informations protégées par le secret professionnel de l'avocat ou du notaire ou par le privilège relatif au litige.

Je vous prie d'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) est fier de ce qu'il a accompli au cours de la dernière année. Nous avons surmonté les défis liés à la pandémie et poursuivi notre mission avec une énergie renouvelée et dans un esprit d'innovation réaffirmée, sachant que nous pouvons nous adapter, voire prospérer dans ce nouvel environnement. En 2022, notre organisme s'est attaché à mettre en place et à affiner ses processus afin de soutenir nos examinateurs et spécialistes en matière de plaintes dans l'accomplissement de leur travail. Ces efforts ont renforcé notre capacité à relever les défis rencontrés dans le cadre de nos mandats d'examen et d'enquête, et donc à améliorer la transparence et la responsabilisation des activités en matière de sécurité nationale et de renseignement de l'ensemble de l'administration fédérale.

Tout en menant à bien un large éventail d'examens et d'enquêtes, nous avons pris du recul pour réfléchir à notre travail et à nos activités au cours des premières années de notre mandat. Bien que notre organisme soit relativement nouveau, nous sommes désormais en mesure de formuler des observations plus générales sur les thèmes et les tendances de notre travail, ainsi que sur la communauté visée par nos examens. En effet, au fur et à mesure que nous acquérons de l'expérience, les approches que nous adoptons aux fins de nos examens et de nos enquêtes mûrissent et évoluent. Nous atteignons nos objectifs d'efficacité et d'expertise accrues en nous engageant à relever les défis auxquels nous sommes confrontés et en cherchant des pratiques exemplaires au moyen de partenariats élargis avec des institutions nationales et internationales ayant la même vocation que la nôtre.

Au cours de la brève histoire de l'OSSNR, les ministres de la Couronne nous ont renvoyé certaines questions pour examen, comme le prévoit la *Loi sur l'Office de surveillance des activités en matière de sécurité nationale et de renseignement*. Au moment de la rédaction du présent rapport, nous sommes en train de donner suite à un tel renvoi. Au fur et à mesure de l'avancement de cet important examen, nous veillerons à maintenir notre engagement envers l'indépendance et le professionnalisme de nos examens dans l'ensemble de nos activités.

Le présent rapport reprend les thèmes des rapports annuels précédents en présentant une vue d'ensemble de notre travail, une discussion sur la mobilisation des entités examinées et un compte rendu des initiatives que nous avons menées pour garantir que nos produits sont complets, exhaustifs et professionnels. Nous sommes convaincus qu'à mesure que nous nous développons, nous renforçons la confiance du public canadien grâce à chaque examen et enquête que nous menons.

Nous tenons à remercier nos anciens membres, Ian Holloway et Faisal Mirza, pour leur engagement et leur contribution à l'avancement des travaux importants de l'OSSNR au cours de leur mandat, et nous leur souhaitons beaucoup de succès dans leurs projets à venir. Enfin, nous remercions le personnel du Secrétariat de l'OSSNR pour son professionnalisme et son dévouement dans l'accomplissement du mandat de l'office, et nous sommes convaincus que l'année à venir sera marquée par de nouvelles réussites pour l'OSSNR.

Marie Deschamps Marie–Lucie Morin Foluke Laosebikan
Craig Forcese Matthew Cassar

Résumé

1. En 2022, l'Office de surveillance des activités en matière de sécurité nationale et de renseignement (OSSNR) a continué à exécuter ses mandats d'examen et d'enquête dans le but d'améliorer la responsabilisation et la transparence des activités en matière de sécurité nationale et de renseignement au Canada. Les examens et enquêtes ont visé non seulement les activités du Service canadien du renseignement de sécurité (SCRS) et du Centre de la sécurité des télécommunications (CST), mais aussi celles d'autres ministères et organismes fédéraux participant à de telles activités, notamment :

    - le ministère de la Défense nationale (MDN) et les Forces armées canadiennes (FAC);
    - l'Agence des services frontaliers du Canada (ASFC);
    - tous les ministères et organismes menant des activités en matière de sécurité nationale ou de renseignement dans le contexte des examens annuels de l'OSSNR au titre 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. L'OSSNR a réfléchi à son travail à ce jour et a constaté que l'adoption d'un point de vue horizontal à l'égard de toutes ses conclusions et recommandations au cours des trois dernières années révèle que trois thèmes majeurs se dégagent : la gouvernance, le bien-fondé ainsi que la gestion et le partage de l'information. L'OSSNR observe que ces questions sont interreliées et se chevauchent, et estime par conséquent que l'amélioration de la gouvernance pourrait entraîner des améliorations plus vastes dans tous les thèmes.

Examens

3. Les points saillants des examens terminés en 2022, ainsi que les principaux résultats, sont présentés ci-dessous-. Le nombre d'examens définis comme terminés ne comprend pas les examens en cours ni les examens terminés au cours des années précédentes, mais qui ont fait l'objet ou sont en train de faire l'objet de consultations en vue de leur diffusion au public. L'annexe C énumère toutes les conclusions et recommandations associées aux examens terminés en 2022, ainsi que les réponses correspondantes des entités examinées, si elles ont été fournies.

4. Outre les examens décrits ci-dessous-, l'OSSNR a décidé de mettre fin ou d'abandonner un certain nombre d'examens en cours. Ces décisions, fondées sur diverses considérations, permettent à l'OSSNR de réorienter ses efforts et ses ressources vers d'autres questions importantes.

Service canadien du renseignement de sécurité

5. Au cours de l'année 2022, l'OSSNR a réalisé les examens suivants portant sur les activités du SCRS :

    - le troisième examen annuel des mesures de réduction de la menace du SCRS, qui a fourni un aperçu de toutes les mesures de ce type prises en 2021, mais qui a également porté sur un sous-ensemble de ces mesures afin d'examiner la mise en œuvre de chaque mesure, l'adéquation entre ce qui s'est passé et ce qui avait été proposé, et, de manière connexe, le rôle des risques juridiques;
    - un examen annuel des activités du SCRS, qui a orienté, en partie, le rapport annuel 2022 de l'OSSNR au ministre de la Sécurité publique.

Centre de la sécurité des télécommunications

6. Au cours de l'année 2022, l'OSSNR a réalisé deux examens spécifiques portant sur le CST et a entamé un examen annuel des activités du CST :

    - un examen des cyberopérations actives (COA) et des cyberopérations défensives (COD), qui s'inscrit dans le prolongement de l'examen de la gouvernance des COA et COD par le CST et Affaires mondiales Canada, réalisé par l'OSSNR en 2021;
    - un examen d'un programme de nature sensible de collecte de renseignements étrangers du CST, qui a aidé l'OSSNR à mieux renseigner la ministre de la Défense nationale sur les activités du CST;
    - un examen annuel des activités du CST semblable à celui du SCRS, entamé pour la première fois en 2022 et qui a orienté, en partie, le rapport annuel 2022 de l'OSSNR au ministre de la Défense nationale.

Ministère de la Défense nationale et Forces armées canadiennes

7. Dans le cadre d'un examen des activités de gestion des sources humaines du ministère de la Défense nationale et des Forces armées canadiennes (MDN et FAC), l'OSSNR a produit à l'intention de la ministre de la Défense nationale un rapport le 9 décembre 2022, en vertu de l'article 35 de la *Loi sur l'Office de surveillance des activités en matière de sécurité nationale et de renseignement*, portant sur une activité spécifique. L'article 35 exige que l'OSSNR

présente au ministre compétent un rapport sur toute activité liée à la sécurité nationale ou au renseignement qui, de l'avis de l'OSSNR, pourrait ne pas être conforme à la loi. L'OSSNR terminera l'examen plus général des activités de gestion des sources humaines du MDN et des FAC en 2023.

Agence des services frontaliers du Canada

8. L'OSSNR a terminé son premier examen approfondi des activités de l'Agence des services frontaliers du Canada (ASFC) en matière de sécurité nationale ou de renseignement en 2022 : un examen du ciblage des passagers aériens. Cet examen a porté sur l'évaluation des risques que présentent les passagers avant leur arrivée, effectuée par l'ASFC en se fondant sur des données recueillies par les transporteurs aériens commerciaux. Il visait à évaluer si les activités de l'ASFC étaient conformes aux exigences législatives et aux obligations du Canada en matière de non-discrimination.

Examens multiministériels

9. En 2022, l'OSSNR a réalisé deux examens multiministériels obligatoires :

   - un examen des directives établies concernant la *Loi visant à éviter la complicité dans les cas de mauvais traitements infligés par des entités étrangères*;
   - un examen de la communication d'information au titre de la *Loi sur la communication d'information ayant trait à la sécurité du Canada*.

Travaux d'examen n'ayant pas donné lieu à un rapport final

10. Au cours de la dernière année, l'OSSNR a décidé de mettre fin certains travaux d'examen en cours ou de ne pas produire de rapport final à l'intention d'un ministre dans le cadre de certains examens. Ces décisions permettent à l'OSSNR de demeurer agile et de réorienter son plan de travail. Plusieurs considérations peuvent mener à la décision de fermer un examen. De telles décisions permettent à l'OSSNR de réorienter ses efforts et ressources.

Rôle de la technologie dans les examens

11. En 2022, l'OSSNR a élargi sa Direction de la technologie afin de suivre l'évolution de l'utilisation des technologies numériques par la communauté de la sécurité nationale et du renseignement. L'équipe est composée d'experts techniques et d'examinateurs, soutenus par des chercheurs universitaires. Cette équipe élargie a lancé le premier examen de l'OSSNR axé sur la technologie portant sur le cycle de vie de l'information obtenue dans le cadre des

mandats du SCRS. En plus de soutenir directement les examens de l'OSSNR, la Direction de la technologie a également commencé à organiser des séances d'apprentissage et des forums de discussion visant à améliorer les connaissances des employés de l'OSSNR sur des questions techniques d'ordre général.

Interaction avec les entités examinées

12. L'OSSNR continue d'examiner et d'améliorer certains aspects de ses interactions avec les entités examinées au cours du processus d'examen. Des améliorations et des difficultés constantes ont été relevées, et l'OSSNR s'efforce de fournir des évaluations complètes et transparentes à cet égard. Des critères mis à jour seront utilisés pour évaluer ses interactions. Ces critères sont essentiels pour soutenir les efforts de l'OSSNR pendant un examen. Cette approche s'appuie sur les précédents énoncés sur le niveau de confiance de l'office et fournit une évaluation plus cohérente et plus complète de ses interactions.

13. L'OSSNR poursuit l'optimisation de ses méthodes d'accès, de réception et de suivi de l'information nécessaire à la réalisation des examens. Des discussions avec les entités examinées et leur soutien continu sont nécessaires à cette fin. Les limites et les difficultés de ce processus sont abordées directement et communiquées publiquement dans la mesure du possible.

Enquêtes sur les plaintes

14. À l'aube de sa troisième année d'existence en 2022, l'OSSNR a continué à affiner et à moderniser les processus nécessaires à l'exécution de son mandat d'enquête. La phase d'évaluation de la compétence a été normalisée, en intégrant un protocole de vérification pour les trois organismes pour lesquels l'OSSNR est compétent en matière de plaintes. Afin d'accélérer le processus d'enquête, les entrevues d'enquête sont de plus en plus fréquentes et remplacent les audiences officielles que l'OSSNR utilisait auparavant.

15. La pandémie a continué d'avoir une incidence sur le déroulement des enquêtes au cours du premier semestre de 2022. Les protocoles liés à la COVID-19 entraient en conflit avec les protocoles de sécurité des enquêtes, qui exigent des rencontres en personne. Les procédures établies en 2022 devraient permettre de réduire les retards dans la réalisation des enquêtes à venir.

16. Le nombre d'activités d'enquête est demeuré élevé l'année dernière, notamment compte tenu de l'achèvement du renvoi d'un groupe de 58 plaintes par la Commission canadienne des droits de la personne.

17. Des initiatives lancées en matière de gestion des données et de normes de service devraient améliorer la gestion des dossiers de plainte au cours de l'année à venir.

Partenariats

18. Au cours de la dernière année, l'OSSNR a renforcé ses efforts de mobilisation auprès de ses précieux partenaires, tant à l'échelle nationale qu'internationale, et en a déjà récolté les fruits grâce à la mise en commun de pratiques exemplaires. En tant qu'office relativement nouveau, l'OSSNR considère ces relations comme une priorité pour son développement institutionnel. L'OSSNR a eu le privilège de rendre visite à de nombreux partenaires étrangers en tant que participant actif au Conseil de surveillance et d'examen du renseignement du Groupe des cinq, et a également mobilisé d'autres partenaires européens dans le cadre de divers forums qui rassemblent des organismes de surveillance, d'examen et de protection des données du monde entier ayant une optique commune.

01 //

Introduction

1.1 Qui sommes-nous

19. 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. Les organismes canadiens d'examen qui ont précédé l'OSSNR n'avaient pas la capacité de collaborer ou d'échanger leurs informations classifiées; ils pouvaient seulement effectuer des examens sur un ministère ou un organisme spécifique. En revanche, l'OSSNR a le pouvoir d'examiner de manière intégrée toutes les activités en matière de sécurité nationale et de renseignement du gouvernement du Canada, ce qui confère au Canada l'un des systèmes d'examen indépendant de la sécurité nationale les plus complets au monde.

1.2 Mandat

20. L'OSSNR a le double mandat de mener des examens et des enquêtes sur des plaintes en rapport avec les activités en matière de sécurité nationale ou de renseignement du Canada.

Examens

21. Le mandat d'examen de l'OSSNR est vaste, comme le stipule 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)[1]. Il 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 tous les autres ministères et organismes fédéraux. De plus, l'OSSNR examine toute question liée à la sécurité nationale ou au renseignement dont l'OSSNR est saisi par un ministre de la Couronne[2].

Enquêtes

22. 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.

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

02 //

Observations et thèmes

24. L'OSSNR bénéficie d'un point de vue horizontal et approfondi du milieu canadien de la sécurité nationale, ce qui lui permet d'évaluer l'approche complexe et interdépendante qu'adopte le Canada en matière de sécurité nationale. Les rapports annuels de l'OSSNR traitent de ses activités dans ce cadre. Le présent rapport annuel offre l'occasion de réfléchir horizontalement à l'ensemble des travaux de l'OSSNR et d'examiner les grandes tendances ou les thèmes qui en émergent.

25. Les conclusions et recommandations de l'OSSNR concernent de nombreux aspects des activités et des opérations du gouvernement. Le regroupement de toutes les conclusions et recommandations en fonction de sujets relevant de trois grands thèmes permet de simplifier l'évaluation horizontale des tendances observées à ce jour. Cette catégorisation et la terminologie utilisée peuvent évoluer au fil du temps.

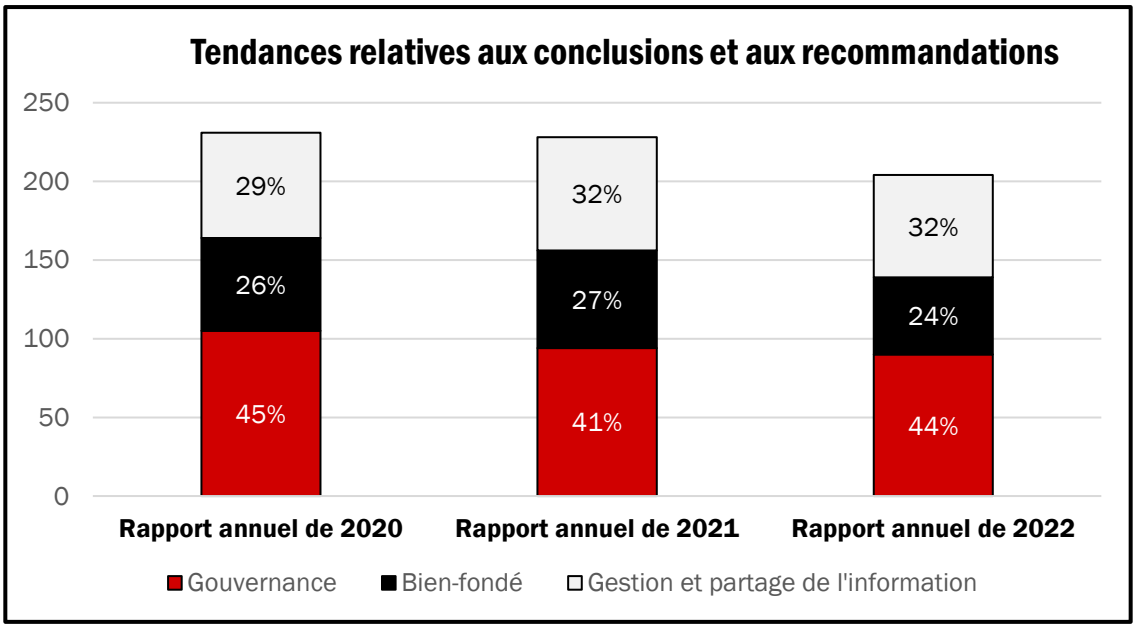
26. Les thèmes qui se dégagent sont la gouvernance, le bien-fondé, ainsi que la gestion et le partage de l'information. Ces thèmes apparaissent année après année dans les rapports annuels de l'OSSNR. Les sujets suivants s'inscrivent dans ces thèmes :

Thème	Sujets
Gouvernance	• Politiques, procédures, cadre et autres textes de référence • Surveillance à l'interne • Gestion des risques, évaluation et pratiques • Prise de décisions et responsabilisation, y compris la responsabilisation et l'orientation ministérielles • Formation, outils et ressources en personnel
Bien-fondé	• Raisonnabilité, nécessité, efficacité et proportionnalité • Seuils et conseils juridiques, conformité et protection de la vie privée
Gestion et partage de l'information	• Collecte, documentation, suivi, mise en œuvre, rapports, contrôle et protection • Partage et communication de l'information • Conserver et fournir en temps opportun de l'information exacte et à jour

27. Ces thèmes se retrouvent dans chaque rapport annuel de l'OSSNR, et celui de cette année ne fait pas exception. Dans le rapport annuel de cette année, les exemples suivants illustrent les trois thèmes :

- gouvernance :
    - l'examen des communications faites en vertu de la *Loi sur la communication d'information ayant trait à la sécurité du Canada* pour 2021 a révélé que les employés n'avaient pas reçu des directives adéquates pour s'acquitter de leurs obligations, et il a été recommandé d'apporter des améliorations à la formation;
    - l'examen d'une activité du CST en matière de renseignement étranger a révélé plusieurs cas d'activités de programme qui n'avaient pas été saisies adéquatement dans les demandes du CST visant certaines autorisations ministérielles, ce qui a mené à la recommandation au CST de renseigner plus efficacement le ministre de la Défense nationale sur certains aspects de ses relations bilatérales avec certains partenaires, l'étendue de sa participation à certains types d'activités, ainsi que la mise à l'essai et l'évaluation de produits.
- bien-fondé :
    - dans un rapport présenté à la ministre de la Défense nationale en vertu de l'article 35 de la Loi sur l'OSSNR, l'OSSNR a expliqué que, à son avis, certaines activités entreprises par les Forces armées canadiennes pouvaient ne pas être conformes à la loi;
    - l'examen des mesures de réduction de la menace du Service canadien du renseignement de sécurité a révélé que cet organisme n'avait pas respecté les exigences de sa politique interne concernant les échéances de présentation des rapports sur la mise en œuvre des mesures de réduction de la menace.
- gestion et partage de l'information :
    - l'examen du ciblage des passagers aériens par l'Agence des services frontaliers du Canada a révélé que cet agence ne documente pas ses pratiques de tri qui utilisent les données sur les passagers d'une manière qui permette de vérifier efficacement si toutes les décisions de tri sont conformes aux restrictions légales et réglementaires.

28. Une vue d'ensemble des trois derniers rapports annuels illustre le nombre de conclusions et de recommandations de l'OSSNR pour chaque année, séparées selon le thème. Au cours des trois années, les conclusions et recommandations relatives à la gouvernance ont représenté 43 % du nombre total de conclusions et recommandations. Les chiffres comparables pour les catégories du bien-fondé ainsi que de la gestion et de la mise en commun de l'information sont respectivement de 26 % et 31 %. Le tableau suivant présente la séparation selon l'année :



29. La nature interreliée des problèmes relevés dans les examens de l'OSSNR, ainsi que l'équilibre des thèmes illustrés dans le graphique ci-dessus, permet une interprétation. En effet, les problèmes sont rarement isolés – les problèmes liés à la gouvernance ainsi qu'à la gestion et au partage de l'information peuvent, par exemple, aboutir à des problèmes de bien-fondé. Le nombre de conclusions et de recommandations formulées en trois ans sur la gouvernance, le bien-fondé de même que la gestion et le partage de l'information montre qu'il s'agit de questions qui méritent une attention particulière. Il est attendu que les employés mènent avec succès les missions relatives aux services de renseignement et de sécurité nationale tout en respectant les politiques et exigences légales. Les améliorations apportées à la formation et au perfectionnement du personnel à cet égard sont susceptibles d'avoir les effets les plus importants.

03 //

Examens

30. Les détails fournis sur les examens individuels constituent un résumé général de leur contenu et de leurs résultats. Les versions complètes de chaque examen sont disponibles après qu'elles ont été expurgées pour être rendues publiques.

3.1 Examens visant le Service canadien du renseignement de sécurité

Aperçu

31. L'OSSNR a pour mandat d'examiner toute activité du Service canadien du renseignement de sécurité (SCRS). En vertu de la *Loi sur l'Office de surveillance des activités en matière de sécurité nationale et de renseignement* (Loi sur l'OSSNR), l'OSSNR doit également présenter chaque année un rapport annuel sur les activités du SCRS au ministre de la Sécurité publique et de la Protection civile (puisque ces responsabilités sont maintenant réparties entre deux portefeuilles, l'OSSNR présente actuellement ces rapports au ministre de la Sécurité publique). Ces rapports classifiés contiennent de l'information sur le respect par le SCRS de la loi et des directives ministérielles applicables, ainsi que sur le caractère raisonnable et la nécessité de l'exercice par le SCRS de ses pouvoirs.

32. En 2022, l'OSSNR a réalisé un examen spécifique portant sur le SCRS ainsi que son rapport annuel sur les activités du SCRS tous deux résumés ci-dessous. De plus, le SCRS participe à d'autres examens multiministériels 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 dans la section Examens multiministériels.

Examen des mesures de réduction de la menace

33. Il s'agit du troisième examen annuel par l'OSSNR des mesures de réduction de la menace (MRM) du SCRS, qui sont des mesures visant à réduire les menaces à la sécurité du Canada, à

l'intérieur ou à l'extérieur du Canada[4]. L'article 12.1 de la *Loi sur le Service canadien du renseignement de sécurité* (Loi sur le SCRS) autorise le SCRS à prendre de telles mesures.

