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

Canada

NSIRA

2021 // Annual Report

ISSN: 2563-5778
Catalogue No. PS106-9E-PDF

July 18, 2022

The Right Honourable Justin Trudeau, P.C., M.P.
Prime Minister of Canada
Office of the Prime Minister and Privy Council
Ottawa, ON
K1A 0A2

Dear Prime Minister,

On behalf of the National Security and Intelligence Review Agency, it is my pleasure to present you with our third annual report. Consistent with subsection 38(1) of *the National Security and Intelligence Review Agency Act*, the report includes information about our activities in 2021, as well as our findings and recommendations.

In accordance with paragraph 52(1)(b) of the *National Security and Intelligence Review Agency Act*, our report was prepared after consultation with relevant deputy heads, in an effort to ensure that it does not contain information the disclosure of which would be injurious to national security, national defence or international relations, or is information that is subject to solicitor-client privilege, the professional secrecy of advocates and notaries, or to litigation privilege.

Yours sincerely,

The Honourable Marie Deschamps, C.C.

Chair // National Security and Intelligence Review Agency

Table of contents

Message from the members

The National Security and Intelligence Review Agency (NSIRA) is pursuing its mission of enhancing accountability for national security and intelligence activities in Canada. In 2021, our agency continued to grow in size and improved its ability to fully take advantage of its broad review and investigations mandate covering the national security and intelligence activities of departments and agencies across the federal government.

It is our pleasure to present to you our third annual report in which we discuss our progress and activities in our second full year of operation. Despite the recurrent challenges posed by the COVID-19 pandemic and delays caused by a cyber incident, we completed a wide array of reviews and investigations, and continued improving our processes across the agency. Indeed, we pursued the reform of our processes and methods for doing reviews and investigations, both of which helped us to improve the consistency and efficiency of our work tremendously. These reforms, in conjunction with our growing experience, have allowed us to implement and deliver on our review plan. All of this was made possible by the development of a much stronger corporate policy framework backed by a corporate group that really cares about service delivery and the health of the agency.

In accordance with our continued commitment to transparency and public engagement, this report will present our intention to use future annual reports to publicly assess and track the implementation of previous recommendations. In the same spirit of holding us and the reviewed organizations accountable, we also formalized standards that will allow us to assess the timeliness of responses. It is our hope that these initiatives, in addition to the stringent verification process to assess our confidence in each review that we are currently developing, will inspire confidence and trust in our recommendations and findings.

We would like to thank the staff of NSIRA's Secretariat for their efforts, patience and resilience throughout this challenging year and we hope you share our enthusiasm for what we can accomplish in the year ahead.

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

Executive summary

1. The National Security and Intelligence Review Agency (NSIRA) marked its second full year in operation in 2021. With the agency's broad jurisdiction under the *National Security and Intelligence Review Agency Act* (NSIRA Act), it reviewed and investigated national security and intelligence matters relating to not only the Canadian Security Intelligence Service (CSIS) and the Communications Security Establishment (CSE), but also several federal departments and agencies, including:

    - the Department of National Defence (DND) and the Canadian Armed Forces (CAF);
    - the Royal Canadian Mounted Police (RCMP);
    - Immigration, Refugees and Citizenship Canada (IRCC);
    - the Canada Border Services Agency (CBSA);
    - Transport Canada; and
    - all departments and agencies engaging in national security and intelligence activities in the context of NSIRA's yearly reviews of the *Security of Canada Information Disclosure Act* and the *Avoiding Complicity in Mistreatment by Foreign Entities Act*.

2. In 2021, NSIRA continued to grow in capacity and sought to enhance its technical and subject-matter expertise.

Review highlights

Canadian Security Intelligence Service

3. Over the course of 2021, NSIRA completed four reviews that strengthened its knowledge of important areas of CSIS activity:

    - a review of the cultural, governance and systemic issues arising in the context of the manner in which CSIS seeks and receives legal services from the Department of Justice and prepares and executes the warrants it needs to collect information;
    - a survey of CSIS's suite of technical capabilities, along with its associated governance structure, and areas of interest or concern to which NSIRA may return in future reviews;
    - the second annual review of CSIS's Threat Reductions Measures (TRMs) that expands on findings from the previous review by examining a larger number of TRMs; and
    - an annual compliance review of CSIS's activities.

Communications Security Establishment

4. In 2021, NSIRA completed two reviews of CSE activities, and directed CSE to conduct one departmental study:

    - a review of CSE's governance framework that guides the conduct of active and defensive cyber operations, including whether CSE appropriately considered its legal obligations and the foreign policy impacts of operations;
    - a review focused on internal information sharing within CSE between the foreign intelligence aspect and the cybersecurity and information assurance aspect of its mandate; and
    - a departmental study on whether CSE disclosures of Canadian-identifying information were conducted in a manner that complies with the *Communications Security Establishment Act,* and were essential to international affairs, defence, security or cybersecurity.