34. L'OSSNR a constaté que les activités du SCRS dans le cadre de son mandat concernant les MRM en 2021 étaient essentiellement conformes aux activités de même type des années précédentes. L'OSSNR a observé que 2018 a constitué un point d'inflexion pour l'utilisation par le SCRS du mandat concernant les MRM. Au cours de cette année, le SCRS a proposé presque autant de MRM qu'au cours de l'ensemble des trois années précédentes – les trois premières années du mandat. Cependant, au cours de l'année suivante, le nombre a légèrement diminué, puis a connu une réduction plus importante en 2020. Le nombre de MRM proposées en 2021 a légèrement augmenté par rapport à l'année précédente, de même que le nombre d'approbations et de mises en œuvre.

35. L'OSSNR a choisi trois MRM mises en œuvre en 2021 à des fins d'examen plus approfondi, et a évalué la conformité des mesures avec les lois applicables, les instructions ministérielles et les politiques. Parallèlement, l'OSSNR a examiné la mise en œuvre de chaque mesure, y compris la concordance entre ce qui avait été proposé et ce qui s'est produit, et le rôle des évaluations des risques juridiques pour guider les activités du SCRS, ainsi que la documentation des résultats.

36. Pour toutes les mesures examinées, l'OSSNR a constaté que le SCRS avait rempli ses obligations en vertu de la loi, en particulier la *Charte canadienne des droits et libertés* et les articles 12.1 et 12.2 de la Loi sur le SCRS. Outre la conformité juridique générale, l'OSSNR a constaté que le SCRS avait suffisamment établi un « lien rationnel » entre la mesure proposée et la menace cernée.

37. Dans un cas, l'OSSNR a constaté que le SCRS n'avait pas rempli ses obligations en vertu des instructions du ministre sur les opérations et la reddition de comptes de 2015 et des instructions du ministre de 2019 concernant la reddition de comptes émises par le ministre de la Sécurité publique.

38. La MRM en question comportait certains facteurs de nature sensible. L'OSSNR estime que la présence de ces facteurs aurait dû être prise en compte dans l'évaluation globale des risques liés à la mesure. Le SCRS a fait valoir que les risques associés à ces facteurs sont principalement liés au risque d'atteinte à la réputation du SCRS, qu'il a évalué dans ce cas. Toutefois, certains risques liés aux facteurs de nature sensible ne sont pas, et en l'occurrence n'ont pas été, pris en compte dans l'évaluation du risque d'atteinte à la réputation du SCRS.

39. De même, l'évaluation des risques juridiques pour cette MRM n'était pas conforme aux instructions ministérielles. L'OSSNR a recommandé que des évaluations des risques juridiques soient effectuées pour les MRM comportant ces facteurs de nature sensible et, en outre, que le SCRS examine et évalue si le processus actuel d'évaluation des risques juridiques est conforme aux instructions ministérielles applicables.

40. Une analyse comparative des deux évaluations des risques juridiques fournies pour les autres MRM examinées a révélé l'utilité pratique de la fourniture d'instructions juridiques claires et précises au personnel du SCRS. Des instructions claires permettent aux enquêteurs de connaître et de comprendre les paramètres juridiques dans le cadre desquels le personnel du SCRS peut mener ses activités; elles permettent également de rendre des comptes, une fois la mesure prise, sur le respect des limites de ces paramètres juridiques lors de la mise en œuvre.

41. En ce qui concerne la documentation des résultats, l'OSSNR a également relevé des problèmes liés à la rapidité avec laquelle le SCRS produit certains rapports après la mise en œuvre d'une MRM. Bien que l'OSSNR reconnaisse que des exigences trop lourdes en matière de documentation peuvent indûment entraver les activités du SCRS, il estime néanmoins que les recommandations formulées sont prudentes et raisonnables. Disposer d'informations pertinentes, disponibles en temps opportun, est avantageux pour les activités du SCRS.

Examen annuel des activités du Service canadien du renseignement de sécurité

42. En 2022, l'OSSNR a réalisé son examen annuel des activités du SCRS, qui vise à cerner les défis liés à la conformité, les tendances générales et les nouveaux problèmes en utilisant les documents du SCRS dans 12 catégories (exigées par la loi et supplémentaires) du 1er janvier 2022 au 31 décembre 2022. En plus de contribuer au rapport annuel de l'OSSNR au ministre de la Sécurité publique sur les activités du SCRS, l'examen peut permettre de cerner des domaines qui méritent de faire l'objet de nouveaux examens par l'OSSNR, et une séance d'information ou un rapport en contenant les observations, conclusions et recommandations peut être élaboré. L'OSSNR a présenté son rapport sur les activités du SCRS en 2021 au ministre de la Sécurité publique le 12 octobre 2022. La présidente a ensuite rencontré le ministre pour discuter du contenu de ce rapport ainsi que des enjeux et défis en cours liés à l'examen du SCRS par l'OSSNR.

Statistiques et données

43. Pour accroître la responsabilisation à l'égard du public, l'OSSNR a demandé 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 de mandat

44. 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 de l'information, des dossiers ou des documents. Il convient de noter que chaque demande de mandat peut viser plusieurs personnes ou concerner l'utilisation de multiples pouvoirs d'intrusion[5].

Tableau 1 : Demandes de mandat en vertu de l'article 21 présentées par le Service canadien du renseignement de sécurité (de 2018 à 2022)

	2018	2019	2020	2021	2022
Nombre total de demandes en vertu de l'article 21	24	24	15	31	28
Nombre total de mandants approuvés	24	23	15	31	28
Nouveaux mandants	10	9	2	13	6
Demandes de remplacement	11	12	8	14	14
Demandes supplémentaires	3	2	5	4	8
Nombre total de demandes de mandat rejetées	0	1	0	0	0

Mesures de réduction de la menace

45. Le SCRS est autorisé à demander un mandat judiciaire pour une MRM 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. La Loi sur le SCRS indique clairement que si une MRM proposée limite un droit ou une liberté protégés par la *Charte canadienne des droits et libertés* ou est contraire aux lois canadiennes, un mandat judiciaire autorisant la mesure est nécessaire. À ce jour, le SCRS n'a demandé aucune autorisation judiciaire pour entreprendre des MRM dans le cadre d'un mandat. Les MRM approuvées au cours d'une année peuvent être exécutées au cours des années suivantes. Des motifs opérationnels peuvent également empêcher l'exécution d'une MRM approuvée.

Tableau 2 : Nombre total de mesures de réduction de la menace approuvées et exécutées (de 2015 à 2022)

	2015	2016	2017	2018	2019	2020	2021	2022
Mesures de réduction de la menace approuvées	10	8	15	23	24	11	23	16
Mesures de réduction de la menace exécutées	10	8	13	17	19	8	17	12
Mesures de réduction de la menace dans le cadre d'un mandat	0	0	0	0	0	0	0	0

Cibles du Service canadien du renseignement de sécurité

46. 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[6]. 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 entités faisant l'objet d'une enquête du SCRS, qu'il s'agisse de personnes ou de groupes, sont appelées des « cibles[7] ».

Tableau 3 : Nombre de cibles du Service canadien du renseignement de sécurité (de 2018 à 2022)

	2018	2019	2020	2021	2022
Nombre de cibles	430	467	360	352	340

Ensembles de données

47. 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*, qui est entrée en vigueur en 2019, a accordé au SCRS 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 à exercer 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 responsabilisation ministérielle. Le SCRS doit satisfaire à différentes exigences avant de pouvoir utiliser certains types d'ensemble de données[8].

48. 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 du traitement d'ensembles de données doivent être fournis à l'OSSNR, sous certaines conditions et dans des délais raisonnables. 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.

Tableau 4 : Évaluation et conservation d'ensembles de données accessibles au public, d'ensembles de données canadiens et d'ensembles de données étrangers par le Service canadien du renseignement de sécurité (de 2019 à 2022)

	2019	2020	2021	2022
Ensembles de données accessibles au public				
Évalués	9	6	4	4
Conservés	9	6	2[a]	4
Ensembles de données canadiens				
Évalués	0	0	2	0
Conservés (approuvés par la Cour fédérale)	0	0	0	2[b]
Refusés par la Cour fédérale	0	0	0	0
Ensembles de données étrangers				
Évalués	10	0	0	1
Conservés (approuvés par le ministre et le commissaire au renseignement)	0	1	1[c]	1
Refusés par le ministre	0	0	0	0
Refusés par le commissaire au renseignement	0	0	0	0

Remarque : les statistiques présentées dans ce tableau sont à jour en date de mai 2023. Les statistiques des rapports annuels précédents ont été mises à jour pour tenir compte des nouvelles données reçues.

[a] En 2021, le SCRS a évalué quatre ensembles de données accessibles au public et en a conservé 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'aucune information ne soit conservée. 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.

[b] Les ensembles de données recueillis et évalués en 2021 ont reçu une autorisation judiciaire et ont donc été conservés en 2022.

[c] En 2019, le SCRS a demandé l'autorisation ministérielle de conserver huit ensembles de données étrangers. Bien qu'aucun ensemble de données étranger n'ait été évalué en 2021, un ensemble de données étranger a été conservé

après autorisation ministérielle (par le directeur désigné) et ratification par le commissaire au renseignement, à la suite d'une demande présentée en 2019.

Cadre de justification

49. 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 qui autorise les employés du SCRS et les personnes agissant sous leur direction à mener des activités qui constitueraient par ailleurs des infractions aux lois canadiennes. Le cadre de justification du SCRS est inspiré des protections dont bénéficient déjà les services canadiens d'application de la loi[9]. Le cadre de justification apporte au SCRS et à la population canadienne 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 public de veiller à ce que les employés du SCRS puissent s'acquitter efficacement de leurs fonctions de collecte de renseignements, notamment par la commission d'actes et d'omissions qui seraient par ailleurs illégaux, dans l'intérêt du public et conformément à la primauté du droit. Les types d'actes et d'omissions par ailleurs illégaux qui sont autorisés par le cadre de justification sont déterminés par le ministre et approuvés par le commissaire au renseignement. Il existe des limites quant aux activités qui peuvent être réalisées, et le cadre de justification ne permet pas de commettre un acte ou une omission qui porterait atteinte à un droit ou à une liberté garantis par la Charte.

50. Selon le paragraphe 20.1(2) de la Loi sur le SCRS, les employés doivent être désignés par le ministre de la Sécurité publique et de la Protection civile pour être visés par le cadre de justification lorsqu'ils commettent un acte ou une omission par ailleurs illégal ou en ordonnent la commission. Les employés désignés sont des employés du SCRS qui ont besoin du cadre de justification pour exécuter 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.

Tableau 5 : Autorisations, commissions et directives en vertu du cadre de justification (de 2019 à 2022)

	2019	2020	2021	2022
Autorisations	83	147	178	172
Commissions par les employés	17	39	51	61
Directives de commettre	32	84	116	131

Désignations en situation d'urgence	0	0	0	0

Conformité

51. L'unité du 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 dirigeant une approche pour signaler et évaluer les incidents potentiels de non-conformité, et à fournir aux employés des conseils et des directives en temps opportun sur les politiques et procédures internes. Ce programme constitue le centre de traitement de tous les cas de non-conformité liés aux activités opérationnelles.

52. L'OSSNR note que le SCRS signale des infractions à la Charte comme des cas de non-conformité opérationnelle. L'OSSNR continuera de surveiller de près les cas de non-conformités canadiennes et à la Charte, et collaborera avec le SCRS pour améliorer la transparence quant à ces activités.

Tableau 6 : Nombre total d'incidents de non-conformité traités par le SCRS (de 2019 à 2022)

	2019	2020	2021	2022
Incidents de non-conformité traités[a]	53	99	85	59
Incidents administratifs		53	64	42
Incidents opérationnels[b]	40[c]	19[c]	21	17
Lois canadiennes	–	–	1	2
Charte	–	–	6	5
Conditions des mandats	–	–	6	3
Gouvernance du SCRS	–	–	8	15

[a] 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.

[b] Pour 2021, chaque incident de non-conformité opérationnel a été comptabilisé en fonction de l'échelon de non-conformité (c.-à-d. qu'un incident de non-conformité à la Charte et à la gouvernance du SCRS n'est comptabilisé que dans la catégorie Charte). Pour 2022, chaque incident est comptabilisé dans toutes les catégories dans lesquelles il y a eu non-conformité. Ainsi, la somme des incidents de non-conformité opérationnels dans les différentes catégories est plus élevée que le nombre total d'incidents de ce type, soit 17.

[c] 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 comme celles de la Loi sur le SCRS, de la Charte, des conditions des mandats ou des procédures et politiques internes du SCRS.

3.2 Examens visant le Centre de la sécurité des télécommunications

Aperçu

53. L'OSSNR a pour mandat d'examiner toute activité menée par le Centre de la sécurité des télécommunications (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 l'évaluation par l'OSSNR du caractère raisonnable et de la nécessité de l'exercice des pouvoirs du CST.

54. En 2022, l'OSSNR a effectué deux examens visant le CST et a entrepris un examen annuel des activités du CST, tous sont résumés ci-dessous. De plus, le CST participe à d'autres examens multiministériels 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*. Les résultats de ces examens sont décrits dans la section Examens multiministériels.

Examen des cyberopérations actives et des cyberopérations défensives du Centre de la sécurité des télécommunications

55. 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). Les COA et les COD du CST sont devenues un outil en matière de politique étrangère et de sécurité pour le gouvernement du Canada. En 2021, l'OSSNR a examiné la gouvernance par le CST des COA et des COD ainsi que le processus général de planification et d'approbation des activités liées aux COA et aux COD[10]. L'examen de la gouvernance a permis de formuler plusieurs observations sur la gouvernance des COA et des COD par le CST et, dans une moindre mesure, par Affaires mondiales Canada (AMC). Certaines de ces observations ont permis de relever des lacunes qui ont donné lieu à des recommandations. S'appuyant sur l'examen de la gouvernance, le rapport était axé sur les COA et les COD du CST elles-mêmes :

- les opérations;
- la mise en œuvre de la gouvernance du CST;
- le cadre juridique dans le contexte de COA et de COD spécifiques.

56. L'OSSNR a intégré dans cet examen AMC, le SCRS, la Gendarmerie royale du Canada (GRC) ainsi que le ministère de la Défense nationale (MDN) et les Forces armées canadiennes (FAC) en raison des divers degrés de coordination ou de participation de ces organisations en ce qui concerne ces activités du CST. L'OSSNR a également inspecté certains éléments techniques d'une étude de cas de COA afin de vérifier certains aspects de l'opération de manière indépendante et d'approfondir sa compréhension du fonctionnement d'une COA. Bien que l'OSSNR ait examiné toutes les COA et COD planifiées ou menées par le CST jusqu'à la

mi-2021, l'examen a essentiellement porté sur un échantillon de ces COA ou COD, chacune présentant des caractéristiques particulières.

57. Dans l'ensemble, l'OSSNR a constaté que les COA et les COD planifiées ou réalisées par le CST au cours de la période d'examen étaient légales, et a constaté des améliorations dans les évaluations d'AMC en ce qui concerne les risques sur le plan de la politique étrangère et le droit international. L'OSSNR a également observé que le CST avait développé et amélioré ses processus de planification et de réalisation des COA et des COD conformément à certaines des observations de l'OSSNR formulées lors de l'examen de la gouvernance.

58. L'OSSNR a également formulé des conclusions sur la manière dont le CST pourrait améliorer certains aspects de la planification des COA et des COD, ainsi que la communication avec le ministre de la Défense nationale et la coordination avec d'autres entités du gouvernement du Canada. Plus précisément, l'OSSNR a cerné de possibles domaines de risque :

- la capacité d'AMC à évaluer de manière indépendante les risques potentiels découlant des COA et des COD du CST;
- l'exactitude de l'information fournie et les problèmes liés à la délégation, en ce qui a trait à certaines des demandes d'autorisation pour les COA et les COD;
- le degré de collaboration du CST avec le SCRS et la GRC par rapport aux COA et aux COD, et les explications du CST sur la manière dont il a déterminé que l'objectif d'une COA ou d'une COD ne pourrait raisonnablement pas être atteint par d'autres moyens;
- la mesure dans laquelle le CST a décrit la collecte de renseignements susceptible d'être effectuée parallèlement aux COA ou aux COD ou en raison de celles-ci dans les demandes d'autorisation des COA et COD et dans la documentation opérationnelle;
- le chevauchement entre les activités menées dans le cadre des volets COA et COD du mandat du CST, ainsi qu'entre les quatre volets du mandat du CST.

59. Il convient de noter que l'OSSNR a été confronté à d'importantes difficultés d'accès à l'information du CST dans le cadre de cet examen. Ces difficultés d'accès ont eu une incidence négative sur l'examen. En conséquence, l'OSSNR n'était pas en mesure de se fier à l'exhaustivité de l'information fournie par le CST.

Examen d'une activité en matière de renseignement étranger

60. En 2022, l'OSSNR a réalisé un examen d'un programme de nature sensible de collecte de renseignements étrangers du CST. Au cours de l'examen, l'OSSNR a formulé plusieurs constatations et observations concernant les activités menées dans le cadre de ce programme. L'OSSNR a notamment relevé plusieurs cas où les activités du programme n'étaient pas bien indiquées dans les demandes du CST visant certaines autorisations ministérielles. L'OSSNR a donc recommandé au CST de renseigner plus efficacement le ministre de la Défense nationale sur certains aspects de ses relations bilatérales avec certains partenaires, l'étendue de sa participation à certains types d'activités, ainsi que la mise à l'essai et l'évaluation de produits.

61. L'OSSNR a également constaté que dans plusieurs domaines, le programme ne disposait pas de structures de gouvernance adéquates, ce qui se traduit par une mauvaise application d'exigences clés en matière de politique et de procédure liées à l'échange d'information, à la confirmation du caractère étranger et au processus d'évaluation des risques de mauvais traitements du CST. L'OSSNR a formulé des recommandations visant à renforcer ces processus, à établir des structures de gouvernance propres au programme et à améliorer les autres structures de gouvernance qui s'appliquent de façon générale à l'ensemble du CST.

Examen annuel des activités du Centre de la sécurité des télécommunications

62. En 2022, l'OSSNR a lancé l'examen annuel des activités du CST, qui visait à cerner les défis liés à la conformité, les tendances générales et les nouveaux problèmes en utilisant les documents du CST dans 11 catégories (exigées par la loi et supplémentaires) du 1er janvier 2022 au 31 décembre 2022. En plus de contribuer au rapport annuel de l'OSSNR au ministre de la Défense nationale sur les activités du CST, l'examen peut permettre de cerner des aspects qui méritent de faire l'objet de nouveaux examens par l'OSSNR, ainsi que d'élaborer une séance d'information ou un rapport en contenant les observations, conclusions et recommandations. Il s'inspire largement de la structure de l'examen annuel des activités du SCRS, mais a été adapté au CST. La présidente de l'OSSNR a rencontré la ministre de la Défense nationale le 15 décembre 2022 pour discuter des enjeux et défis en cours liés aux examens des activités du CST par l'OSSNR.

Statistiques et données

63. Pour accroître la responsabilisation et la transparence, l'OSSNR a demandé au CST de lui fournir des statistiques et des données sur les aspects de ses activités liés à l'intérêt public et à la conformité. L'OSSNR est d'avis que ces statistiques permettront de fournir au public de l'information importante 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

64. Les autorisations ministérielles sont délivrées au CST par le ministre de la Défense nationale. Ces autorisations appuient les activités précises liées au renseignement étranger ou à la cybersécurité, ou des cyberopérations défensives ou actives menées par le CST conformément aux volets de son mandat. Les autorisations sont délivrées lorsque ces activités pourraient autrement contrevenir à une loi du Parlement ou compromettre l'attente raisonnable en matière de respect de la vie privée d'un Canadien ou d'une personne se trouvant au Canada.

Tableau 7 : Autorisations ministérielles délivrées (de 2019 à 2022)

Type d'autorisation ministérielle	Article habilitant de la Loi sur le CST	Délivrées en 2019	Délivrées en 2020	Délivrées en 2021	Délivrées en 2022
Renseignement étranger	26(1)	3	3	3	3
Cybersécurité – infrastructures fédérales et non fédérales	27(1) et 27(2)	2	1	2	3
Cyberopérations défensives	29(1)	1	1	1	1
Cyberopérations actives	30(1)	1	1	2	3

Remarque : Le tableau présente les 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 2021 et est demeurée en vigueur pendant une partie de 2022, elle est comptée uniquement comme une autorisation ministérielle de 2021.

65. Les arrêtés ministériels sont délivrés par le ministre pour 1) désigner comme étant importantes pour le gouvernement fédéral de l'information électronique, des infrastructures de l'information ou des catégories d'information électronique ou d'infrastructures de l'information [article 21(1) de la Loi sur le CST]; ou 2) désigner des destinataires de l'information qui se

rapporte à des Canadiens ou à des personnes se trouvant au Canada, c'est-à--dire de l'information nominative sur un Canadien [articles 45 et 44(1) de la Loi sur le CST].

Tableau 8 : Arrêtés ministériels en vigueur en 2022

Nom de l'arrêté ministériel [traduction]	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.	21(1)
Désignation des destinataires de l'information qui se rapporte à un Canadien ou à une personne se trouvant au Canada qui a été acquise, utilisée ou analysée dans le cadre des volets du mandat du CST touchant la cybersécurité et l'assurance de l'information.	45 et 44(1)
Désignation des destinataires de l'information nominative sur un Canadien utilisée, analysée ou conservée au titre d'une autorisation touchant le renseignement étranger en vertu de l'article 45 de la Loi sur le CST.	45 et 43
Désignation de l'information électronique et des infrastructures de l'Ukraine comme étant des systèmes d'importance.	21(1)
Désignation de l'information électronique et des infrastructures de la Lettonie comme étant des systèmes d'importance.	21(1)

Remarque : Les arrêtés ministériels demeurent en vigueur jusqu'à ce qu'ils soient annulés par le ministre.

Rapports sur le renseignement étranger

66. 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. Au sens de la Loi sur le CST, l'infrastructure mondiale de l'information est ainsi définie : « [v]ise notamment les émissions électromagnétiques et tout équipement produisant de telles émissions, les systèmes de communication, les systèmes et réseaux des technologies de l'information ainsi que les données et les renseignements techniques qu'ils transportent, qui s'y trouvent ou qui les concernent. » Le CST utilise, analyse et diffuse l'information dans le but de fournir des renseignements étrangers, en conformité avec les priorités du gouvernement fédéral en matière de renseignement.

Tableau 9 : Nombre de rapports sur le renseignement étranger produits (de 2019 à 2022)

Rapports sur le renseignement étranger du CST	2019	2020	2021	2022
Nombre de rapports produits	S.O.	S.O.	3 050	3 185
Nombre de ministères et organismes	S.O.	>25	28	26
Nombre de clients précis au sein des ministères et organismes	S.O.	>2 100	1 627	1 761

Remarque: L'OSSNR n'a pas demandé au CST de statistiques concernant les rapports sur le renseignement étranger pour son rapport public annuel de 2019. En 2020, des statistiques ont été demandées, mais les statistiques fournies étaient de nature générale en raison de la classification des données à l'époque, et le CST a indiqué que la publication de détails supplémentaires porterait atteinte à la sécurité nationale.

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

67. L'information qui se rapporte à un Canadien ou à une personne se trouvant au Canada (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 au titre d'une autorisation ministérielle. La collecte fortuite renvoie à de l'information qui n'était pas délibérément recherchée par le CST 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. Selon la politique du CST, l'IRCPC constitue toute information reconnue comme se rapportant 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.

68. L'OSSNR 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] « cette information demeure classifiée. Nous avons déterminé que la communication de cette information pourrait porter atteinte aux relations internationales, à la défense nationale et à la sécurité nationale du Canada. De plus, la communication de cette information fournirait un niveau de détail supplémentaire sur la réussite des programmes de collecte canadiens, notre niveau de dépendance à l'égard de l'information provenant de partenaires du Groupe des cinq pour produire du renseignement, ainsi qu'un niveau de détail sur l'utilisation du Groupe des cinq et les rapports connexes pour la collecte canadienne qui n'ont pas encore été rendus publics. »

Information nominative sur un Canadien

69. Il est interdit au CST de cibler des Canadiens ou des personnes se trouvant au Canada dans le cadre de ses activités. Toutefois, en raison des méthodes de collecte du CST, de telles informations peuvent parfois être recueillies incidemment. Lorsque ces informations recueillies incidemment sont utilisées dans un rapport sur le renseignement étranger du CST, toute partie susceptible d'identifier un Canadien ou une personne se trouvant au Canada est supprimée afin de protéger la vie privée des personnes en question. Le CST peut communiquer l'information nominative sur un Canadien (INC) non supprimée 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).

Tableau 10 : Nombre de demandes de communication d'INC (2021 et 2022)

Type de demande	2021	2022
Demandes du gouvernement du Canada	741	657
Demandes du Groupe des cinq	90	62
Demandes d'organismes ne faisant pas partie du Groupe des cinq	0	0
Total	831	719

70. En 2022, sur les 719 demandes qui ont été reçues, le CST a indiqué avoir rejeté 65 demandes. À la fin de l'année, 51 demandes étaient toujours en cours de traitement.

71. L'OSSNR a également demandé au CST de publier le nombre de cas où de l'INC a été supprimée de rapports sur la cybersécurité ou le renseignement étranger du CST. Le CST a répondu que [traduction] « la communication du nombre de cas où de l'INC a été supprimée de rapports sur le renseignement du CST porterait atteinte aux capacités du CST. Une telle communication révélerait de l'information sur les capacités du CST, y compris sur ses limites. L'information pourrait ainsi être utilisée dans le cadre de menaces hostiles envers la sécurité pour contrer les capacités du CST, ce qui empêcherait ce dernier de protéger le Canada et ses citoyens. »

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

72. 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 compromise 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[11] et, pour les incidents liés à la protection des renseignements personnels attribuables à un partenaire secondaire ou à un partenaire national, de son dossier des incidents liés à la protection des renseignements personnels de seconde partie.

Tableau 11 : Nombre d'incidents liés à la protection des renseignements personnels saisis par le CST (2021 et 2022)

Type d'incident	2021	2022
Incidents liés à la protection des renseignements personnels	96	114
Incidents liés à la protection des renseignements personnels de seconde partie	33	23

Cybersécurité et assurance de l'information

73. 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 celles des entités non fédérales désignées par le ministre comme étant d'importance pour le gouvernement fédéral.

74. Le Centre canadien pour la cybersécurité (CCC) est l'autorité canadienne unifiée en matière de cybersécurité. Le CCC, qui fait partie du CST, offre une orientation, des services et une formation spécialisés, tout en travaillant en collaboration avec les intervenants des secteurs privé et public. Le CCC traite les incidents survenus au sein du gouvernement et des institutions désignées, notamment les types d'incidents qui comprennent ce qui suit :

- les activités de reconnaissance menées par des auteurs de menace dotés de techniques sophistiquées;
- les incidents d'hameçonnage, soit les courriels contenant des maliciels;
- les accès non autorisés à des environnements de technologie de l'information (TI) organisationnels;

- les attaques imminentes par rançongiciel;
- les exploits du jour zéro (exploitation de vulnérabilités critiques dans des logiciels n'ayant pas fait l'objet de correctifs).

Tableau 12 : Nombre de dossiers de cyberincident ouverts par le CST (2022)

Type de cyberincident	2022
Institutions fédérales	1 070
Infrastructures essentielles	1 575
Total	2 645

Cyberopérations actives et défensives

75. 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 celles des entités non fédérales désignées par le ministre comme étant d'importance pour le gouvernement fédéral contre les cyberattaques hostiles.

76. 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.

77. L'OSSNR a demandé au CST de publier le nombre de COD et de COA approuvées et le nombre de COD et de COA menées en 2022. 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

78. Dans le cadre du volet du mandat du CST touchant l'assistance technique et opérationnelle, le CST reçoit des demandes d'assistance d'organismes canadiens chargés de l'application de la loi et de la sécurité de même que de la part du ministère de la Défense nationale et des Forces armées canadiennes[12].

Tableau 13 : Nombre de demandes d'assistance que le CST a reçues et auxquelles il a donné suite (de 2020 à 2022)

	2020	2021	2022
Approuvées	23	32	59
Non approuvées	1	3	S.O.
Annulées	Non disponible	Non disponible	1
Refusées	Non disponible	Non disponible	2
Nombre total de demandes reçues	24	35	62

Remarque : Pour 2020 et 2021, le CST n'a pu fournir que le nombre de demandes reçues et auxquelles il a donné suite. Le CST a toutefois indiqué qu'il a depuis amélioré son système de suivi interne des demandes d'assistance. Pour 2022, le CST était désormais en mesure de fournir le nombre de demandes d'assistance approuvées, refusées ou annulées.

3.3 Autres ministères

Aperçu

79. Outre les examens visant le SCRS et le CST mentionnés ci-dessus, l'OSSNR a réalisé les examens suivants auprès de ministères et organismes en 2022 :

- un examen du ministère de la Défense nationale et des Forces armées canadiennes;
- un examen de l'Agence des services frontaliers du Canada;
- les examens annuels par l'OSSNR 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*, auxquels participent davantage de ministères et d'organismes qui font partie de l'appareil de la sécurité nationale et du renseignement du Canada.

Ministère de la Défense nationale et Forces armées canadiennes

Rapport en vertu de l'article 35 de la Loi sur l'OSSNR

80. Dans le cadre d'un examen des activités de gestion des sources humaines du ministère de la Défense nationale et des Forces armées canadiennes (MDN et FAC), qui était toujours en cours au moment de la rédaction du présent document, l'OSSNR a produit à l'intention de la ministre de la Défense nationale un rapport le 9 décembre 2022, en vertu de l'article 35 de la Loi sur l'OSSNR. Selon l'article 35, l'OSSNR doit présenter un rapport au ministre compétent sur toute activité liée à la sécurité nationale ou au renseignement qui, à son avis, pourrait ne pas être conforme à la loi. La ministre de la Défense nationale a transmis une copie de ce rapport au procureur général du Canada et y a joint ses commentaires indiquant que son interprétation des faits et de la loi diffère de celle de l'OSSNR. L'OSSNR maintient sa position et estime que la position de la ministre est fondée sur une interprétation étroite des faits et de la loi. L'OSSNR terminera l'examen plus général des activités de gestion des sources humaines du MDN et des FAC en 2023. Bien que le rapport en vertu de l'article 35 ne contienne pas de recommandations, l'examen plus général abordera la responsabilisation et la surveillance du programme, son cadre de gestion des risques et la manière dont le MDN et les FAC s'acquittent de leur devoir de diligence en ce qui concerne les sources humaines. L'examen porte également sur la légalité du programme et de ses activités connexes, ainsi que sur le caractère suffisant de ses fondements juridiques et stratégiques. Le rapport pourrait donc inclure des recommandations donnant suite aux observations formulées dans le rapport établi au titre de l'article 35.

Agence des services frontaliers du Canada

Examen du ciblage des passagers aériens

81. Le programme de ciblage des passagers aériens de l'Agence des services frontaliers du Canada (ASFC) repère, au moyen d'évaluations des risques effectuées avant l'arrivée, les voyageurs aériens entrants qui présentent un risque élevé d'interdiction de territoire au Canada ou dont l'entrée, ou l'entrée de leurs marchandises, pourrait contrevenir à la législation frontalière de l'ASFC.

82. La première étape de ces évaluations en plusieurs phases consiste à trier les voyageurs en fonction des caractéristiques et des habitudes de voyage communiquées à l'ASFC par les transporteurs aériens commerciaux dans les données relatives à l'information préalable sur les

voyageurs et aux dossiers passagers. Ce triage peut être manuel (ciblage au moyen de la liste de vol) ou automatisé (ciblage fondé sur des scénarios). Dans les deux cas, l'ASFC s'appuie sur de l'information et du renseignement provenant de diverses sources pour déterminer quels éléments de données doivent être traités comme des indicateurs de risque en lien avec des problèmes particuliers liés à l'exécution de la loi, y compris ceux qui se rapportent à la sécurité nationale. L'utilisation de ces indicateurs peut amener l'ASFC à établir des distinctions entre les voyageurs lors des étapes ultérieures du ciblage ou à la frontière, ce qui a des répercussions sur le temps, la vie privée et l'égalité de traitement des passagers.

83. L'examen du ciblage des passagers aériens a constitué la première évaluation approfondie par l'OSSNR du respect par l'ASFC des lois pertinentes. L'OSSNR s'est tout d'abord attaché à déterminer si l'ASFC respecte les restrictions relatives à l'utilisation des données sur les passagers établies par la *Loi sur les douanes* et le *Règlement sur la protection des renseignements relatifs aux passagers*. L'examen a ensuite porté sur la question de savoir si l'utilisation par l'ASFC de ces types de données sur les passagers était discriminatoire au regard de la *Loi canadienne sur les droits de la personne* et de la *Charte canadienne des droits et libertés*.

84. L'OSSNR a constaté que l'utilisation par l'ASFC de ces deux types de données sur les passagers dans le cadre d'un ciblage fondé sur des scénarios se faisait à des fins autorisées par la *Loi sur les douanes*. Toutefois, en ce qui concerne le ciblage au moyen des listes de vol, l'ASFC ne documente pas les raisons qui sous--tendent ses décisions de triage. L'OSSNR n'a donc pas été en mesure de vérifier la conformité du ciblage au moyen des listes de vol aux limites établies par la *Loi sur les douanes*. De plus, la documentation n'a pas permis à l'OSSNR de vérifier que l'utilisation par l'ASFC des données du dossier passager dans le cadre de l'une ou l'autre méthode de triage était conforme au *Règlement sur la protection des renseignements relatifs aux passagers*, qui exige que l'accès aux données conservées se fasse à des fins liées au repérage des personnes qui ont commis ou pourraient avoir commis une infraction de terrorisme ou un crime transnational grave.

85. L'OSSNR a également constaté que l'ASFC ne justifiait pas toujours adéquatement son choix d'indicateurs en particulier en tant que signaux de risque accru. En l'absence d'une justification adéquate, le fait d'établir des distinctions entre les passagers en se fondant sur des motifs de distinction illicite (tels que l'âge, l'origine nationale ou ethnique, ou le sexe) crée un risque de discrimination.

86. L'OSSNR a recommandé à l'ASFC de documenter ses pratiques de triage de manière à démontrer qu'elle respecte la *Loi sur les douanes* et, le cas échéant, le *Règlement sur la*

protection des renseignements relatifs aux passagers. Il a recommandé à l'ASFC de veiller de façon continue à ce que sa sélection d'indicateurs de risque soit dûment justifiée au moyen d'informations ou de renseignements bien documentés. L'OSSNR a également recommandé à l'ASFC d'exercer une surveillance plus rigoureuse et régulière du ciblage des passagers aériens, y compris des mises à jour des politiques, des procédures, de la formation et des autres directives. L'OSSNR a également recommandé à l'ASFC de commencer à recueillir les données nécessaires pour cerner, analyser et atténuer les risques liés à la discrimination découlant du ciblage des passagers aériens.

3.4 Examens multiministériels

Examen des communications d'information par des institutions fédérales au titre de la *Loi sur la communication d'information ayant trait à la sécurité du Canada* en 2021

87. L'examen des communications d'information par des institutions fédérales au titre de la *Loi sur la communication d'information ayant trait à la sécurité du Canada* (LCISC) en 2021 décrit les résultats d'un examen des communications d'information faites en 2021 par des institutions fédérales en vertu de cette loi[13]. En 2022, l'examen de l'OSSNR était axé sur les communications proactives d'Affaires mondiales Canada (AMC).

88. La LCISC vise à encourager les institutions fédérales à communiquer entre elles de l'information et à faciliter une telle communication, afin de protéger le Canada contre des activités qui menacent la sécurité nationale ou qui y portent atteinte, sous réserve de certaines conditions. La LCISC impose un critère en deux temps qui doit être respecté avant toute communication d'information par une institution :

    - la communication d'information doit aider à l'exercice de la compétence ou des attributions de l'institution fédérale destinataire à l'égard d'activités portant atteinte à la sécurité du Canada [alinéa 5(1)a)];
    - l'incidence de la communication d'information sur le droit à la vie privée d'une personne doit se limiter à ce qui est raisonnablement nécessaire dans les circonstances [alinéa 5(1)b)].

89. La LCISC comporte également des dispositions et des principes directeurs relatifs à la gestion des communications d'information, notamment aux déclarations concernant l'exactitude et la fiabilité ainsi qu'aux obligations en matière de conservation de documents.

90. L'OSSNR a relevé des sources de préoccupation qui mettent en évidence la nécessité pour AMC d'améliorer ses formations. En outre, l'OSSNR était d'avis qu'il existe des risques de confusion lorsqu'il s'agit d'établir si la LCISC constitue le mécanisme devant s'appliquer à certaines communications d'information touchant la sécurité nationale. Certaines communications d'AMC Canada ne remplissaient pas le critère en deux temps imposé par la LCISC avant que l'information soit communiquée, ce qui contrevient aux dispositions de la LCISC. Deux communications ne comprenaient aucune déclaration concernant l'exactitude et la fiabilité, ce qui est contraire aux dispositions de la LCISC. En ce qui concerne la conservation de documents, l'OSSNR a recommandé que les ministères documentent, au moment où ils décident de communiquer de l'information en vertu de la LCISC, les renseignements sur lesquels ils se fondent pour conclure que la communication est autorisée par la Loi [alinéa 9(1)e)].

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* pour 2021

91. Cet examen a porté sur la mise en œuvre par les ministères des instructions reçues par le biais de décrets délivrés en vertu de la *Loi visant à éviter la complicité dans les cas de mauvais traitements infligés par des entités étrangères* (LCMTIEE). Il s'agit du troisième examen annuel prescrit par la loi de la mise en œuvre des instructions données en vertu de la LCMTIEE. L'examen a permis d'évaluer la mise en œuvre par les ministères des directives transmises au titre de la LCMTIEE et leur opérationnalisation de cadres pour satisfaire aux exigences de la LCMTIEE. Cet examen constitue donc le premier examen approfondi de la LCMTIEE au sein des différents ministères.

92. L'examen de cette année portait sur l'année civile 2021 et a été divisé en trois sections. La première section traitait des obligations légales de tous les ministères. Les deuxième et troisième sections étaient des analyses approfondie de la manière dont la Gendarmerie royale du Canada (GRC) et Affaires mondiales Canada (AMC) ont mis en œuvre les directives au titre de la LCMTIEE. L'OSSNR a utilisé des études de cas, dans la mesure du possible, pour examiner la mise en œuvre par ces ministères de leur cadre de la LCMTIEE.

93. Pour une troisième année consécutive, aucun cas n'a été transmis aux administrateurs généraux, tous ministères confondus. Il s'agit d'une exigence des décrets qui doit être respectée si les fonctionnaires ne sont pas en mesure d'établir s'il est possible d'atténuer le risque sérieux. Les prochains examens porteront sur la question de la transmission des cas et sur les processus décisionnels des ministères.

94. Au cours de l'examen des cadres ministériels visant à éviter la complicité dans les cas de mauvais traitements par des entités étrangères de 2019 de l'OSSNR[14], l'OSSNR a recommandé que la définition du terme « risque sérieux » soit codifiée dans la loi ou dans les instructions publiques. L'OSSNR notait que certains ministères ont pallié cette lacune en utilisant la définition du terme « risque sérieux » qui figure dans les instructions ministérielles de 2017. À la lumière de l'examen en cours prévu par la loi visant la *Loi sur la sécurité nationale de 2017* et de l'importance du concept de risque sérieux pour le régime de la LCMTIEE, l'OSSNR réitérait sa recommandation de 2019 selon laquelle la définition de risque sérieux doit être codifiée dans la loi.

95. Lors de l'examen de la mise en œuvre de la LCMTIEE par les ministères en 2020, l'OSSNR a déterminé que l'Agence des services frontaliers du Canada (ASFC) et Sécurité publique Canada n'avaient pas encore mis au point leurs politiques relatives à la LCMTIEE. Bien que l'ASFC et Sécurité publique Canada continuent de progresser, ces ministères n'ont pas entièrement mis en œuvre le cadre à l'appui de la LCMTIEE et les politiques et procédures qui l'accompagnent.

96. La GRC dispose d'un solide cadre pour le triage et le traitement des dossiers liés à la LCMTIEE. Le volet analyse approfondie de cet examen a révélé que la GRC ne dispose pas d'un système centralisé de documentation des garanties et qu'elle n'assure pas régulièrement le contrôle et la mise à jour de l'évaluation de la fiabilité des garanties. La GRC n'a pas non plus élaboré de mécanismes pour mettre à jour les profils des pays et des entités en temps opportun, et l'information recueillie par l'agent de liaison au cours d'une opération n'est pas documentée de manière centralisée afin de pouvoir être utilisée aux fins d'évaluations futures.

97. En analysant l'un des dossiers du Comité consultatif sur les risques – Information de l'étranger de la GRC, l'OSSNR a constaté que les motifs invoqués par le commissaire adjoint de la GRC pour le rejet des conseils du Comité consultatif sur les risques ne tenaient pas suffisamment compte des préoccupations qui découlent des dispositions des décrets. L'OSSNR a notamment constaté que le commissaire adjoint avait mal évalué l'importance de la future relation stratégique potentielle avec une entité étrangère lors de l'évaluation du risque potentiel de mauvais traitements à l'égard d'une personne.

98. L'OSSNR a constaté qu'AMC s'en remet désormais fortement au personnel opérationnel et aux chefs de mission pour la prise de décisions et la responsabilisation dans le cadre de la LCMTIEE. Il s'agit d'un changement notable par rapport aux conclusions de l'examen de 2019, selon lesquelles la prise de décisions était assurée par le Comité de conformité à la directive ministérielle à l'administration centrale.

99. AMC n'a pas non plus procédé à un exercice de schématisation interne pour déterminer les secteurs d'activité les plus susceptibles d'être concernés par la LCMTIEE. Compte tenu du faible nombre de cas cette année et de la taille d'AMC, et du fait que la formation sur la

LCMTIEE n'est pas obligatoire pour le personnel, l'OSSNR est préoccupé par le fait que tous les secteurs concernés par l'échange d'information au sein d'AMC puissent ne pas être adéquatement informés de leurs obligations en vertu de la LCMTIEE.

100. L'OSSNR a également noté qu'AMC ne dispose pas d'un mécanisme officiel de suivi ou de documentation pour le suivi des mises en garde et demandes de garantie. Cela pose un problème, car le personnel de mission est permutant et peut donc ne pas avoir connaissance des mises en garde et demandes de garantie liées à des cas antérieurs d'échange d'information.

3.5 Examens annulés

101. Au cours de la dernière année, l'OSSNR a décidé de mettre fin à certains travaux d'examen en cours ou de ne pas produire de rapport final à l'intention d'un ministre dans le cadre de certains examens. Ces décisions permettent à l'OSSNR de demeurer agile et de réorienter son plan de travail. Des considérations telles que l'évolution des priorités, les demandes en matière de ressources, le travail en cours au sein de l'entité faisant l'objet de l'examen et l'harmonisation avec les organismes d'examen partenaires peuvent toutes être des facteurs qui mènent à la décision de mettre fin à un examen. De telles décisions permettent à l'OSSNR de réorienter ses efforts et ses ressources vers d'autres questions importantes et ainsi de maximiser la valeur de son travail.

102. Par exemple, un examen visant la sous-direction de la recherche opérationnelle de la Gendarmerie royale du Canada (GRC) a été annulé. Le fait que cette sous-direction de la GRC ait cessé ses activités a contribué à cette décision. Un autre exemple est la décision de mettre fin à l'examen en cours portant sur la manière dont la GRC traite le chiffrement lors de l'interception de communications privées dans le cadre d'enquêtes criminelles liées à la sécurité nationale. Cet examen a été annulé dans le cadre d'efforts d'harmonisation avec le Comité des parlementaires sur la sécurité nationale et le renseignement (CPSNR), qui menait un examen semblable. Enfin, un examen portant sur le financement d'activités terroristes et le régime d'échange d'information du Centre d'analyse des opérations et des déclarations financières du Canada (CANAFE), qui en était à ses débuts, a été annulé au moment où l'OSSNR a décidé d'entamer un examen de la Division de la revue et de l'examen de l'Agence du revenu du Canada (ARC), laquelle exécute le mandat antiterroriste de l'ARC.

3.6 Rôle de la technologie dans les examens

Intégration de la technologie aux examens

103. Les technologies numériques continuent de jouer un rôle essentiel dans les activités opérationnelles de la communauté de la sécurité nationale et du renseignement du Canada, car les organismes utilisent de plus en plus les nouvelles technologies à l'appui de leurs mandats, pour proposer de nouvelles pistes d'activités et pour surveiller les menaces émergentes.

104. Il est essentiel qu'un organisme de responsabilisation comme l'OSSNR assure le suivi de l'utilisation des technologies numériques au sein de l'appareil canadien de la sécurité nationale et du renseignement. En se tenant au courant de l'évolution rapide des écosystèmes technologiques, l'OSSNR peut s'assurer que les organismes visés par son mandat de surveillance s'acquittent de leur mandat de manière légale, raisonnable et appropriée.

105. La Direction de la technologie de l'OSSNR est composée d'une équipe d'ingénieurs, d'informaticiens, de technologues et d'examinateurs de la technologie. Le mandat de la Direction de la technologie de l'OSSNR est le suivant :

- diriger l'examen relatif aux systèmes et aux capacités de la Technologie de l'information (TI);
- évaluer le respect des lois, des instructions ministérielles et des politiques relatives à la TI par une entité faisant l'objet d'un examen;
- mener des enquêtes techniques indépendantes;
- recommander des mesures de protection concernant les systèmes de TI et les données pour minimiser le risque de non-conformité sur le plan juridique;
- produire des rapports pour expliquer et vulgariser des sujets techniques;
- faire en sorte que les thèmes liés à la technologie soient intégrés dans les plans d'examens annuels de l'OSSNR;
- tirer parti d'une expertise externe afin de mieux comprendre et évaluer les risques touchant la TI;
- appuyer les membres de l'OSSNR affectés aux enquêtes sur les plaintes contre le SCRS, le CST ou la GRC lorsque l'examen des éléments de preuve requiert une expertise technologique.

106. En 2022, la Direction de la technologie est passée d'un effectif d'un employé à temps plein à trois, et a accueilli un étudiant du Programme d'enseignement coopératif et deux chercheurs

externes. Grâce à ses capacités accrues, la Direction de la technologie a élargi son analyse des technologies dans le cadre de nombreux examens de l'OSSNR et a commencé à officialiser sa méthodologie de recherche et à organiser des séances de microapprentissage et des forums de discussion axés sur des questions techniques pertinentes, notamment les interfaces truquées, le renseignement de sources ouvertes et le chiffrement.

107. La Direction de la technologie a également commencé à établir un réseau de recherche universitaire à l'appui des examens de l'OSSNR. À ce jour, les participants au réseau de recherche ont produit de très utiles notes de service internes, rapports et forums de discussion, ce qui a permis d'améliorer les connaissances de l'OSSNR sur un large éventail d'enjeux techniques.

108. Au cours de la dernière année, la Direction de la technologie a également lancé le premier examen de l'OSSNR axé sur la technologie, qui porte sur le cycle de vie de l'information recueillie par le SCRS par des moyens technologiques au titre d'un mandat de la Cour fédérale. Cet examen est l'occasion pour l'OSSNR de s'inspirer des normes techniques et des processus d'examen utilisés par ses homologues du Groupe des cinq et par le milieu international de l'examen et de la surveillance. L'OSSNR a utilisé cet examen pour élaborer un modèle d'évaluation des risques et un plan d'inspection technique, qui seront ajoutés à sa trousse plus générale d'outils d'examen.

Avenir de la technologie dans les examens

109. Au cours de l'année prochaine, l'OSSNR continuera d'accroître le nombre d'employés travaillant à temps plein au sein de la Direction de la technologie, de favoriser l'enseignement coopératif et de faire appel à des chercheurs externes pour renforcer ses capacités. Ce faisant, l'OSSNR renforcera sa capacité à assurer le suivi de l'évolution rapide et de l'utilisation croissante des technologies numériques au sein de l'écosystème canadien de la sécurité nationale et du renseignement.

110. S'appuyant sur la réussite de son réseau de recherche universitaire, la Direction de la technologie a l'intention d'accorder la priorité à la recherche non classifiée portant sur un certain nombre de sujets, notamment le renseignement fondé sur les sources ouvertes, les technologies publicitaires et les métadonnées (données liées au contenu et données non liées au contenu).

111. La Direction de la technologie de l'OSSNR appuiera aussi l'équipe chargée des enquêtes sur les plaintes de l'OSSNR afin de comprendre où et quand la technologie entre en ligne de compte dans ses processus et activités.

3.7 Interaction avec les entités examinées

Améliorations et difficultés actuelles

112. Comme indiqué dans les rapports annuels précédents, en tant que nouvel organisme d'examen, l'OSSNR a initialement rencontré des difficultés dans ses interactions avec les ministères et les organismes faisant l'objet de ses examens. Ces difficultés sont traitées de façon continue, et les relations de l'OSSNR avec les ministères et organismes faisant l'objet de ses examens ont mûri. Bien que le travail sur ce front ne soit pas terminé, on note des améliorations chez les entités examinées en ce qui a trait à la coopération et au soutien au processus d'examen indépendant. La discussion qui suit présente des commentaires généraux sur la mobilisation globale des entités visées par les examens de l'année dernière. Les aperçus couvrent l'année 2022 et la période allant jusqu'à la date de rédaction du présent rapport. Le cas échéant, des commentaires ou des questions propres aux examens sont abordés dans la vue d'ensemble de chaque examen ci-dessus.

Service canadien du renseignement de sécurité

113. Après la levée des restrictions temporaires et des modifications liées à la COVID-19, l'OSSNR a retrouvé son niveau d'occupation d'avant la pandémie à l'administration centrale du SCRS pour les examens portant sur le SCRS. L'OSSNR dispose notamment d'espaces de travail dédiés et de laissez-passer pour ses employés chargés d'examiner les activités du SCRS. Les employés de l'OSSNR ont un accès direct aux bases de données du SCRS, et le SCRS fournit toute la formation nécessaire, sur demande, pour naviguer dans ces systèmes et y accéder. En règle générale, le SCRS répond aux demandes d'information de l'OSSNR dans des délais raisonnables. Des retards et des difficultés surviennent parfois, mais la communication entre l'OSSNR et le SCRS est constructive et permet de résoudre les problèmes.

Centre de la sécurité des télécommunications

114. L'OSSNR a continué à utiliser l'espace fourni à l'administration centrale du CST, dans l'édifice Edward Drake, pour réaliser ses activités liées à des examens. Peu d'améliorations ont été apportées en 2022 en ce qui a trait aux exigences d'accès de l'OSSNR au sein du CST. Toutefois, l'OSSNR participera en 2023 à un projet pilote d'accès direct limité au principal

dépôt institutionnel de documents du CST, GCdocs. Des problèmes subsistent et l'OSSNR n'est pas en mesure d'évaluer l'utilité du projet pilote. Dans certains cas, le CST a amélioré sa réactivité aux demandes d'information de l'OSSNR sur le plan de la rapidité, même si la qualité des réponses demeure problématique. L'OSSNR continue de travailler avec diligence avec le CST pour régler ces problèmes.

Ministère de la Défense nationale

115. Les discussions se poursuivent en ce qui concerne l'aménagement d'un espace de bureau dédié et l'accès aux réseaux. Bien que les solutions à long terme n'aient guère progressé, le MDN et les FAC ont collaboré avec l'OSSNR pour permettre l'accès aux documents pertinents, y compris aux dossiers de nature sensible. Le MDN et les FAC ont fourni un bon accès à leurs installations et à leur personnel. En règle générale, les réponses aux demandes d'information ont été fournies en temps opportun; toutefois, le manque de proactivité du MDN et des FAC en ce qui a trait aux communications a obligé l'OSSNR à envoyer des demandes supplémentaires pour s'assurer de l'exhaustivité et de l'exactitude de l'information. Dans l'ensemble, la communication entre l'OSSNR et le MDN et les FAC a été constructive.

Gendarmerie royale du Canada

116. L'année dernière a été marquée par des incohérences dans les réponses de la GRC aux demandes d'information de l'OSSNR. La GRC a pris des mesures pour renforcer sa capacité à répondre aux demandes de l'OSSNR, ce qui a donné des résultats positifs. L'OSSNR n'a pas d'accès direct aux systèmes d'information, mais a été autorisé à accéder aux dossiers liés aux questions examinées. L'OSSNR a dû, à plusieurs reprises, envoyer des demandes supplémentaires pour s'assurer de l'exhaustivité des dossiers fournis. Dans la plupart des cas, les documents sont examinés sur place, dans les locaux à bureaux qui ont été mis à la disposition de l'OSSNR au sein de la Direction générale de la GRC. Malgré les difficultés rencontrées au début de l'année, l'OSSNR a de manière générale eu accès à des personnes, y compris des membres réguliers de la GRC qui sont des experts dans les domaines examinés. Dans l'ensemble, la coopération entre l'OSSNR et la GRC s'est améliorée.

Affaires mondiales Canada

117. AMC a répondu aux demandes de l'OSSNR, s'est efforcé de clarifier les demandes et a organisé toutes les réunions demandées. Lors de l'examen de la mise en œuvre par le ministère de la *Loi visant à éviter la complicité dans les cas de mauvais traitements infligés par des entités étrangères* en 2021, AMC a fourni à l'OSSNR les documents demandés dans

un délai raisonnable. L'OSSNR n'avait pas d'accès direct aux systèmes d'AMC, mais cela n'a pas eu d'incidence sur la capacité de l'OSSNR à vérifier l'information ou à accéder aux dossiers de nature sensible puisqu'AMC a été en mesure de transférer tous les documents demandés par courrier électronique ou par l'intermédiaire de son portail sécurisé.

Agence des services frontaliers du Canada

118. L'ASFC a fourni à l'OSSNR un accès adéquat à l'information et aux personnes. Certains problèmes sur le plan de la rapidité ont été résolus rapidement après l'envoi par l'OSSNR d'un avis concernant une lettre d'avis en attente. Ces difficultés semblent liées à la lenteur du processus d'approbation de l'ASFC pour la communication de documents à l'OSSNR. L'OSSNR n'a pas d'accès direct aux systèmes de l'ASFC, mais cela ne l'a pas empêché d'accéder aux dossiers de nature sensible. Dans l'ensemble, l'ASFC a répondu aux demandes de l'OSSNR et a fait en sorte que ses employés soient disponibles pour répondre aux questions de l'OSSNR.

Affiner les énoncés sur le niveau de confiance de l'OSSNR

Évaluation de la réactivité et de la vérification

119. L'OSSNR continue d'accorder de l'importance à l'évaluation de la qualité et de l'efficacité globales de ses interactions avec les entités examinées. Auparavant, l'OSSNR consignait cette évaluation dans un « énoncé sur le niveau de confiance », qui fournissait un contexte supplémentaire important à l'examen, en indiquant aux lecteurs dans quelle mesure l'OSSNR avait été à même de vérifier l'information nécessaire ou pertinente, et si cet exercice avait eu une incidence sur la confiance dans l'information fournie. Ces énoncés étaient également influencés par des aspects tels que l'accès aux systèmes d'information et les délais de réception de l'information demandée.

120. L'OSSNR a affiné et normalisé son approche d'évaluation de ces aspects clés de ses interactions avec les entités examinées et, à l'avenir, évaluera les critères suivants dans le cadre de chaque examen :
    - la rapidité des réponses aux demandes d'information;
    - la qualité des réponses aux demandes d'information;
    - l'accès aux systèmes;
    - l'accès aux personnes;
    - l'accès aux installations;
    - le professionnalisme;

- la proactivité.

Suivi des délais et des lettres d’avis

121. Dans son rapport annuel public de 2021, l’OSSNR s’est engagé à prendre des mesures pour régler les problèmes constants rencontrés pour obtenir des réponses rapides aux demandes d’information de la part des entités examinées. Au cours de la dernière année, tous les retards ont été saisis dans un système de suivi des demandes d’information. Les résultats renseignent l'un des critères examinés ci-dessus. L’OSSNR continue également d’utiliser son approche en trois étapes pour remédier aux retards persistants en envoyant des lettres d’avis aux cadres supérieurs et, en dernier ressort, aux ministres compétents si les retards persistent. Cet outil a été utilisé à cinq reprises en 2022. Trois lettres d’avis ont été envoyées au CST et deux à la GRC.

122. Des lettres d’avis envoyées à une entité examinée au cours d’un examen peuvent être annexées au rapport final afin que le ministre compétent et le public soient informés de ces retards. En les combinant avec les critères d'évaluation actualisés mentionnés ci-dessus, l’OSSNR s’efforce d’assurer la transparence et d’accroître la sensibilisation aux difficultés et aux réussites concernant les interactions avec les entités examinées.

04 //

Enquêtes sur les plaintes

4.1 Aperçu

123. Depuis sa création il y a trois ans, l'OSSNR s'est attaché à réformer le processus d'enquête sur les plaintes et à élaborer des procédures et des pratiques pour garantir l'équité, la rapidité et la transparence des enquêtes. L'OSSNR a précédemment abordé dans ses rapports la création de ses règles de procédure, sa politique d'engagement à publier des rapports d'enquête caviardés et la mise en œuvre de l'utilisation de la technologie vidéo. Au cours de la dernière année, l'OSSNR a rationalisé sa phase d'évaluation des compétences et son processus d'enquête en recourant davantage à des entrevues d'enquête comme principal moyen d'établir les faits. Ces développements ont permis à l'OSSNR de traiter un volume important de plaintes au cours de la période visée par le présent rapport.

124. Après avoir reçu une plainte, l'OSSNR doit déterminer si l'enquête sur la plainte relève de sa compétence en se fondant sur les conditions énoncées dans la *Loi sur l'Office de surveillance des activités en matière de sécurité nationale et de renseignement* (Loi sur l'OSSNR). En ce qui concerne les plaintes à l'encontre du Service canadien du renseignement de sécurité (SCRS) ou du Centre de la sécurité des télécommunications (CST), l'OSSNR doit être convaincu que la plainte contre l'organisation mise en cause se rapporte à une activité menée par l'organisation et que la plainte n'est pas frivole, vexatoire ou sans objet. Pour les plaintes renvoyées par la Commission civile d'examen et de traitement des plaintes (CCETP) relatives à la Gendarmerie royale du Canada (GRC), l'OSSNR doit recevoir une plainte renvoyée en vertu du paragraphe 45.53(4.1) ou 45.67(2.1) de la *Loi sur la Gendarmerie royale du Canada* et mène une enquête s'il est convaincu que la plainte n'est pas frivole, vexatoire, sans objet ou entachée de mauvaise foi. En ce qui a trait aux habilitations de sécurité refusées qui ont des répercussions sur des personnes, comme le prévoit la Loi sur l'OSSNR, l'OSSNR doit recevoir la plainte et enquêter sur celle-ci.

125. L'OSSNR a mis au point un processus solide pour examiner et vérifier de manière indépendante l'information fournie par les organisations mises en cause, en tenant compte des intérêts du plaignant et des impératifs liés à la sécurité de l'organisation.

126. Dans le passé, le Comité de surveillance des activités de renseignement de sécurité traitait régulièrement les plaintes concernant le SCRS en recourant à des audiences formelles. Bien que l'OSSNR conserve ce pouvoir législatif, il s'est efforcé de recourir de plus en plus à des entrevues pour vérifier s'il dispose des éléments de preuve nécessaires à une enquête complète et à l'examen des plaintes. Compte tenu des contraintes de sécurité qui limitent la communication d'information aux plaignants lors des audiences formelles, les entrevues d'enquête permettent à l'OSSNR d'accéder à l'information en temps opportun et devrait réduire les délais de résolution des plaintes. Cela sera important, car l'OSSNR doit faire face à une augmentation du nombre de plaintes compte tenu de son mandat (qui comprend les plaintes liées au SCRS, au CST, à la GRC et aux habilitations de sécurité), ainsi qu'aux retards attribuables aux effets de la COVID-19 accumulés au cours des trois dernières années.

4.2 Initiatives en cours

127. L'OSSNR s'est engagée à établir des normes de service pour l'examen des plaintes, avec pour objectif de mener à bien 90 % des enquêtes dans le respect des normes de service de l'OSSNR d'ici mars 2024. En 2022, l'OSSNR a commencé à élaborer ces normes de service, qui visent également à favoriser une prise de décision administrative rapide et efficace. Les normes de service établiront des délais internes pour certaines étapes de l'enquête pour chaque type de plainte, dans des circonstances normales. Les normes de service préciseront les circonstances dans lesquelles ces délais ne s'appliquent pas. L'élaboration des normes de service comprend le suivi et la collecte de données pour déterminer si l'OSSNR respecte ses propres normes de service lors des enquêtes sur les plaintes. L'OSSNR finalisera et publiera ses normes de service en 2023 et s'engage à rendre compte du respect de ces normes.

128. Au cours de l'année à venir, l'OSSNR continuera d'améliorer son site Web afin de favoriser l'accessibilité aux enquêtes sur les plaintes. Plus précisément, l'OSSNR élaborera un portail en ligne protégé par un mot de passe qui permettra aux plaignants de déposer des plaintes et de recevoir des mises à jour sur l'état d'avancement de leur dossier.

129. L'OSSNR a entamé la dernière phase de l'étude commandée conjointement avec la CCETP sur les données sur la race et la collecte de données démographiques. L'étude évalue la viabilité de la collecte de données sur l'identité et démographiques dans le cadre des initiatives de lutte contre le racisme en cours de la CCETP. Il est nécessaire d'améliorer et de rendre plus précis et plus uniformes le suivi, la collecte et la mesure des données pour soutenir les efforts de lutte contre le racisme au sein du gouvernement. Au terme de l'étude, la CCETP et l'OSSNR disposeront d'information sur les éléments suivants :

- la collecte de données significative et ciblée;

- les difficultés liées à la collecte de données;
- une perspective sur la manière dont les données recueillies peuvent être utilisées pour éliminer tout obstacle systémique potentiel dans le processus d'enquête de l'OSSNR et dans ses initiatives de lutte contre le racisme;
- le sentiment du public à l'égard de la conservation des données sur l'identité.

Observations sur les domaines de réforme juridique

130. L'OSSNR note que certaines réformes de sa loi faciliteraient l'accomplissement de son mandat d'enquête. Ces réformes permettraient notamment aux membres de l'OSSNR d'avoir la compétence pour mener à bien tous les dossiers d'enquête sur des plaintes qu'ils ont entamés, même si leur mandat prend fin. L'élargissement des droits d'accès aux personnes et aux installations des organisations examinées renforcerait les activités de vérification.

4.3 Résumés des rapports d'enquête

Allégations concernant le rôle du SCRS dans le retard des évaluations de sécurité relatives aux demandes de visa de résident permanent et de résident temporaire (07-403-30)

Contexte

131. Les plaignants ont déposé une plainte contre le SCRS, alléguant qu'il a causé des retards dans leurs demandes de visa de résident permanent et de résident temporaire.

Enquête

132. Au cours de l'enquête de l'OSSNR, le SCRS a donné son avis sur les demandes de résidence permanente des plaignants. À la lumière de cette information, l'OSSNR a demandé aux plaignants de confirmer s'ils souhaitaient toujours donner suite à leur plainte. Les plaignants ont précisé qu'ils souhaitaient recevoir une compensation financière ou une explication pour le retard pris dans le traitement de leur dossier.

Conclusion

133. L'OSSNR a informé les plaignants qu'il n'est pas habilité à rendre des ordonnances remédiatrices obligeant par exemple le SCRS à verser une compensation financière à un

plaignant. Toutefois, l'OSSNR a demandé au SCRS s'il souhaitait participer à un processus de résolution informel afin de résoudre l'ensemble ou une partie des problèmes soulevés dans la plainte. Dans le cadre de la procédure de résolution informelle de l'OSSNR, de l'information a été fournie aux plaignants sur la participation du SCRS à leurs demandes de visa de résident permanent et de résident temporaire. L'OSSNR a tenté de communiquer avec les plaignants à plusieurs reprises afin de déterminer s'ils avaient des questions susceptibles d'aider à préciser les circonstances de leur plainte.

134. L'OSSNR a conclu que des efforts raisonnables avaient été déployés pour communiquer avec les plaignants, et a communiqué les motifs pour lesquels la plainte était réputée avoir fait l'objet d'un désistement conformément aux Règles de procédure de l'OSSNR. Le dossier d'enquête sur la plainte a été fermé.

Allégations contre le SCRS, Immigration, Réfugiés et Citoyenneté Canada, l'Agence des services frontaliers du Canada et Sécurité publique Canada concernant leur rôle dans le traitement des demandes d'immigration (07-405-1 et coll.)

Contexte

135. En vertu de la sous-section 45(2) de la *Loi canadienne sur les droits de la personne*, la Commission canadienne des droits de la personne (CCDP) a renvoyé 58 plaintes individuelles et collectives à l'OSSNR. C'était la première fois que l'OSSNR était saisi de renvois par la CCDP en vertu de l'article 45.

136. Les plaignants, des ressortissants iraniens, allèguent que le gouvernement du Canada a exercé à leur encontre une discrimination fondée sur l'origine nationale ou ethnique ou sur la race en raison des retards dans le traitement de leur demande de visa de résidence temporaire ou permanente, ou de citoyenneté canadienne.

137. En vertu de l'article 46 de la *Loi canadienne sur les droits de la personne*, l'OSSNR est tenu de mener une enquête et de remettre un rapport à la CCDP. Cet article prévoit également qu'en se fondant sur le rapport de l'OSSNR, la CCDP peut rejeter la plainte ou en poursuivre le traitement.

138. Le rôle de l'OSSNR dans les renvois au titre de l'article 45 se limite à examiner les éléments d'une affaire qui sont fondés sur des considérations ayant trait à la sécurité du Canada, et à rendre compte des conclusions de son enquête sur de l'information classifiée à la CCDP de

manière non classifiée. L'OSSNR n'est pas habilité à exercer le pouvoir discrétionnaire conféré par la loi à la CCDP de renvoyer l'affaire au Tribunal canadien des droits de la personne.

Enquête

139. Au cours de son enquête, l'OSSNR a examiné les éléments de preuve fournis par les témoins et les observations de leurs avocats lors d'une entrevue d'enquête, ainsi que la documentation et les observations soumises par les parties gouvernementales, y compris les documents classifiés communiqués à l'OSSNR par le SCRS, Immigration, Réfugiés et Citoyenneté Canada (IRCC), l'Agence des services frontaliers du Canada (ASFC) et Sécurité publique Canada.

140. Il est important de noter que l'OSSNR a entendu les parties gouvernementales au sujet d'un indicateur obligatoire en particulier élaboré par l'ASFC et utilisé par les agents d'IRCC pour prendre des décisions sur les renvois aux fins de contrôle de sécurité des demandes d'immigration iraniennes. Avant les réformes effectuées en août 2018, un indicateur était entièrement fondé sur la nationalité iranienne, et n'était associé qu'à l'âge et au sexe du demandeur. Lorsqu'un demandeur répondait aux critères, les agents d'IRCC transmettaient automatiquement le dossier à l'ASFC et au SCRS aux fins de contrôle de sécurité. Les éléments de preuve montrent que le gouvernement a abandonné les indicateurs obligatoires en 2018 pour des raisons d'efficacité et parce qu'ils contribuaient à des retards.

141. L'OSSNR a également constaté qu'IRCC ne consignait pas d'information sur l'indicateur en particulier sur lequel le renvoi se fondait. Cela a nui à la capacité de l'OSSNR à enquêter sur les autres indicateurs susceptibles d'avoir eu une incidence sur le traitement de la demande d'immigration d'un plaignant. Cela dit, l'OSSNR a reconnu qu'un système de codes de suivi des indicateurs faisait l'objet d'un projet pilote au moment de l'entrevue d'enquête. Cette solution technique permettrait d'assurer le suivi des décisions des agents d'IRCC de renvoyer des demandes d'immigration aux fins de contrôle de sécurité au moyen d'un système de codes indiquant le motif du renvoi.

Conclusion

142. Voici ce qu'a constaté l'OSSNR :

- l'indicateur obligatoire d'âge et de sexe utilisé par IRCC dans le traitement des demandes d'immigration jusqu'en mai 2018 reposait exclusivement sur la nationalité, l'âge et le sexe, qui figurent parmi les motifs de distinction illicite aux termes de l'article 5 de la *Loi canadienne sur les droits de la personne*;

- l'indicateur obligatoire d'âge et de sexe a désavantagé (notamment en entraînant des retards) les Iraniens soumis à un contrôle de sécurité et ceux dont les dossiers étaient liés à ces demandeurs;

- à l'époque des faits en cause dans cette affaire, l'application de cet indicateur obligatoire n'était pas justifiable pour des raisons de sécurité nationale;

- la procédure de contrôle de sécurité applicable aux demandes de citoyenneté dans cette affaire n'a pas entraîné de désavantage fondé sur les motifs énumérés dans la *Loi canadienne sur les droits de la personne*, étant donné que les demandes de citoyenneté reçues par IRCC sont envoyées au SCRS aux fins de contrôle de sécurité, quel que soit le pays de naissance du demandeur.

143. L'OSSNR a soumis son rapport à la CCDP afin qu'elle puisse déterminer s'il y a un fondement raisonnable dans la preuve pour un renvoi au Tribunal canadien des droits de la personne ou s'il convient de rejeter les plaintes.

Enquête sur une plainte concernant la révocation d'une habilitation de sécurité par le chef d'état–major de la défense (1170-17-7)

Contexte

144. Le plaignant était un soldat de la Force régulière titulaire d'une habilitation de sécurité « Très secret ». Les résultats du test polygraphique du plaignant, même si on ne s'est pas exclusivement fondé sur ceux-ci, ont été la principale influence dans les évaluations de sécurité du plaignant préparées par le SCRS et l'agent de sécurité du ministère de la Défense. À la suite de ces évaluations, le chef d'état-major de la défense (CEMD) a révoqué l'habilitation de sécurité du plaignant. Le plaignant a déposé une plainte auprès de l'OSSNR contre le CEMD concernant la révocation de l'habilitation de sécurité.

Enquête

145. Au cours de l'enquête, l'OSSNR a entendu des témoins gouvernementaux du MDN et du SCRS au sujet du test polygraphique, de l'enquête sur le plaignant et du processus qui a mené à la révocation de l'habilitation de sécurité du plaignant. Outre les témoignages oraux, les parties gouvernementales ont déposé des documents et présenté des observations. L'OSSNR a également examiné les témoignages oraux et les observations écrites fournies par le plaignant.

146. L'OSSNR a examiné tous les éléments de preuve reçus afin de déterminer si le CEMD avait des motifs raisonnables de révoquer l'habilitation de sécurité du plaignant et de s'assurer de l'exactitude de l'information utilisée par le CEMD pour prendre la décision de révoquer l'habilitation.

147. L'OSSNR a constaté plusieurs lacunes dans la manière dont le test polygraphique du plaignant avait été effectué et dont les résultats avaient été communiqués et diffusés. De plus, l'OSSNR a constaté que les faits disculpatoires n'avaient pas été contextualisés ni présentés au CEMD avant la prise de la décision de révocation.

Conclusion

148. L'OSSNR a constaté que l'information sur laquelle le CEMD s'était fondé pour prendre la décision de révocation n'était pas exacte. Par conséquent, la décision de révoquer l'habilitation n'était pas raisonnable.

149. L'OSSNR a recommandé au SCRS de présenter des excuses au plaignant pour la manière dont le test polygraphique a été effectué et dont les résultats ont été communiqués et diffusés, et a recommandé au CEMD de revenir sur la décision de révoquer l'habilitation de sécurité du plaignant.

Examen du rapport de la Gendarmerie royale du Canada concernant une plainte du public (07-407-3)

Contexte

150. Le plaignant a déposé une plainte auprès de la CCETP concernant le comportement de membres de la GRC. Le plaignant alléguait que la GRC avait procédé à l'arrestation injustifiée et arbitraire de son fils d'âge mineur, qu'elle avait effectué une fouille zélée et abusive du domicile familial et qu'elle avait rendu publique l'arrestation.

151. Le plaignant alléguait également que la GRC avait communiqué de l'information aux autorités américaines, avait déclaré que le formulaire d'arrestation du fils du plaignant serait oublié et détruit, et avait violé la sécurité de son fils et de sa famille, leurs droits constitutionnels et leurs droits à titre de dénonciateurs.

152. La GRC a conclu, dans un rapport envoyé au plaignant conformément à l'article 45.64 de la *Loi sur la Gendarmerie royale du Canada* (Loi sur la GRC), que ses membres avaient agi de manière appropriée et, par conséquent, n'a confirmé aucune des allégations du plaignant.

153. Le plaignant a soumis sa plainte à la CCETP pour examen puisqu'il n'était pas satisfait des conclusions de la GRC. La CCETP a renvoyé la plainte à l'OSSNR en vertu du paragraphe 45.53(4.1) de la Loi sur la GRC.

Enquête

154. L'OSSNR a déterminé qu'il avait compétence pour examiner le rapport de la GRC en vertu de l'article 19 de la Loi sur l'OSSNR.

155. L'enquête de l'OSSNR a comporté un examen des éléments suivants :

- la plainte;
- la demande d'examen déposée par le plaignant auprès de la CCETP;
- le dossier d'enquête de la GRC concernant la plainte, y compris les documents fournis par le plaignant au cours de l'enquête;
- le dossier opérationnel de la GRC concernant la plainte, y compris de nombreux enregistrements audio et vidéo, ainsi que les politiques et les lois pertinentes.

Conclusion

156. L'OSSNR a déterminé que les conclusions du rapport de la GRC étaient raisonnables.

157. Nonobstant ce qui précède, l'OSSNR a fait remarquer à la GRC qu'il est important que le décideur et le signataire d'un rapport de la GRC n'aient aucun lien antérieur avec le dossier faisant l'objet de la plainte, et de prendre des notes complètes au moment de l'exécution.

4.4 Statistiques concernant les enquêtes sur les plaintes

158. Les activités d'enquête se sont poursuivies à des niveaux importants en 2022 (voir l'annexe D). Une différence notable dans ces activités entre 2021 et 2022 est la baisse considérable du nombre d'enquêtes actives, qui est passé de 81 en 2021 à 19 au cours de la période visée par le présent rapport. Cette baisse est largement attribuable à un renvoi de près de 60 dossiers connexes par la CCDP, qui ont été traités au cours de la période visée par le présent rapport.

159. En vertu de l'article 16 de la Loi sur l'OSSNR, toute personne peut porter plainte auprès de l'OSSNR contre des activités du SCRS; l'article 17 porte sur les plaintes contre des activités du CST. Toutefois, pour que l'OSSNR puisse accepter une plainte, la personne qui souhaite porter plainte contre le SCRS doit d'abord envoyer une lettre de plainte au directeur du SCRS; pour les plaintes contre le CST, une lettre doit d'abord être envoyée au chef du CST. L'OSSNR fera enquête sur la plainte si le plaignant n'a pas reçu de réponse dans un délai que l'OSSNR

juge raisonnable ou si le plaignant est insatisfait de la réponse. À cet égard, l'OSSNR observe qu'en 2022, 53 % des plaignants n'ont pas reçu de lettre du SCRS en réponse à leur lettre de plainte adressée au directeur du SCRS.

160. Il est nécessaire de faire mieux connaître et comprendre aux membres du public et aux plaignants le mandat et la procédure d'enquête de l'OSSNR. Par exemple, les membres de l'OSSNR ne sont pas habilités à rendre des ordonnances remédiatrices, notamment d'indemnisation, ou à ordonner à un ministère de verser des dommages -intérêts aux plaignants. L'OSSNR continue d'apporter des améliorations à son site Web public afin d'accroître la sensibilisation à cet effet et de mieux renseigner le public et les plaignants sur son mandat d'enquête et les procédures d'enquête qu'il suit.

05 //

Élargissement des partenariats de l'OSSNR

161. L'OSSNR estime qu'il est essentiel d'établir une communauté de pratique dans le domaine de la surveillance et de l'examen indépendants et contribue activement à cet effort. Au cours de la dernière année, il a repris et renforcé ses efforts de mobilisation auprès de ses précieux partenaires, tant à l'échelle nationale qu'internationale, et a déjà récolté les fruits de ces efforts.

Partenariats internationaux

162. L'OSSNR a fait des relations internationales avec ses homologues une priorité pour son développement institutionnel. Au cours de la dernière année, l'OSSNR a bénéficié d'excellentes interactions fluides et soutenues avec ses partenaires étrangers les plus proches. Une meilleure compréhension des paramètres des activités d'examen et de surveillance des homologues étrangers de l'OSSNR et la mise en commun de pratiques exemplaires sont essentiels à la croissance de l'organisme.

Conseil de surveillance et d'examen du renseignement du Groupe des cinq

163. Depuis sa création, l'OSSNR participe activement au Conseil de surveillance et d'examen du renseignement du Groupe des cinq. Le conseil est composé d'organismes ayant un mandat de surveillance et d'examen des activités de sécurité nationale dans leurs pays respectifs (Canada, Australie, Nouvelle-Zélande, Royaume-Uni et États-Unis). L'OSSNR participe, aux côtés du Bureau du commissaire au renseignement, à la délégation du Canada au Conseil. Le groupe se réunit chaque année, et l'OSSNR a participé à la conférence du Conseil de surveillance et d'examen du renseignement du Groupe des cinq à Washington en 2022. L'OSSNR aura le plaisir d'accueillir les partenaires du Conseil à Ottawa à l'automne 2023.

164. L'OSSNR entretient aussi fréquemment des relations bilatérales avec les partenaires du Conseil au niveau opérationnel. Les échanges permettent à l'OSSNR de mieux comprendre les enjeux cruciaux qui ont une incidence sur son travail, de comparer les défis auxquels il est

confronté et les pratiques exemplaires en matière de méthode d'examen et de surveillance, et de discuter de sujets d'intérêt et de préoccupation mutuels. Par exemple, en apprendre sur les droits d'accès à l'information des partenaires du Conseil et le cadre juridique permettant cet accès a aidé à contextualiser certains des défis en matière d'accès auxquels est confronté l'OSSNR.

165. L'OSSNR a rencontré l'un de ses partenaires du Conseil, l'Investigatory Powers Commissioner's Office à Londres, au Royaume-Uni. Le Commissioner's office a un vaste mandat d'activités qui comprend, entre autres, l'approbation des mandats autorisés par le secrétaire d'État et la surveillance indépendante de l'utilisation des pouvoirs par l'appareil de la sécurité et du renseignement du Royaume-Uni. Les rencontres de plusieurs jours ont permis de mieux comprendre les organisations respectives de chacun, d'échanger des idées et de mettre en commun des pratiques exemplaires. L'OSSNR a rencontré un certain nombre de services avec lesquels le Commissioner's office collabore et a assisté à une inspection d'une journée menée par le Commissioner's office. L'approche adoptée par le Commissioner's office concernant le suivi de la mise en œuvre des recommandations qu'il formule et ses réflexions sur la production de rapports annuels ont particulièrement retenu l'attention de l'OSSNR. Le soutien à cet important partenariat se poursuit, et l'OSSNR a continué le dialogue avec le personnel du Commissioner's office pour consolider cette relation solide.

166. L'OSSNR a également pu effectuer des visites opérationnelles au bureau de l'inspecteur général du renseignement et de la sécurité de l'Australie et aux bureaux de certains membres de la communauté des inspecteurs généraux des États-Unis à Washington.

Efforts supplémentaires de mobilisation en Europe

167. L'OSSNR a également participé à l'International Intelligence Oversight Forum (forum international sur les mécanismes de surveillance des services de renseignement), qui réunit des organismes de surveillance, d'examen et de protection des données du monde entier. L'événement s'est avéré productif, car l'OSSNR a bénéficié d'échanges bilatéraux constructifs avec les institutions participantes.

168. Dans le cadre de ses efforts visant à établir des relations solides avec ses homologues d'Europe continentale dans des administrations aux vues similaires dotées de solides mécanismes de responsabilisation, l'OSSNR a rendu visite à la Commission parlementaire norvégienne de contrôle des services de renseignement et de sécurité, au Conseil danois de surveillance des services de renseignement, à la Commission néerlandaise de contrôle des

services de renseignement et de sécurité et à l'Autorité de surveillance indépendante des activités de renseignement de la Suisse.

169. Chacune de ces visites très productives a permis à l'OSSNR d'apprendre de ces partenaires et d'accroître la visibilité de son travail auprès de ces organismes de contrôle.

Resserrement de la coordination nationale

170. L'OSSNR a continué d'investir dans le renforcement des relations avec ses principaux partenaires nationaux – le Comité des parlementaires sur la sécurité nationale et le renseignement (CPSNR), la Commission civile d'examen et de traitement des plaintes relatives à la GRC et le Bureau du commissaire au renseignement, ainsi qu'avec les divers agents du Parlement qui jouent un rôle clé dans la responsabilisation gouvernementale.

171. L'OSSNR et le CPSNR jouent des rôles complémentaires dans le renforcement de la responsabilisation à l'égard des activités fédérales en matière de sécurité nationale et de renseignement, et sont tenus par la loi de coopérer dans l'accomplissement de leurs mandats respectifs. Des réunions de coopération sont régulièrement organisées à différents niveaux et les deux organismes continuent d'affiner leurs modalités de coopération et de coordination. L'OSSNR et le CPSNR se sont soutenus mutuellement en entretenant une communication régulière sur les plans d'examen afin d'éviter les doubles emplois et de procéder à des ajustements le cas échéant. Ces efforts de coordination ont contribué à la décision de l'OSSNR de cesser les travaux d'examen du chiffrement par la GRC. L'OSSNR a également fourni, après consultation ministérielle, un grand nombre de ses rapports finaux au CPSNR. Pour sa part, le CPSNR a fourni à l'OSSNR ses rapports classifiés et ses notes d'information. Ces échanges ont permis aux deux organisations d'affiner leurs thèmes et méthodologies d'examen. Les équipes juridiques du CPSNR et de l'OSSNR ont également collaboré de manière productive, notamment afin de résoudre des problèmes mutuels d'accès. Ces échanges fréquents et approfondis constituent une base importante pour un appareil solide et cohérent de surveillance des activités en matière de sécurité nationale et de renseignement, et l'OSSNR et le CPSNR jouissent d'un niveau de coopération qui compte parmi les plus solides parmi leurs homologues étrangers.

172. Comme indiqué dans la section Initiatives en cours, l'OSSNR et la Commission civile d'examen et de traitement des plaintes relatives à la GRC ont commandé conjointement une étude sur les données sur la race et la collecte de données démographiques. Cette étude orientera l'approche adoptée par chaque organisation pour l'élaboration et la mise en œuvre d'une stratégie relative aux données sur l'identité dans le cadre de ses enquêtes sur les plaintes.

L'étude en est actuellement à sa dernière phase et devrait être terminée au cours de l'exercice 2023-2024.

173. En 2022, le Secrétariat de l'OSSNR a rejoint un réseau de juristes issus des différents agents du Parlement. En tant qu'organisme et employeur distinct chargé de favoriser une surveillance indépendante, le Secrétariat de l'OSSNR tire avantage de la collaboration avec cette communauté de pratique au moyen de discussions sur des questions juridiques d'intérêt commun, et des initiatives de perfectionnement professionnel et de transfert de connaissances.

Coopération naissante en matière de technologie

174. L'établissement de partenariats permet à la Direction de la technologie de l'OSSNR, en pleine expansion, de recueillir divers points de vue, de collaborer dans la poursuite d'objectifs communs, d'affiner les méthodologies et de s'appuyer sur des pratiques exemplaires établies. En 2022, l'équipe s'est attachée à nouer des relations avec des pairs qui partagent des mandats sur des sujets techniques, notamment les technologies d'amélioration de la confidentialité, la prise de décisions automatisée et la conception de services. Au Canada, elle a notamment collaboré avec la Direction de l'analyse de la technologie du Commissariat à la protection de la vie privée, l'équipe chargée de l'intelligence artificielle au sein du Bureau du dirigeant principal de l'Information du Secrétariat du Conseil du Trésor et le Service numérique canadien.

175. Les collaborations internationales et universitaires ont permis d'accéder aux larges connaissances techniques et à l'expertise d'autres organes d'examen et de surveillance. La gestion des connaissances, le maintien en poste des employés talentueux et l'évolution des capacités techniques sont devenus le point central d'une collaboration régulière avec les équipes de l'Investigatory Powers Commissioner's Office, de l'inspecteur général du renseignement et de la sécurité de l'Australie et de la Commission parlementaire norvégienne de contrôle des services de renseignement et de sécurité. Enfin, 2022 a donné lieu au programme de recherche externe de l'OSSNR visant à orienter et à soutenir les examens déjà en cours grâce à une expertise technique pertinente fournie en temps opportun. En s'appuyant sur les efforts déployés l'année dernière, la Direction de la technologie entend continuer à établir des partenariats au pays et à l'étranger, notamment en élargissant son réseau d'universitaires, de représentants de la société civile et de dirigeants commerciaux, afin de s'assurer que les enjeux technologiques clés sont pris en compte dans ses approches.

06 //

Conclusion

176. L'OSSNR, jouant son rôle dans le milieu canadien de la sécurité et du renseignement, est continuellement motivé par l'importance vitale de son mandat. Cela se manifeste dans chaque examen et chaque enquête sur les plaintes qu'il mène à bien. En exécutant sa mission en 2022, il s'est efforcé de mettre en place des pratiques exemplaires dans l'ensemble de l'organisme, et sa croissance et son évolution continuent de le placer en bonne position pour relever de nouveaux défis.

177. Son expérience s'enrichit au fur et à mesure que ses connaissances se développent, et sa confiance en sa capacité à être un chef de file dans le discours sur l'examen et les enquêtes est renforcé. Ses partenariats et ses efforts de mobilisation auprès des entités examinées gagnent en maturité, et il en tire déjà d'importants avantages. L'application des enseignements tirés de ces partenariats ont permis de répéter et d'améliorer ses processus et ses approches. Bien qu'il reste encore beaucoup à faire, les résultats sont encourageants.

178. Lorsque les membres de l'OSSNR examinent les réalisations de l'organisme au cours de la dernière année, ils sont fiers de la diligence et de l'enthousiasme dont le personnel du Secrétariat a fait preuve. Ils ont relevé le défi de l'évolution des circonstances et de la croissance, et l'ont fait avec un professionnalisme remarquable. Tous sont impatients d'entamer l'année à venir et de poursuivre l'important mandat de l'OSSNR.

07 //

Annexes

Annexe A : Abréviations

Abréviation	Nom complet
AM	Autorisation ministérielle
AMC	Affaires mondiales Canada
ARC	Agence du revenu du Canada
ASFC	Agence des services frontaliers du Canada
CANAFE	Centre d'analyse des opérations et déclarations financières du Canada
CCC	Centre canadien pour la cybersécurité
CCETP	Commission civile d'examen et de traitement des plaintes relatives à la GRC
CCDP	Commission canadienne des droits de la personne
CCRIE	Comité consultatif sur les risques – Information de l'étranger
CEMD	Chef d'état-major de la défense
COA	Cyberopérations actives
COD	Cyberopérations défensives
CPPC	Cadre de pouvoirs et de planification commun
CPSNR	Comité des parlementaires sur la sécurité nationale et le renseignement
CST	Centre de la sécurité des télécommunications
DSJ	Direction des services juridiques
FAC	Forces armées canadiennes
GLCSN	Groupe litiges et conseils en sécurité nationale (ministère de la Justice)
GRC	Gendarmerie royale du Canada
INC	Information nominative sur un Canadien

IRCC	Immigration, Réfugiés et Citoyenneté Canada
IRCPC	Information qui se rapporte à un Canadien ou à une personne se trouvant au Canada
JUS	Ministère de la Justice
LCISC	*Loi sur la communication d'information ayant trait à la sécurité du Canada*
LCMTIEE	*Loi visant à éviter la complicité dans les cas de mauvais traitements infligés par des entités étrangères*
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
SCRS	Service canadien du renseignement de sécurité
SIGINT	Renseignement d'origine électromagnétique
SP	Sécurité publique Canada
SSD	Sous-section des déposants
TI	Technologie de l'information

Annexe B : Aperçu financier, dotation, réalisations et priorités

Aperçu financier

179. Le Secrétariat de l'OSSNR est organisé en fonction de deux principaux secteurs d'activité : la gestion du mandat et les services internes. Le tableau ci-dessous présente une comparaison des dépenses effectuées en 2021 et en 2022 pour chacun de ces deux secteurs d'activité.

(en dollars)	Dépenses (2022)	Dépenses (2021)
Gestion du mandat	7 679 950	7 523 552
Services internes	11 033 465	8 926 178
Total	**18 713 415**	**16 449 730**

180. Au cours de l'année civile 2022, les dépenses du Secrétariat se sont élevées à 18,7 millions de dollars, ce qui représente une augmentation de 2,3 millions de dollars (14 %) par rapport aux dépenses de 16,4 millions de dollars en 2021. Cette augmentation des dépenses est principalement attribuable à l'intensification d'un important projet d'infrastructure et à un recours accru aux services externes pour les activités organisationnelles.

Dotation

181. En date du 30 juin 2023, le personnel du Secrétariat de l'OSSNR comptait 76 employés. Pour tenter de résoudre les problèmes d'embauche et de maintien en poste, le Secrétariat a mis en œuvre plusieurs initiatives, notamment l'entrée en vigueur d'un programme de perfectionnement interne pour les employés du secteur de la gestion du mandat. Ce programme vise à promouvoir les employés en place après qu'ils ont acquis les connaissances et compétences requises pour être promus. Le programme est personnalisé et s'appuie sur un examen régulier des progrès réalisés par rapport à l'atteinte des attentes en matière de connaissances et de compétences de base. Le Secrétariat a également lancé un programme visant à embaucher des personnes titulaires depuis peu d'un doctorat dans des domaines d'expertise présentant un intérêt pour le mandat de l'OSSNR.

182. Le Secrétariat continue également à utiliser des stratégies, des procédures et des pratiques de dotation modernes et souples. Il a adapté ses opérations et ses activités pour permettre, dans la mesure du possible, d'adopter un modèle de travail hybride et flexible.

183. Une définition plus claire de ses profils de compétences de base ainsi que de ses méthodologies et de ses pratiques opérationnelles a également permis une intégration plus efficace des employés au sein de l'organisation.

184. Ayant embauché un employé chargé de la mise en œuvre d'un programme de mieux-être des employés et d'un comité actif de santé mentale et de mieux-être, plusieurs initiatives ont été mises en œuvre dans le but de favoriser le bien-être au travail et d'accroître les interactions entre les employés.

Progrès en ce qui a trait aux initiatives fondamentales

Accessibilité, équité en matière d'emploi, diversité et inclusion

185. En se fondant sur son plan d'action triennal et ses engagements envers le greffier du Conseil privé, le comité interne du Secrétariat chargé de l'accessibilité, de l'équité en matière d'emploi, de la diversité et de l'inclusion a invité des personnes et mené des discussions dans le but d'accroître la sensibilisation, de célébrer la diversité de l'effectif du Secrétariat et de cerner les obstacles et les solutions en ce qui concerne ces thèmes.

186. L'OSSNR a également pris des mesures concrètes dans le cadre des activités qui s'inscrivent dans son mandat afin d'inclure, entre autres, une analyse comparative entre les sexes Plus dans la conception et la mise en œuvre de ses politiques et de ses programmes. Le plan d'examen prospectif renouvelé de l'OSSNR s'appuie donc sur des considérations liées à la lutte contre le racisme, à l'équité et à l'inclusion. Ces considérations s'appliquent au processus de sélection des examens à entreprendre, ainsi qu'à l'analyse effectuée dans le cadre des examens individuels. Les examens de l'OSSNR tiennent régulièrement compte de la possibilité que les activités en matière de sécurité nationale ou de renseignement aboutissent à des résultats disparates pour les différentes communautés et continueront à le faire au cours de l'année à venir.

187. En 2022, l'OSSNR a également poursuivi sa collaboration avec un autre organisme d'examen afin d'élaborer des stratégies pour la collecte, l'analyse et l'utilisation des données sur l'identité. Le but de l'exercice est de s'appuyer sur des consultations publiques pour déterminer comment le public perçoit la collecte, l'analyse et l'utilisation des données sur l'identité dans le cadre du mandat.

188. Enfin, le Secrétariat a également élaboré et publié son premier plan d'accessibilité sur le site Web externe de l'OSSNR. Ce plan décrit les mesures qui seront prises au cours des

trois prochaines années pour accroître l'accessibilité physique et l'accès à l'information, tant pour les employés de l'organisation que pour la population canadienne en général.

Projets d'installations, technologie et sécurité

189. Le Secrétariat est en train d'aménager des espaces de travail supplémentaires afin de pouvoir accueillir tous ses employés dans un seul immeuble. La phase de construction devrait se terminer à la fin de 2023. Au cours de l'année 2022, le Secrétariat a travaillé en étroite collaboration avec les principaux organismes de sécurité pour s'assurer que l'aménagement correspond aux pratiques exemplaires et aux normes établies.

Transparence et protection de la vie privée

190. Le Secrétariat continue de favoriser la transparence en consacrant des ressources au caviardage, à la déclassification et à la publication des rapports précédents du Comité de surveillance des activités de renseignement de sécurité, en plus de la publication proactive des examens de l'OSSNR. En 2022, une importante mise à jour du site Web externe de l'OSSNR a été entamée dans le but d'améliorer l'accès à l'information, y compris l'accès aux rapports d'examen caviardés et aux recommandations. Le site Web devrait être publié en 2023.

191. Pour ce qui est de la protection de la vie privée, le Secrétariat de l'OSSNR a continué à progresser à la suite de l'exercice d'évaluation des facteurs relatifs à la vie privée réalisé au cours de l'exercice 2021-2022 en ce qui concerne les activités d'examen et les services internes. Il a aussi entamé une évaluation des facteurs relatifs à la vie privée pour la fonction d'enquêtes. Les travaux devraient se terminer au cours de l'exercice 2023-2024.

192. Compte tenu de l'importance de la protection de la vie privée dans le cadre de ses activités, l'OSSNR a pris des mesures concrètes pour mettre en œuvre des pratiques exemplaires afin de protéger la vie privée des personnes dans le cadre des enquêtes sur les plaintes et dans le cadre de la réalisation des examens.

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

La présente annexe dresse une liste complète des conclusions et des recommandations découlant des examens de l'Office de surveillance des activités en matière de sécurité nationale et de renseignement (OSSNR) achevés en 2022, ainsi que des réponses de la direction des entités examinées à ses recommandations, dans la mesure du possible au moment de la publication du présent rapport. L'OSSNR mettra à jour cette information pour tous les examens à mesure qu'ils sont publiés sur son site Web.

Examen visant le Service canadien du renseignement de sécurité

Examen annuel des mesures de réduction de la menace

Conclusions de l'OSSNR

1. L'OSSNR constate que, dans l'ensemble, le Service canadien du renseignement de sécurité (SCRS) a utilisé son mandat concernant les MRM en 2021 de la même manière qu'au cours des années précédentes.

2. Pour tous les cas examinés, l'OSSNR constate que le SCRS a rempli ses obligations en vertu de la loi, en particulier la *Charte canadienne des droits et libertés* et les articles 12.1 et 12.2 de la Loi sur le SCRS.

3. Pour tous les cas examinés, l'OSSNR constate que le SCRS a suffisamment établi un « lien rationnel » entre la mesure proposée et la menace cernée.

4. Pour les cas 1 et 2, l'OSSNR constate que le SCRS a rempli ses obligations en vertu des instructions du ministre sur les opérations et la reddition de comptes de 2015 et des instructions du ministre de 2019 concernant la reddition de comptes communiquées par le ministre de la Sécurité publique.

5. Pour le cas 3, l'OSSNR constate que le SCRS n'a pas rempli ses obligations en vertu des instructions du ministre sur les opérations et la reddition de comptes de 2015 et des instructions du ministre de 2019 concernant la reddition de comptes communiquées par le ministre de la Sécurité publique.

6. En ce qui concerne les évaluations des risques juridiques, l'OSSNR constate que davantage de spécificité quant aux risques juridiques et des directives sur la manière dont ces risques peuvent être atténués ou évités a permis de produire des rapports plus détaillés sur les résultats en matière de conformité juridique.

7. Pour les cas 2 et 3, l'OSSNR constate que le SCRS n'a pas rempli ses obligations en ce qui concerne une exigence de la conduite de ses opérations, l'article 12.1 Mesures de réduction de la menace, version 4. Le SCRS n'a pas respecté les exigences de sa politique interne concernant les échéances de présentation des rapports sur la mise en œuvre des MRM.

8. Pour le cas 3, l'OSSNR constate que le rapport sur les résultats attendus n'a pas été produit en temps voulu.

9. L'OSSNR constate que la politique actuelle concernant la production des rapports sur l'incidence stratégique peut empêcher la communication en temps opportun d'information importante.

Recommandations de l'OSSNR

Recommandation
Recommandation 1 : L'OSSNR recommande que des évaluations formelles des risques juridiques soient effectuées pour les MRM impliquant des [*facteurs de nature sensible*].
Recommandation 2 : L'OSSNR recommande au SCRS de procéder à un examen et d'évaluer si les évaluations des risques juridiques dans le cadre de la modernisation des MRM sont conformes aux instructions ministérielles applicables.
Recommandation 3 : L'OSSNR recommande au SCRS de collaborer avec le ministère de la Justice afin de s'assurer que l'évaluation des risques juridiques comprend des directives claires et précises sur les risques juridiques possibles et sur la manière de les éviter ou de les atténuer pendant la mise en œuvre de la MRM.
Recommandation 4 : L'OSSNR recommande de préciser dans les rapports sur la mise en œuvre comment les risques juridiques cernés dans l'évaluation des risques juridiques ont été évités ou atténués au cours de la mise en œuvre de la MRM.
Recommandation 5 : L'OSSNR recommande au SCRS de préciser à l'article *12.1 Mesures de réduction de la menace, Conduite des opérations* quand le rapport sur les résultats attendus doit être produit, comme il le fait pour le rapport sur l'incidence stratégique.
Recommandation 6 : L'OSSNR recommande au SCRS d'intégrer dans sa politique l'exigence voulant que le rapport sur l'incidence stratégique doive être produit à la date d'expiration du pouvoir lié à la MRM.

Examens visant le Centre de la sécurité des télécommunications

Examen de la gouvernance des cyberopérations actives et des cyberopérations défensives du Centre de la sécurité des télécommunications – partie 2

Conclusions de l'OSSNR

1. L'OSSNR constate que le processus d'évaluation des risques sur le plan de la politique étrangère d'Affaires mondiales Canada, ainsi que l'évaluation connexe portant sur le droit international, se sont améliorés depuis l'examen de la gouvernance, pour les cyberopérations actives (COA) et les cyberopérations défensives (COD) du Centre de la sécurité des télécommunications (CST).

2. L'OSSNR constate qu'Affaires mondiales Canada n'a pas la capacité d'évaluer de manière indépendante les risques potentiels découlant des techniques utilisées dans le cadre des COA et des COD du CST.

3. L'OSSNR constate que le CST et le ministère de la Justice ont fait preuve d'une compréhension approfondie de l'article 32 de la Loi sur le CST. Toutefois, le CST ne consulte pas comme il se doit le ministère de la Justice lors de [*étape spécifique*][15] pour s'assurer que l'évaluation de la conformité juridique demeure valide.

4. L'OSSNR constate que les demandes du CST visant des autorisations délivrées en vertu des paragraphes 29(1) et 30(1) de la Loi sur le CST pour les activités de [*description*] ne comprenaient pas toute l'information disponible pertinente pour une évaluation significative des exigences des paragraphes 34(1) et (4) de la Loi sur le CST.

5. L'OSSNR constate qu'il existe un risque de chevauchement entre les activités du CST et celles du SCRS dans le contexte des capacités utilisées par le CST pour exécuter ses COA et COD. Toutefois, le CST n'a pas toujours consulté le SCRS au sujet de ses cyberopérations.

6. L'OSSNR constate qu'en dépit d'une étroite collaboration avec Affaires mondiales Canada, le ministère de la Défense nationale et les Forces armées canadiennes en ce qui a trait aux COA et aux COD, le CST n'a pas entretenu un dialogue cohérent avec le SCRS ou la Gendarmerie royale du Canada (GRC) pour déterminer si l'objectif d'une COA ou d'une COD ne pourrait raisonnablement pas être atteint par d'autres moyens.

7. L'OSSNR constate que les demandes du chef concernant les activités liées aux cyberopérations actives et défensives pour la période examinée ne décrivent pas avec précision le lien entre une cyberopération et la collecte de renseignements.

8. L'OSSNR constate que, dans son [*un document spécifique*], le CST n'a pas toujours fait preuve de clarté en ce qui concerne les missions de renseignement étranger.

9. L'OSSNR constate que les COA et les COD du CST planifiées ou réalisées avant le 30 juillet 2021, y compris les études de cas analysées dans le présent rapport, étaient légales.

10. L'OSSNR constate qu'il existe un chevauchement important entre les activités menées dans le cadre des volets COA et COD du mandat du CST, ainsi qu'entre les quatre volets du mandat du CST.

Recommandations de l'OSSNR et réponses du CST

Recommandation	Réponse du CST et d'AMC (21 juin 2023)
Recommandation 1 : L'OSSNR recommande qu'AMC perfectionne ses capacités ou en élabore de nouvelles pour être en mesure d'évaluer en toute indépendance les risques pouvant découler des techniques employées par le CST en cours de COA ou de COD.	**En désaccord.** Le CST et AMC ne sont pas d'accord avec cette recommandation. Conformément avec le cadre de gouvernance CST-AMC, AMC évalue les cyberopérations du CST sur le plan des risques relatifs aux politiques étrangères et de la conformité avec les lois internationales. Le processus interne d'évaluation des risques du CST évalue les risques techniques des cyberopérations selon les techniques employées. Tout comme le CST compte sur AMC pour lui offrir son expertise sur le plan de la politique étrangère et de lois internationales, AMC compte sur le CST pour lui offrir son expertise sur le plan des technologies et des techniques à l'avant-plan des développements. L'évaluation juste de tous les risques liés à une cyberopération se fonde sur la poursuite d'un dialogue ouvert et honnête et sur la confiance entre AMC et le CST. C'est pourquoi le CST continuera de transmettre de l'information à AMC concernant les techniques, lorsque leur utilisation pourrait avoir des répercussions sur l'évaluation des risques sur le plan de la politique étrangère d'AMC.
Recommandation 2 : L'OSSNR recommande que le	**D'accord en principe.** Le CST est d'accord avec

Recommandation	Réponse du CST et d'AMC (21 juin 2023)
ministère de la Justice soit pleinement consulté à toutes les étapes d'une COA ou d'une COD, particulièrement à celles qui sont en amont de l'exécution de l'opération.	cette recommandation en principe. Le CST est d'avis que les avis et les conseils offerts par les représentantes et représentants du ministère de la Justice (JUS) au sein de la Direction des services juridiques (DSJ) du CST sont intégraux à la réussite de la mission du CST. Le CST consulte la DSJ à toutes les étapes pertinentes d'une cyberopération. De manière générale, le CST consulte la DSJ par l'entremise du cadre de pouvoirs et de planification commun (CPPC) à une étape clé. Plus de consultations ont lieu lorsqu'une activité est nouvelle. Les outils internes développés par la DSJ permettent de veiller à ce que les activités ne contreviennent pas aux interdictions énoncées dans la Loi sur le CST et aident les analystes à détecter les risques élevés qui nécessitent un examen juridique approfondi. De plus, l'équipe interne du CST responsable des politiques opérationnelles est consultée lors de toutes étapes clés.
Recommandation 3 : L'OSSNR recommande que le CST renonce à la pratique donnant lieu à la présentation de demandes de COA et de COD génériques (c. à d. au ministre de la Défense nationale, et qu'il soumette plutôt des demandes ponctuelles	**En désaccord.** Le CST et AMC ne sont pas d'accord avec cette recommandation. Au moment de soumettre une application afin d'obtenir une autorisation ministérielle (AM) liée à ce genre de COA ou COD, le CST et AMC veillent toujours à ce que les ministres de la Défense nationale et des Affaires étrangères aient toute l'information nécessaire pour prendre une décision éclairée quant à la nature raisonnable et proportionnelle des activités proposées pas le CST par rapport à un ensemble d'objectifs précis. À cet effet, les AM liées à ce genre de COA ou COD s'articulent autour de grands objectifs visant à contrer de nombreuses menaces clairement définies dans un contexte mondial. En ce sens, elles ne sont pas « génériques », mais leur portée est suffisamment large pour accorder au CST la souplesse d'intervenir contre un grand nombre de

Recommandation	Réponse du CST et d'AMC (21 juin 2023)
	cibles, dans un contexte où l'identité des auteures et auteurs de menace ou le lieu et le contexte sont inconnus au moment de soumettre l'application. Dans le cas de toute opération évaluée comme relevant de l'autorité de ces AM, le cadre de gouvernance actuel permet la gestion appropriée des risques de l'opération. Le CST fournit à AMC des plans de mission détaillés de chaque opération, afin de bien évaluer les risques sur le plan de la politique étrangère en lien avec les cyberopérations du CST. À la suite de la recommandation 1 de l'examen de gouvernance (FCO 1), le CST et AMC ont augmenté la quantité d'information inscrite dans l'application 2021 pour cet AM. Le degré de détail demandé a augmenté davantage pour l'application 2022. De plus, le CST et AMC collaborent sur de nouvelles AM visant à garantir que les objectifs pertinents sur le plan de la politique étrangère concordent et que les opérations autorisées ont une portée suffisante. Si une activité ne correspond pas à la catégorie correspondant à ces AM, le CST soumettra une nouvelle application particulière à la situation.
Recommandation 4 : L'OSSNR recommande que le CST prenne invariablement contact avec le SCRS, la GRC et tout autre ministère ou organisme concerné du gouvernement fédéral pour déterminer si ces ministères et organismes seraient raisonnablement en mesure d'atteindre l'objectif d'une cyberopération.	**D'accord.** Le CST est d'accord avec cette recommandation. Le CST reconnaît l'importance de consulter tous les intervenants pertinents du gouvernement du Canada. Au cours de la planification d'une opération, le CST renforce et continuera de renforcer ses liens de collaboration avec ses partenaires, notamment en communiquant avec le SCRS, la GRC et tout autre ministère ou organisme fédéral dont le mandat pourrait coïncider avec une COA ou une COD prévue.
Recommandation 5 : L'OSSNR recommande que les demandes présentées par le chef concernant les cyberopérations actives et défensives indiquent	**D'accord.** Le CST et AMC sont d'accord avec cette recommandation. Les applications 2022-2023 d'AM liées aux COA

Recommandation	Réponse du CST et d'AMC (21 juin 2023)
au ministre de la Défense nationale qu'une acquisition d'information au titre d'une autorisation dûment délivrée pour le renseignement étranger, la cybersécurité ou l'assurance de l'information pourrait avoir lieu en conséquence desdites cyberopérations.	et COD appliquent déjà cette recommandation.
Recommandation 6 : L'OSSNR recommande que les documents préparés selon le cadre des cyberopérations du CST (le Cadre de pouvoirs et de planification commun) fournissent en toute clarté les liens avec toutes les missions de renseignement étranger (ou de cybersécurité) concernées qui pourraient se dérouler en même temps que les COA ou les COD.	**D'accord.** Le CST est d'accord avec cette recommandation. Depuis la période faisant l'objet d'un examen, le CST a mis en œuvre ce changement dans son cadre pour les cyberopérations, en partie en raison des recommandations de l'OSSNR présentées dans l'examen de gouvernance (FCO 1). Selon le cadre actuel, les documents comprennent maintenant des liens vers les opérations en vertu des articles 16 ou 17 qui sont pertinentes aux cyberopérations réalisées en vertu des articles 18 ou 19.
Recommandation 7 : L'OSSNR recommande que le CST continue de définir et de perfectionner les distinctions qu'il convient d'établir entre les activités menées au titre des divers volets de son mandat, particulièrement entre les activités des COA et des COD, mais aussi entre les activités de renseignement étranger et de cybersécurité.	**D'accord en principe.** Le CST est d'accord avec cette recommandation en principe. Le CST est d'accord avec le principe de comprendre les nuances de son mandat. La Loi sur le CST (articles 15 à 20) précise les cinq volets de son mandat. Les opérations sont planifiées selon la compréhension de la portée et des limites que le volet du mandat autorise. Le CST collabore étroitement avec la Direction des services juridiques (DSJ) et son équipe responsable des politiques opérationnelles afin de garantir que les opérations sont planifiées et effectuées en vertu des pouvoirs pertinents. Dans le corps de son rapport, l'OSSNR reconnaît la clarté de la Loi et la capacité du CST d'expliquer les raisons qui sous-tendent l'autorisation d'une opération selon un volet précis de son mandat. Les politiques et les procédures du CST permettant de planifier et de mener des opérations se fondent sur les distinctions entre les volets du mandat. L'ensemble des politiques

Recommandation	Réponse du CST et d'AMC (21 juin 2023)
	relatives à la mission du CST traite de chaque volet du mandat et présente des distinctions entre les COA et COD. Le cadre pour les cyberopérations propose des documents de planification qui établissent les raisons pour lesquelles les objectifs et la nature de l'opération prévue concordent avec les pouvoirs liés à une COA comparativement à une COD, sans compter les techniques utilisées. Enfin, le CST est en voie de lancer une formation actualisée sur les lois et les politiques à l'intention de son personnel opérationnel.

Examen d'une activité en matière de renseignement étranger

Conclusions de l'OSSNR

1. L'OSSNR constate que le CST n'a pas renseigné le ministre de la Défense nationale depuis [*année*] sur ses relations avec un partenaire étranger.

2. L'OSSNR constate que, dans le cadre d'une opération conjointe, les échanges analytiques du CST avec un partenaire n'ont pas respecté toutes les exigences stratégiques internes du CST concernant de tels échanges avec ses partenaires.

3. L'OSSNR constate que les demandes d'autorisation touchant le renseignement étranger adressées par le CST au ministre de la Défense nationale ne décrivaient pas toute l'étendue de la participation du CST à [*activité spécifique*].

4. L'OSSNR constate que le CST n'a pas correctement appliqué son processus d'évaluation du risque de mauvais traitements à l'information échangée avec un partenaire étranger. Le CST n'a procédé à une évaluation du risque de mauvais traitements qu'après avoir déjà échangé une quantité importante d'information avec ce partenaire.

5. L'OSSNR constate que le CST n'a pas justifié de manière appropriée le risque de mauvais traitements pour les cibles d'une opération.

6. [*Cette conclusion ne peut être communiquée dans un rapport public.*]

7. L'OSSNR constate que le CST ne dispose pas d'un mécanisme permettant de procéder rapidement à une vérification concrète du statut au Canada d'une personne afin de s'assurer que ses activités ne visent pas des Canadiens.

8. L'OSSNR constate que le CST n'a pas élaboré de politiques et de procédures régissant sa participation à [*activité spécifique*].

9. L'OSSNR constate que les contributions du CST aux opérations avec ses partenaires ne sont régies par aucune entente écrite concernant les activités opérationnelles.

10. L'OSSNR constate que les contributions du CST aux opérations menées par un partenaire n'étaient pas accompagnées de la planification opérationnelle et de l'évaluation des risques décrites par le CST au ministre de la Défense nationale.

11. L'OSSNR constate que le CST n'obtient pas les plans opérationnels ou les évaluations des risques élaborés par ses partenaires qui dirigent les opérations, et ne contribue pas non plus à l'élaboration de ces plans ou des paramètres connexes.

12. L'OSSNR constate que la demande d'autorisation du CST n'indiquait pas au ministre de la Défense nationale son intention de mener des activités d'essai et d'évaluation au titre de l'autorisation.

Recommandations de l'OSSNR et réponses du CST

Recommandation	Réponse du CST (14 mars 2023)
Recommandation 1 : Le CST devrait renseigner le ministre de la Défense nationale sur ses relations avec un partenaire étranger.	**D'accord.** Le CST est d'accord avec cette recommandation. Le CST est d'accord et renseigne régulièrement le ministre sur des sujets importants, notamment sur l'état des relations avec les partenaires étrangers. Le CST prévoit de continuer à fournir au ministre des mises à jour complètes sur ses efforts de mobilisation à l'échelle internationale et ses relations avec les partenaires étrangers, y compris avec le partenaire étranger en question.
Recommandation 2 : Le CST devrait se conformer aux exigences en matière de produits SIGINT communicables conformément à l'ensemble des politiques relatives à la mission en matière de	**D'accord.** Le CST est d'accord avec cette recommandation. Le CST reconnaît qu'en dépit de solides politiques, pratiques et procédures, des améliorations

Recommandation	Réponse du CST (14 mars 2023)
renseignement étranger lorsqu'il procède à des échanges analytiques avec ses partenaires dans le cadre de l'exécution de toutes les activités opérationnelles.	peuvent encore être apportées en matière de sensibilisation et de formation du personnel de mission. Le CST effectue actuellement une révision complète de sa formation juridique et stratégique opérationnelle et tiendra compte de cette recommandation lors de l'élaboration de ses plans en matière de conformité pour 2023-2024.
Recommandation 3 : Le CST devrait indiquer au ministre de la Défense nationale toute l'étendue de sa participation à des activités lorsqu'il demande des autorisations relatives au renseignement étranger.	**D'accord.** Le CST est d'accord avec cette recommandation. Le CST fournira des détails pertinents pour préciser [*activités spécifiques*] dans sa prochaine demande d'autorisation ministérielle, à un niveau de détail correspondant aux demandes d'autorisation ministérielle.
Recommandation 4 : Le CST doit procéder à une évaluation du risque de mauvais traitements avant d'échanger de l'information avec [*pays*], conformément aux paramètres établis avec le ministre de la Défense nationale, le ministre des Affaires étrangères et le Bureau du Conseil privé lors de l'élaboration de l'entente de travail entre le CST et ce partenaire.	**D'accord en principe.** Le CST est d'accord avec cette recommandation en principe. Le CST estime que ses instruments stratégiques sont déjà clairs et que des pratiques exemplaires sont déjà en place pour l'échange d'information avec des entités étrangères sur des personnes identifiables. Le CST cherche toujours à améliorer la mise en œuvre des politiques internes, ainsi que les programmes de formation et de sensibilisation interne s'adressant à ses analystes. Il est également important de souligner la présence d'un fort facteur atténuant dans les ententes globales conclues avec [*pays*], qui contiennent des dispositions explicites sur la manière dont le SIGINT peut être utilisé, ainsi que des interdictions explicites concernant les fins susceptibles de donner lieu à des mauvais traitements.
Recommandation 5 : Lors de l'évaluation du risque de mauvais traitements, le CST devrait préciser pourquoi et comment sa cote de risque s'applique à chaque personne participant à l'échange	**D'accord en principe.** Le CST est d'accord avec cette recommandation en principe. Depuis 2011, le CST n'a cessé d'affiner son processus d'évaluation du risque de mauvais

Recommandation	Réponse du CST (14 mars 2023)
d'information avec un partenaire étranger.	traitements et la documentation connexe. Dans certains cas, lorsqu'une évaluation initiale a permis de déterminer que toutes les conditions de l'échange d'information seront identiques pour une catégorie de personnes dans le cadre d'une activité, le CST a établi qu'une évaluation collective du risque de mauvais traitements indique de manière appropriée les profils de risque de toutes les personnes associées à cette activité. Si les conditions relatives à l'échange d'information changent ou si des caractéristiques spécifiques liées à une personne associée à l'activité peuvent modifier le risque, une évaluation distincte est effectuée. Le CST a poursuivi l'amélioration de la documentation afin de mieux refléter l'analyse qui sous-tend l'évaluation du risque et la raison pour laquelle une justification s'applique à un groupe de personnes dans le cadre d'une activité unique. Au fur et à mesure que les activités opérationnelles du CST évoluent, le processus d'évaluation du risque de mauvais traitements s'enrichit en fonction des exigences de ces activités.
Recommandation 6 : Le CST devrait veiller à ce qu'une évaluation du caractère étranger soit réalisée avant de commencer à recueillir des données et à établir des rapports sur des personnes. Le CST devrait également définir des exigences stratégiques pour la documentation, le suivi et l'examen par la direction des évaluations du caractère étranger.	**D'accord en principe.** Le CST est d'accord avec cette recommandation en principe. Dans le cadre du processus SIGINT, et en s'appuyant sur une combinaison de moyens stratégiques, administratifs et technologiques, le CST documente déjà une justification de ciblage démontrant des motifs raisonnables de croire qu'une cible est une entité étrangère à l'extérieur du Canada. Cette justification vérifiable cristallise l'état actuel des connaissances sur le caractère étranger d'une cible, au moment du ciblage. De plus, au fur et à mesure que les analystes accomplissent leurs tâches et acquièrent des connaissances sur une cible, une évaluation du caractère étranger est effectuée tout au long de

Recommandation	Réponse du CST (14 mars 2023)
	l'analyse SIGINT dans le cadre d'un processus guidé par l'ensemble des politiques relatives à la mission. Chaque nouveau fragment d'information acquis sur une cible s'ajoute à l'ensemble de connaissances évalué par un analyste, et fournit notamment de l'information sur le caractère étranger d'une cible qui n'était peut-être pas disponible au moment du ciblage. Si, à un moment donné, l'analyste n'a plus de motifs raisonnables de croire que la cible est une entité étrangère située en dehors du Canada, il doit « décibler » les sélecteurs connexes et signaler un incident lié à la protection des renseignements personnels à l'équipe chargée du programme de conformité opérationnelle du CST, qui orientera les processus internes quant aux mesures correctives supplémentaires requises, telles que l'élimination de toute information recueillie. De plus, une vérification de la citoyenneté peut également être demandée à Immigration, Réfugiés et Citoyenneté Canada (IRCC) si l'information disponible est suffisante.
Recommandation 7 : Le CST devrait élaborer un mécanisme avec Immigration, Réfugiés et Citoyenneté Canada, ou d'autres institutions fédérales le cas échéant, afin de permettre de confirmer rapidement et concrètement le statut au Canada des personnes impliquées dans les activités opérationnelles du CST.	**D'accord.** Le est d'accord avec à cette recommandation. Cette recommandation a déjà été formulée dans le rapport final sur la LCISC de 2020. Le CST poursuit ses discussions avec IRCC en vue d'une entente d'échange d'information. Le CST relance le dialogue à l'échelon opérationnel et de direction pour faire avancer ce dossier. Il convient de reconnaître que pour produire des résultats plus exacts, un contrôle de la citoyenneté doit inclure de l'information spécifique sur une cible individuelle, ce dont le CST ne dispose pas toujours. En l'absence de cette information, on ne peut pas garantir que le contrôle de la citoyenneté produise des résultats concluants et il ne peut pas être considéré comme une confirmation concrète du statut de citoyenneté. De plus, le CST croit

Recommandation	Réponse du CST (14 mars 2023)
	savoir que les bases de données d'IRCC ne recensent peut-être pas les Canadiens nés avec la citoyenneté canadienne. Le processus de vérification de la citoyenneté et les délais connexes relèvent entièrement de la compétence d'IRCC.
Recommandation 8 : Le CST devrait élaborer des politiques et des procédures régissant sa participation à [*activités spécifiques*] dans le cadre du programme.	**D'accord.** Le CST est d'accord avec cette recommandation. Le CST demeure déterminé à mettre en œuvre de solides cadres stratégiques pour régir ses activités et s'assurer que son travail se poursuit au plus haut niveau d'intégrité. Bien qu'au moment de l'examen, les politiques et procédures propres au programme étaient toujours en cours d'élaboration, les politiques et procédures actuelles du CST comprennent des principes qui régissent toutes les activités en matière de renseignement étranger menées sous l'autorité du CST, y compris [*programme*].
Recommandation 9 : Le CST devrait conclure des ententes écrites avec ses partenaires participant aux activités, afin de définir les paramètres de la collaboration à ces activités.	**En désaccord.** Le CST est en désaccord avec cette recommandation. Le CST entretient des relations particulièrement solides avec ses partenaires depuis [*durée*]. Le Canada bénéficie grandement de cette mise en commun des capacités qui multiplie de manière exponentielle sa capacité à fournir de l'information de qualité. La coopération avec nos partenaires signifie que nous [*description*], et des procédures sont en place pour gérer nos interactions. Les opérations du CST avec ses partenaires reposent sur des ententes bilatérales d'échange d'information et de coopération technique.
Recommandation 10 : Lors de la collaboration avec un partenaire dans le cadre d'une opération, le CST devrait préparer un plan opérationnel et procéder à une évaluation des risques liés à l'activité afin de s'assurer que l'opération est conforme aux priorités	**D'accord.** Le CST est d'accord avec cette recommandation. La politique du CST prévoit que, lors de l'exécution d'opérations SIGINT, y compris d'opérations

Recommandation	Réponse du CST (14 mars 2023)
du CST et à ses niveaux de tolérance au risque. Le CST devrait également s'assurer que les paramètres et les éventuelles mises en garde concernant [*activité spécifique*] du partenaire sont décrits et compris.	conjointes avec un partenaire, l'activité doit être approuvée par le biais d'un plan opérationnel et d'une évaluation des risques afin d'exercer un volet du mandat du CST. Dans le cadre d'une collaboration visant [*activité spécifique*] sans participation à l'opération qui en découle, CST n'a pas à créer de plans opérationnels ou d'évaluations des risques. Cela incombe plutôt à l'organisme partenaire qui mène l'opération et en assume le risque. Le CST s'assurera toutefois que l'organisme partenaire est informé de toute mise en garde ou de tout paramètre connexe et qu'il en prend acte.
Recommandation 11 : Lors d'une demande d'autorisation ministérielle, le CST devrait indiquer au ministre toute activité de mise à l'essai ou d'évaluation qu'il a l'intention d'entreprendre en vertu de l'alinéa 23(1)c) de la Loi sur le CST.	**En désaccord.** Le CST est en désaccord avec cette recommandation. L'objectif d'une autorisation ministérielle est de demander des pouvoirs afin de mener des activités qui contreviendraient à une loi fédérale ou impliqueraient l'acquisition d'information portant atteinte aux attentes raisonnables de protection en matière de vie privée d'un Canadien ou de toute personne se trouvant au Canada. Les activités de mise à l'essai, conformément à l'alinéa 23(1)c) de la Loi sur le CST, ne sont pas menées en vertu des pouvoirs conférés par une autorisation ministérielle si elles ne risquent pas de contrevenir à une loi fédérale ou si elles n'impliquent pas l'acquisition d'information qui porterait atteinte aux attentes raisonnables de protection en matière de vie privée d'un Canadien ou d'une personne se trouvant au Canada. Dans de tels cas, il n'est pas nécessaire de demander au ministre des pouvoirs pour mener des activités de mise à l'essai par le biais d'une autorisation ministérielle. Toutefois, à la discrétion du chef, le CST informera le ministre des activités ne reposant pas sur des autorisations ministérielles par d'autres moyens. L'alinéa 23(1)c) prévoit une exception à

Recommandation	Réponse du CST (14 mars 2023)
	l'interdiction faite au CST de mener des activités visant un Canadien ou une personne se trouvant au Canada lorsqu'il met à l'essai ou évalue des produits, des logiciels et des systèmes. Cela signifie que le CST peut mener ces activités qui ne seront pas considérées comme visant un Canadien ou une personne se trouvant au Canada. Toute activité en matière de renseignement étranger, y compris les activités de mise à l'essai, qui contrevient à une loi fédérale ou implique l'acquisition d'information qui porte atteinte aux attentes raisonnables de protection en matière de vie privée d'un Canadien ou d'une personne se trouvant au Canada ne peut être menée qu'en vertu de pouvoirs conférés par une autorisation ministérielle. Dans de tels cas, les activités doivent être menées en vertu de pouvoirs conférés par une autorisation ministérielle existante, ou le ministre doit délivrer une nouvelle autorisation ministérielle. Le ministre serait alors pleinement informé des activités envisagées avant d'être en mesure de les approuver.

Examen visant le ministère de la Défense nationale et les Forces armées canadiennes

Rapport établi au titre de l'article 35 de la Loi sur l'OSSNR

Conclusions de l'OSSNR

1. Le rapport contenait une conclusion selon laquelle, d'après l'OSSNR, certaines activités entreprises par les Forces armées canadiennes pouvaient ne pas être conformes à la loi.

   Réponse du ministère de la Défense nationale/des Forces armées canadiennes (MDN et FAC)

   Le MDN et les FAC reconnaissent l'importance d'un examen indépendant et externe des activités du gouvernement du Canada en matière de sécurité nationale et de renseignement.

Nous soutenons pleinement le mandat d'examen de l'OSSNR et prenons tous ses rapports au sérieux.

Après avoir reçu le rapport de conformité de l'OSSNR en vertu de l'article 35, le MDN et les FAC ont procédé à une analyse complète, et ils sont en désaccord avec l'opinion de l'OSSNR. Notre analyse confirme que les activités examinées ont été menées conformément à la loi dans le cadre d'un système solide de surveillance et de responsabilisation. De plus, un examen externe indépendant antérieur correspondait à notre analyse et soutenait un certain nombre de recommandations qui ont été mises en œuvre pour renforcer le cadre de gouvernance. Le ministre suit les étapes afin de satisfaire à toutes les exigences énoncées à l'article 35 de la Loi.

Examen visant l'Agence des services frontaliers du Canada

Examen du ciblage des passagers aériens

Conclusions de l'OSSNR

1. L'utilisation de données relatives à l'information préalable sur les voyageurs et aux dossiers passagers par l'Agence des services frontaliers du Canada (ASFC) dans le cadre d'un ciblage fondé sur des scénarios était conforme au paragraphe 107(3) de la *Loi sur les douanes*.

2. L'ASFC ne documente pas ses pratiques de triage d'une manière qui permette de vérifier efficacement si toutes les décisions de triage sont conformes aux restrictions légales et réglementaires.

3. L'ASFC n'a pas toujours démontré qu'il existait une justification adéquate pour ses pratiques de triage aux fins de ciblage des passagers aériens. La faiblesse du lien entre les indicateurs utilisés pour trier les passagers et les menaces ou infractions potentielles que l'ASFC cherche à déceler engendre un risque que les pratiques de triage aux fins de ciblage des passagers aériens soient discriminatoires.

4. Les politiques, les procédures et la formation de l'ASFC ne sont pas suffisamment détaillées pour permettre au personnel de l'ASFC de cerner les risques potentiels de discrimination et de prendre des mesures appropriées pour atténuer ces risques dans l'exercice de leurs fonctions.

5. Les structures et pratiques de contrôle de l'ASFC ne sont pas suffisamment rigoureuses pour cerner et atténuer, le cas échéant, les risques potentiels de discrimination. Cette situation est aggravée par l'absence de collecte et d'évaluation de données pertinentes.

Recommandations de l'OSSNR et réponses de l'ASFC

Recommandation	Réponse (Juillet 2022)
Recommandation 1 : L'OSSNR recommande à l'ASFC de documenter ses pratiques de triage d'une manière qui permette de vérifier efficacement si toutes les décisions de triage sont conformes aux restrictions légales et réglementaires.	**D'accord.** L'ASFC procédera à un examen de ses pratiques de triage aux fins de ciblage des passagers aériens afin de s'assurer qu'elles permettent de vérifier efficacement le respect des restrictions légales et réglementaires.
Recommandation 2 : L'OSSNR recommande à l'ASFC de s'assurer, de manière continue, que ses pratiques de triage sont fondées sur de l'information ou du renseignement qui justifie l'utilisation de chaque indicateur. Cette justification devrait être bien documentée afin de permettre une vérification interne et externe efficace de la conformité des pratiques de triage de l'ASFC à ses obligations en matière de non-discrimination.	**D'accord.** Bien que nous soyons convaincus que les pratiques de triage et de ciblage sont justifiées, l'ASFC reconnaît que de meilleures pratiques de documentation pourraient être mises en œuvre pour permettre une vérification interne et externe efficace de la conformité des pratiques de triage de l'ASFC à ses obligations en matière de non-discrimination. Le cadre de gouvernance du ciblage fondé sur des scénarios de l'ASFC sera mis à jour pour inclure de l'information ou du renseignement qui justifie l'utilisation de chaque indicateur. Des examens annuels des scénarios continueront d'être effectués et documentés afin de confirmer que chaque scénario actif est étayé par du renseignement récent et fiable.
Recommandation 3 : L'OSSNR recommande à l'ASFC de s'assurer que toute distinction liée au ciblage des passagers aériens pour des motifs de distinction illicite, susceptible de renforcer, de perpétuer ou d'exacerber un désavantage, constitue une restriction raisonnable aux droits à l'égalité des voyageurs garantis par la Charte.	**D'accord.** L'ASFC examinera ses pratiques en matière de ciblage des passagers aériens afin de s'assurer que les distinctions fondées sur des motifs de distinction illicite sont raisonnables et peuvent être justifiées de manière démontrable dans le contexte de l'administration frontalière et de l'exécution de la loi.
Recommandation 4 : L'OSSNR recommande à l'ASFC d'exercer une surveillance plus rigoureuse et	**D'accord.** L'ASFC reconnaît que les politiques, les procédures, la formation et les autres directives, le

Recommandation	Réponse (Juillet 2022)
régulière du ciblage des passagers aériens afin de s'assurer que ses pratiques ne sont pas discriminatoires. Cela devrait aussi comprendre la mise à jour des politiques, des procédures, de la formation et des autres directives de l'ASFC, le cas échéant.	cas échéant, peuvent être améliorées pour assurer une surveillance rigoureuse et régulière du ciblage des passagers aériens afin de garantir que ses pratiques ne sont pas discriminatoires. L'ASFC procédera à un examen de ses politiques, de ses procédures, de ses lignes directrices et de sa formation afin de s'assurer que les pratiques ne sont pas discriminatoires.
Recommandation 5 : L'OSSNR recommande à l'ASFC de commencer à rassembler et à évaluer les données nécessaires pour cerner, analyser et atténuer les risques de discrimination. Cela inclut des données démographiques ventilées, des données sur les effets du ciblage des passagers aériens sur les examens secondaires qui peuvent transparaître dans les plaintes concernant les droits de la personne, et des données sur un groupe de comparaison de référence.	**D'accord.** À cette fin, l'ASFC prend des mesures délibérées pour renforcer sa capacité à recueillir et à analyser des données fiables et exactes de manière non intrusive. L'Agence s'emploie à élaborer des positions et des cadres normalisés et cohérents pour la collecte, l'utilisation, la gestion et la gouvernance des données ventilées, à mettre au point des paramètres et des indicateurs pour mesurer l'incidence des décisions et des politiques sur différents groupes, à utiliser des données pour élaborer des politiques et des stratégies plus inclusives et plus représentatives, et à repérer les cas possibles de discrimination et de préjugés.

Examens multiministériels

Examen des communications d'information par des institutions fédérales au titre de la *Loi sur la communication d'information ayant trait à la sécurité du Canada* en 2021

Conclusions de l'OSSNR

1. L'OSSNR conclut que dans 12 des 13 communications d'information examinées, AMC avait acquis la certitude que la communication d'information aiderait l'exercice de la compétence ou des attributions de l'institution destinataire à l'égard des activités portant atteinte à la sécurité du Canada, tel qu'il est exigé à l'alinéa 5(1)a) de la LCISC.

2. L'OSSNR conclut que, sans qu'ils aient d'abord mené une analyse en application de l'alinéa 5(1)a) de la LCISC, les ministères risquent de communiquer de l'information qui n'avait pas

trait au mandat en matière de sécurité nationale de l'institution fédérale destinataire ou aux activités portant atteinte à la sécurité du Canada.

3. L'OSSNR conclut que dans une 1 des 13 communications d'information, AMC a consulté plus d'information que nécessaire pour obtenir une confirmation que la communication avait contribué au mandat du SCRS ou qu'elle avait trait aux activités portant atteinte à la sécurité du Canada.

4. L'OSSNR conclut que, dans 10 des 13 communications, AMC était convaincu que l'incidence de la communication sur le droit à la vie privée d'une personne serait limitée à ce qui est raisonnablement nécessaire dans les circonstances, tel qu'il est stipulé à l'alinéa 5(1)b) de la LCISC.

5. L'OSSNR conclut que 2 des 13 communications ne comprenaient aucune déclaration relative à l'exactitude et à la fiabilité, ce qui est contraire au paragraphe 5(2) de la LCISC.

6. L'OSSNR conclut que la formation d'AMC sur la LCISC est dépourvue des exemples illustratifs nécessaires pour fournir aux employés les principes sur lesquels s'appuyer pour répondre à leurs obligations au titre de la LCISC.

Recommandations de l'OSSNR et réponses du gouvernement

Recommandation	Réponse (14 février 2023)
Recommandation 1 : L'OSSNR recommande que les consultations soient limitées à l'information nécessaire pour obtenir une confirmation par le bénéficiaire potentiel que l'information contribue à son mandat et a trait aux activités qui portent atteinte à la sécurité du Canada.	**D'accord.** Le *Guide LCISC 2022 étape par étape* de Sécurité publique (« Guide LCISC 2022 ») a été mis à jour et distribué aux institutions fédérales en octobre 2022. Plusieurs mises à jour du Guide LCISC 2022, qui étaient fondées sur les commentaires des utilisateurs, répondent directement à cette recommandation. Le Guide LCISC 2022 mis à jour précise que les consultations préliminaires avant une communication ne devraient inclure que des informations générales pour s'assurer que les critères de la LCISC sont atteints avant que l'institution communicante ne procède à la communication. De plus, le matériel de formation LCISC a été mis à jour en septembre 2022 avec un accent renouvelé sur la nécessité pour les institutions

Recommandation	Réponse (14 février 2023)
	communicantes de limiter strictement les informations communiquées aux institutions destinataires lors des consultations préliminaires. Plusieurs formations LCISC ont été dispensées aux institutions fédérales en utilisant le nouveau matériel. Sécurité publique continuera de travailler avec les institutions fédérales pour leur donner accès à de la formation, des conseils et à d'autres ressources utiles sur l'utilisation de la LCISC. Étant donné l'objectif de cet examen, Sécurité publique travaillera en étroite collaboration avec AMC pour répondre à cette recommandation.
Recommandation 2 : L'OSSNR recommande que les déclarations relatives à l'exactitude et à la fiabilité soient claires et propres aux circonstances de la communication afin d'offrir le contexte le plus utile et satisfaisant pour l'institution destinataire.	**D'accord.** Les déclarations concernant l'exactitude des informations et la fiabilité de la manière dont elles ont été obtenues sont une partie essentielle du processus de communication. Pour assurer une plus grande conformité à cette exigence, le Guide LCISC 2022 et ses modèles connexes, ainsi que le matériel de formation LCISC mis à jour, soulignent l'importance de fournir des déclarations sur l'exactitude des informations et la fiabilité de la manière dont elles ont été obtenues qui sont claires et spécifiques aux circonstances de la communication. Sécurité publique continuera à fournir une formation et des conseils sur la LCISC aux institutions fédérales afin de souligner l'exigence de déclarations d'exactitude et de fiabilité qui sont claires, complètes, précises et qui n'incluent pas de libellés préétablis à l'appui des communications en vertu de la LCISC.
Recommandation 3 : L'OSSNR recommande que tous les ministères communiquant de l'information préparent simultanément des descriptions des renseignements sur lesquels ils se sont fondés pour conclure que les communications étaient autorisées par la LCISC.	**D'accord.** La conservation de documents est une composante essentielle de la LCISC, et les registres des communications doivent inclure une description suffisamment complète des informations sur lesquelles l'institution communicante s'est basée pour s'assurer que la

Recommandation	Réponse (14 février 2023)
	communication atteint les critères de la LCISC. Le Guide LCISC 2022 comprend des modèles qui aident les institutions fédérales à respecter leurs obligations en matière de conservation de documents. Cela comprend des sections où les institutions communicantes doivent préparer et conserver des documents qui décrivent les informations sur lesquelles elles se sont basées pour satisfaire l'institution communicante que la communication était autorisée en vertu de la LCISC. Bien que l'alinéa 9(1)(e) de la LCISC n'exige pas explicitement que les institutions préparent simultanément les descriptions des informations liées aux communications de la LCISC, Sécurité publique prend note de la recommandation de l'OSSNR de le faire en temps opportun. Sécurité publique continuera de fournir de la formation et des conseils sur la LCISC aux institutions fédérales afin de souligner leurs obligations en matière de conservation de documents pour s'assurer que toutes les communications sont autorisées en vertu de la LCISC et les aider à comprendre leurs pouvoirs de demander et de communiquer des renseignements en vertu de la Loi.
Recommandation 4 : L'OSSNR recommande d'ajouter des exemples et des scénarios illustratifs dans la formation sur la LCISC, y compris sur les exigences minimales sur la communication, les déclarations relatives à l'exactitude et à la fiabilité et les exigences en matière de conservation de documents.	**D'accord.** Le matériel de formation LCISC a été mis à jour en septembre 2022 avec de multiples exemples illustratifs et des études de cas qui fournissent des détails supplémentaires sur la façon d'appliquer les critères d'autorisation de communication, les déclarations d'exactitude et de fiabilité et les exigences en matière de conservation de documents. Des sessions de formation LCISC ont été dispensées aux institutions fédérales en utilisant le nouveau matériel. Étant donné l'objet de cet examen, Sécurité publique travaillera en étroite collaboration avec AMC pour donner suite à cette recommandation.

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* pour 2021

Conclusions de l'OSSNR

7. L'OSSNR constate que l'Agence des services frontaliers du Canada et Sécurité publique Canada n'ont toujours pas entièrement mis en œuvre un cadre à l'appui de la LCMTIEE et que les politiques et procédures qui l'accompagnent sont toujours en cours d'élaboration.

8. L'OSSNR a constaté qu'entre le 1er janvier 2021 et le 31 décembre 2021, aucun cas visé par la LCMTIEE n'a été transmis aux administrateurs généraux d'un ministère.

9. L'OSSNR constate que la GRC dispose d'un solide cadre pour le triage des dossiers liés à la LCMTIEE.

10. L'OSSNR constate que les évaluations des risques du Comité consultatif sur les risques – Information de l'étranger (CCRIE) de la GRC incluent des objectifs qui ne font pas partie des exigences des décrets, tels que le risque lié au fait de ne pas échanger d'information.

11. L'OSSNR constate que l'utilisation par la GRC d'une évaluation des risques en deux parties, celle du profil du pays et celle de la personne, pour déterminer s'il y a un risque sérieux et tenir compte des circonstances particulières de la personne en question dans l'évaluation des risques, constitue une pratique exemplaire.

12. L'OSSNR constate que la GRC ne dispose pas d'un système centralisé de documentation des garanties et qu'elle n'assure pas régulièrement le contrôle et la mise à jour de l'évaluation de la fiabilité des garanties.

13. L'OSSNR constate que la GRC ne met pas régulièrement à jour ses évaluations des pays et des entités et ne dispose pas d'un calendrier pour le faire. Dans de nombreux cas, ces évaluations datent de plus de quatre ans et se fondent fortement sur le regroupement de rapports de sources ouvertes.

14. L'OSSNR constate que l'information recueillie par l'intermédiaire de l'agent de liaison au cours d'une opération n'est pas documentée de manière centralisée afin de pouvoir être utilisée aux fins d'évaluations futures.

15. L'OSSNR constate que les membres du CCRIE ont conclu que la communication d'information entraînerait un risque sérieux de mauvais traitements qui ne pourrait pas être atténué. Le commissaire adjoint a estimé qu'il était possible de l'atténuer. Il s'agit d'un désaccord entre fonctionnaires ou d'une situation dans laquelle « les fonctionnaires ne sont pas en mesure d'établir s'il est possible d'atténuer le risque ».

16. L'OSSNR constate que les motifs invoqués par le commissaire adjoint pour le rejet des conseils du CCRIE ne tenaient pas suffisamment compte des préoccupations conformément aux dispositions des décrets. L'OSSNR constate notamment que le commissaire adjoint a mal évalué l'importance de la future relation stratégique potentielle avec une entité étrangère lors de l'évaluation du risque potentiel de mauvais traitements à l'égard de la personne.

17. L'OSSNR constate qu'Affaires mondiales Canada s'en remet désormais fortement au personnel opérationnel et aux chefs de mission pour la prise de décisions et la responsabilisation dans le cadre de la LCMTIEE.

18. L'OSSNR constate qu'Affaires mondiales Canada n'a pas démontré que ses secteurs d'activité sont tous intégrés dans son cadre de la LCMTIEE.

19. L'OSSNR constate qu'Affaires mondiales Canada n'a pas rendu la formation sur la LCMTIEE obligatoire pour l'ensemble du personnel des secteurs d'activité concernés. Le personnel pourrait ainsi participer à des échanges d'information sans avoir reçu une formation adéquate et sans connaître les répercussions de la LCMTIEE.

20. L'OSSNR constate qu'Affaires mondiales Canada n'a pas régulièrement mis à jour ses rapports sur les droits de la personne. Si nombre d'entre eux ont été mis à jour au cours de l'année d'examen 2021, plus de la moitié n'ont pas été mis à jour depuis 2019. Cette situation est particulièrement problématique lorsque les ministères et organismes s'appuient sur ces rapports comme source clé pour évaluer les risques liés à la LCMTIEE.

21. L'OSSNR constate qu'Affaires mondiales Canada ne dispose pas d'une approche centralisée et normalisée pour le suivi et la documentation des garanties.

Recommandations de l'OSSNR

Recommandation
Recommandation 1 : L'OSSNR recommande que la GRC mette en place un système centralisé permettant de faire un suivi des mises en garde et des garanties fournies par les entités étrangères et, dans la mesure du possible, de vérifier et indiquer si lesdites mises en garde et garanties ont été respectées.
Recommandation 2 : L'OSSNR recommande que dans les cas où le commissaire adjoint de la GRC est en désaccord avec une recommandation du CCRIE selon laquelle une information ne devrait pas être échangée, le dossier soit automatiquement renvoyé au commissaire.
Recommandation 3 : L'OSSNR recommande que l'évaluation du risque sérieux ne porte que sur les termes énoncés dans un décret en conseil – à savoir sur le risque sérieux de mauvais traitements et sur la possibilité d'atténuer ledit risque – et que les objectifs externes, notamment, la promotion des relations stratégiques n'aient aucune incidence sur les décisions à rendre.

Recommandation
Recommandation 4 : L'OSSNR estime que les recommandations du CCRIE devraient être renvoyées à un commissaire adjoint qui n'est pas le responsable de la sous-direction dont le cas est issu.
Recommandation 5 : L'OSSNR recommande qu'AMC veille à ce que la responsabilité en matière de conformité à la Loi visant à éviter la complicité incombe clairement au Comité de conformité pour éviter les mauvais traitements.
Recommandation 6 : L'OSSNR recommande qu'AMC réalise en interne un exercice formel de schématisation des processus d'autres secteurs d'activités potentiellement concernés, de sorte à s'assurer que les obligations qui lui incombent en vertu de la Loi visant à éviter la complicité soient respectées.
Recommandation 7 : L'OSSNR recommande qu'AMC rende obligatoire la formation sur la Loi visant à éviter la complicité, et ce, pour tout le personnel permutant.
Recommandation 8 : L'OSSNR recommande qu'AMC veille à ce que les rapports sur les droits de la personne soient régulièrement mis à jour pour chaque pays, ce qui permettra auxdits rapports de rendre fidèlement compte de l'évolution des enjeux en matière de droits de la personne.
Recommandation 9 : L'OSSNR recommande qu'AMC mette en place un système centralisé permettant de faire un suivi des mises en garde et des garanties fournies par les entités étrangères et de documenter toute occurrence de non-conformité, et ce, dans le but d'appuyer les évaluations de risques devant être réalisées ultérieurement.

Examen découlant de la décision 2020 CF 616 de la Cour fédérale, rebâtir la confiance : réformer le processus du SCRS relatif aux mandats et le processus du ministère de la Justice relatif à la prestation de conseils juridiques

Cet examen a été approuvé en 2022. En vertu de l'article 38(1) de la Loi sur l'OSSNR, l'OSSNR doit donc rendre compte de ses conclusions et recommandations dans son rapport annuel pour l'année civile 2022. Un résumé de cet examen est disponible dans le rapport annuel 2021 de l'OSSNR.

Conclusions de l'OSSNR

22. L'OSSNR constate que le processus de demande et de prestation de conseils juridiques et les limites en matière de ressources du Groupe litiges et conseils en sécurité nationale (GLCSN) du ministère de la Justice, contribuent à des retards importants, [*description de la durée*].

23. 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.

24. 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.

25. 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 GLCSN a fourni des conseils juridiques au SCRS ne répond pas toujours aux besoins des opérations du SCRS.

26. 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.

27. 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.

28. 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.

29. 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.

30. 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.

31. 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.

32. 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.

33. L'OSSNR est d'avis que les intervenants prenant part au processus relatif aux mandats sont susceptibles d'interpréter/de percevoir différemment les motifs justifiant 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.

34. 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.

35. 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.

36. 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.

37. L'OSSNR constate que le SCRS a éprouvé des difficultés lorsqu'il s'est agi de veiller à ce que toute 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. 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.

38. 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.

39. 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.

40. 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 recueillir grâce au mandat.

41. L'OSSNR est d'avis que le rôle « d'avocat indépendant » n'est pas en mesure d'exercer une fonction de contrôle suffisamment rigoureuse.

42. 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.

43. 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.

44. 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 ».

45. 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.

46. 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 : L'OSSNR recommande 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 : • 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	**D'accord.** Avant même le dépôt du rapport de l'OSSNR, le ministère de la Justice travaillait à 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, aux échanges d'information 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. Le ministère de la Justice s'est engagé à améliorer la prestation de services juridiques et à garantir des services juridiques pratiques fournis en temps opportun. 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 et régulière, et de soutenir les avocats au moyen d'une formation interactive visant à mieux comprendre et appuyer

Recommandation	Réponse ministérielle (29 mars 2022)
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.	leur travail en amont. Selon un modèle intégré de collaboration entre le ministère de la Justice 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 en temps opportun, à mesure que l'opération progresse. Le ministère de la Justice a déjà modifié son modèle en ce qui concerne les avocats 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 ciblés en temps opportun, 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. Le ministère de la Justice s'emploie à élaborer une série d'outils pratiques et de mécanismes de prestation de services juridiques pour soutenir le SCRS, notamment les suivants : • 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 : L'OSSNR recommande que le	**D'accord.** Le ministère de la Justice a élaboré des

Recommandation	Réponse ministérielle (29 mars 2022)
GLCSN (de concert avec le SCRS) définisse des indicateurs de rendement clés pour mesurer la prestation des services juridiques au SCRS.	paramètres opérationnels pour mesurer le rendement au chapitre 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 : L'OSSNR recommande 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.** Le ministère de la Justice travaille avec le SCRS pour élaborer et offrir une formation interactive fondée sur des scénarios et est déterminé à poursuivre cette collaboration. Renvoi aux recommandations n° 14 et n° 18.
Recommandation 4 : Afin que le ministère de la Justice puisse fournir des conseils juridiques utiles et adaptés au sens de la recommandation n° 1, l'OSSNR recommande 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 complètement et sincèrement des objectifs, intentions et détails de l'opération.	**D'accord.** Comme il a déjà été mentionné, le ministère de la Justice travaille avec le SCRS pour intervenir plus tôt et de façon plus continue au cours du cycle de vie des opérations afin de fournir en temps opportun des services juridiques ciblés et réguliers.
Recommandation 5 : L'OSSNR recommande 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.** Le ministère de la Justice 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 : L'OSSNR recommande 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 : L'OSSNR recommande que le SCRS mette en place un nouveau processus relatif aux mandats qui élimine les étapes ne contribuant pas indispensablement à l'optimisation des	**D'accord.** Le travail de mise en œuvre est en cours. Le SCRS et le ministère de la Justice sont résolus à simplifier les modèles et les demandes de mandats dans le cadre d'objectifs de

Recommandation	Réponse ministérielle (29 mars 2022)
demandes. Le processus devrait énoncer clairement les règles de responsabilisation qui contribueront à l'optimisation des demandes. Une fois rationalisé, 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.	modernisation plus vastes.
Recommandation 8 : L'OSSNR recommande 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 donner suite 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 : L'OSSNR recommande que le SCRS adopte des politiques et des procédures qui régissent le processus rationalisé 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 du ministère de la Justice 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 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 regroupes 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-	**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	Réponse ministérielle (29 mars 2022)
section des déposants devrait adopter des procédures de vérification des informations ayant été préparées par les régions.	
Recommandation 11 : L'OSSNR recommande 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 donné suite à cette recommandation en classifiant les déposants un échelon au-dessus des agents du renseignement au niveau opérationnel 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 est en cours pour doter des postes de déposants et devrait être terminé d'ici la fin de mars 2022.
Recommandation 12 : L'OSSNR recommande 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 donner suite aux préoccupations qui ont mené à cette constatation et à 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 continue de conseils pendant la durée du cycle de vie du mandat et assure que les obligations en matière de conformité et de franchise sont remplies. Étant donné son importance, le SCRS s'engage à surveiller et à évaluer la Sous-section des déposants de façon continue pour s'assurer que les préoccupations soulevées dans le présent rapport ne se

Recommandation	Réponse ministérielle (29 mars 2022)
	reproduisent pas.
Recommandation 13 : L'OSSNR recommande 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 approuvé 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 : L'OSSNR recommande 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. Le ministère de la Justice appuie le SCRS dans l'élaboration et la prestation d'une formation complète et pratique à l'intention de tous ceux qui travaillent aux demandes de mandats. Renvoi aux recommandations n^{o} 5 et n^{o} 18.
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**. Le ministère de la Justice et le SCRS continueront de collaborer dans les dossiers des ressources et de la dotation.
Recommandation 16 : L'OSSNR recommande que le rôle d'avocat indépendant tel qu'il est tenu par l'avocat du Groupe de la sécurité nationale, 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 Canada serait	**D'accord**. Sécurité publique Canada (SP) créera une fonction de vérification renforcée, qui relèvera de SP et qui tiendra compte des principes et des objectifs établis par l'OSSNR. Sécurité publique Canada élaborera la fonction de vérification améliorée dans le cadre du processus de demande de mandats du SCRS de façon à fournir une fonction de révision rigoureuse qui ne compliquera pas et ne retardera pas

Recommandation	Réponse ministérielle (29 mars 2022)
appuyée par l'équipe de vérification de Sécurité publique Canada 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.	déraisonnablement le processus. Pendant que ce travail est en cours, Sécurité publique Canada prendra des mesures pour renforcer provisoirement la vérification des mandats.
Recommandation 17 : L'OSSNR recommande 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 s'emploie à cerner les besoins en matière de formation.
Recommandation 18 : L'OSSNR recommande 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 : • 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.	**D'accord**. Le SCRS est résolu à améliorer la formation offerte à tous ses employés, comme il est recommandé. Les formations fondées sur des scénarios, 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 augmentera considérablement le nombre de postes à la Division de l'apprentissage et du perfectionnement, 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'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 n° 3 et n° 14.
Recommandation 19 : L'OSSNR recommande que	**D'accord.** Sécurité publique Canada, le SCRS et le

Recommandation	Réponse ministérielle (29 mars 2022)
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.	ministère de la Justice 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 : L'OSSNR recommande 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.

Annexe D : Statistiques concernant les enquêtes sur les plaintes

Du 1er janvier 2022 au 31 décembre 2022

DEMANDES DE TRAITEMENT DE PLAINTE REÇUES	75
Nombre de nouvelles plaintes déposées	**30**
Loi sur l'Office de surveillance des activités en matière de sécurité nationale et de renseignement (Loi sur l'OSSNR), article 16, plaintes visant le Service canadien du renseignement de sécurité (SCRS)	22
Loi sur l'OSSNR, article 17, plaintes visant le Centre de la sécurité des télécommunications (CST)	2
Loi sur l'OSSNR, article 18, habilitations de sécurité	3
Loi sur l'OSSNR, article 19, plaintes renvoyées par la Gendarmerie royale du Canada (GRC)	3
Loi sur l'OSSNR, article 19, *Loi sur la citoyenneté*	0
Loi sur l'OSSNR, article 45, renvois par la Commission canadienne des droits de la personne (CCDP)	0
Décision sur la compétence d'enquêter	**6**

	Acceptée	Rejetée
Loi sur l'OSSNR, article 16, plaintes visant le SCRS	3	16
Loi sur l'OSSNR, article 17, plaintes visant le CST	0	1
Loi sur l'OSSNR, article 18, habilitations de sécurité	1	1
Loi sur l'OSSNR, article 19, plaintes renvoyées par la GRC	2	3
Total	6	24
Enquêtes actives (au moment de la rédaction du présent rapport)	**19**	
Loi sur l'OSSNR, article 16, plaintes visant le SCRS	9	
Loi sur l'OSSNR, article 17, plaintes visant le CST	0	
Loi sur l'OSSNR, article 18, habilitations de sécurité	4	
Loi sur l'OSSNR, article 19, plaintes renvoyées par la GRC	6	
Loi sur l'OSSNR, article 45, renvois par la CCDP	0	

Enquêtes sur des plaintes dont le dossier est clos	**65**			
	Plainte abandonnée	Rapport final	Plainte réglée à l'amiable	Plainte retirée
Loi sur l'OSSNR, article 16, plaintes visant le SCRS	1	0	0	3
Loi sur l'OSSNR, article 17, plaintes visant le CST	0	0	0	0
Loi sur l'OSSNR, article 18, habilitations de sécurité	0	1	0	0
Loi sur l'OSSNR, article 19, plaintes renvoyées par la GRC	0	2	0	0
Loi sur l'OSSNR, article 45, renvois par la CCDP	0	58	0	0
Total	1	61	0	3

Notes de fin

[1] *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

[2] Pour de plus amples renseignements sur le mandat de l'OSSNR, veuillez consulter notre site Web et les rapports annuels précédents.

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

[4] *Loi antiterroriste (2015)*, L.C. 2015, ch. 20.

[5]Les 29 demandes présentées par le SCRS à la Cour fédérale en 2022 (y compris les 28 demandes présentées en vertu de l'article 21 mentionnées dans le tableau 1) ont donné lieu à l'approbation et à la délivrance de 194 autorisations judiciaires, dont 164 mandats et 28 ordonnances d'assistance délivrés en vertu des articles 12, 16 et 21 de la Loi sur le SCRS ainsi que deux autorisations judiciaires délivrées au titre de l'article 11.13 de la Loi. Chaque demande est soumise à un processus de production et d'examen approfondi qui comprend un examen par un conseiller indépendant du ministère de la Justice et une évaluation par un comité composé de cadres du SCRS, de Sécurité publique Canada, du Centre de la sécurité des télécommunications et de la Gendarmerie royale du Canada (le cas échéant) avant que l'approbation ministérielle soit demandée. Un certain nombre de mandats délivrés au cours de la période visée correspondent au développement de nouvelles autorisations et techniques de collecte innovantes, qui ont nécessité une étroite collaboration entre les entités qui font la collecte, les exploitants de technologies, les analystes des politiques et les conseillers juridiques.

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

[7] *Rapport sur les événements concernant Maher Arar*, *Les faits*, vol. I, note 10.

[8] Modifications apportées à la Loi sur la SCRS – Analytique des données, SCRS, 2020 07 18.

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

[10] Cet examen fait actuellement l'objet d'un processus visant à déterminer si l'information peut être communiquée et sera publié à une date ultérieure.

[11] Le CST a cessé depuis le quatrième trimestre de l'exercice 2021-2022 de faire la distinction entre le Dossier relatifs aux incidents liés à la vie privée et le Dossier des erreurs de procédure mineures, puisque les incidents figurant dans les deux dossiers correspondent à la même définition d'un incident lié à la vie privée du CST. Les erreurs de procédure sont désormais saisies dans le Dossier relatif aux incidents liés à la vie privée.

[12] L'OSSNR a demandé au CST de fournir la ventilation des demandes selon le ministère demandeur, mais cette information n'a pas pu être communiquée à des fins de publication en raison de sa classification.

[13] *Loi sur la communication d'information ayant trait à la sécurité du Canada*, L.C. 2015, ch. 20, art. 2, [LCISC] 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, la *Loi sur la communication d'information ayant trait à la sécurité du Canada*, a été en vigueur du 1er août 2015 au 20 juin 2019.

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

[15] Le texte caviardé aux fins de l'article 52(1) de la Loi sur l'OSSNR a été remplacé par un résumé entre crochets, p. ex. [*résumé*].