Department of National Defence and the Canadian Armed Forces

5. In 2021, NSIRA completed two reviews of the DND/CAF:

    - a scoping exercise to gain foundational knowledge of the Defence Intelligence Enterprise, where a significant part of intelligence functions of the DND/CAF are located; and
    - a follow-up review on the previous year's examination of the Canadian Forces National Counter-Intelligence Unit, with emphasis on operational collection and privacy practices.

Multi-departmental reviews

6. NSIRA conducted two specifically mandated multi-departmental reviews in 2021:

    - a review of directions issued with respect to the *Avoiding Complicity in Mistreatment by Foreign Entities Act*; and
    - a review of information sharing within the federal government under the *Security of Canada Information Disclosure Act*.

7. NSIRA also completed a multi-departmental review under its general mandate to review any activity carried out by a department that relates to national security or intelligence:

    - to map the collection and use of biometrics across several federal government departments and agencies in security and intelligence activities related to international travel and immigration, that is, the "border continuum."

Complaints Investigations

8. In 2021, NSIRA saw its complaints investigation caseload increase significantly as a result of 58 complaints referred to NSIRA by the Canadian Human Rights Commission pursuant to subsection 45(2) of the *Canadian Human Rights Act*.

9. Further, the COVID-19 pandemic contributed to delays in NSIRA's investigations by reducing parties' responsiveness in providing access to information and evidence.

10. In 2021, NSIRA completed its investigation process reform initiative after consultation with multiple stakeholders. NSIRA investigations under this new model are already showing improved efficiency.

01 //

Introduction

1.1 Who we are

11. Established in July 2019, the National Security and Intelligence Review Agency (NSIRA) is an independent agency that reports to Parliament and conducts investigations and reviews of the federal government's national security and intelligence activities. Prior to NSIRA's creation, several gaps existed in Canada's national security accountability framework. Notably, NSIRA's predecessor review bodies did not have the ability to collaborate or share their classified information but were each limited to conducting reviews for their specified department or agency.

12. By contrast, NSIRA has the authority to review any Government of Canada national security or intelligence activity in an integrated manner. As noted in the 2019 annual report, with NSIRA's expanded role, Canada now has one of the most extensive systems for independent review of national security.[1]

1.2 Mandate

13. NSIRA has a dual mandate to conduct reviews and investigations of Canada's national security and intelligence activities. Annex B contains a financial and administrative overview of NSIRA.

Reviews

14. NSIRA's review mandate is broad, as outlined in subsection 8(1) of the *National Security and Intelligence Review Agency Act* (NSIRA Act).[2] This mandate includes reviewing the activities of both the Canadian Security Intelligence Service (CSIS) and the Communications Security Establishment (CSE), as well as the national security- or intelligence-related activities of any other federal department or agency. This includes, but is not limited to, the national security or intelligence activities of the Royal Canadian Mounted Police (RCMP), the Canada Border Services Agency (CBSA), the Department of National Defence (DND) and Canadian Armed Forces (CAF), Global Affairs Canada (GAC), and the Department of Justice.

Further, NSIRA reviews any national security or intelligence matters that a minister of the Crown refers to NSIRA. Annex C contains summaries of the reviews completed in 2021.

15. NSIRA reviews assess whether Canada's national security and intelligence activities comply with relevant laws and ministerial directions, and whether they are reasonable and necessary. In conducting its reviews, NSIRA can make any findings or recommendations it considers appropriate.

16. Reviews of CSIS and CSE will always remain a core part of NSIRA's work since the entire focus of these organizations is to address national security and intelligence matters. Unlike its predecessor review bodies, however, NSIRA has an all-encompassing review mandate. NSIRA will thus continue to prioritize and examine how other departments engaging in national security and intelligence activities meet their obligations. NSIRA reviews help keep Parliament and Canadians informed about the lawfulness and reasonableness of Canada's national security and intelligence activities.

Investigations

17. In addition to its review mandate, NSIRA is responsible for investigating national security- or intelligence-related complaints. This duty is outlined in paragraph 8(1)(d) of the NSIRA Act, and involves investigating complaints about:

    - the activities of CSIS or CSE;
    - decisions to deny or revoke certain federal government security clearances; and
    - ministerial reports under the *Citizenship Act* that recommend denying certain citizenship applications.

18. This mandate also includes investigating national security-related complaints referred to NSIRA by the Civilian Review and Complaints Commission for the RCMP (the RCMP's own complaints mechanism)[3] and the Canadian Human Rights Commission.

02 //

Reviews

2.1 Canadian Security Intelligence Service reviews

Overview

19. NSIRA has a mandate to review any Canadian Security Intelligence Service (CSIS) activity. The NSIRA Act requires NSIRA to submit a classified annual report to the Minister of Public Safety and Emergency Preparedness on CSIS activities each year, including information related to CSIS's compliance with the law and applicable ministerial directions, and the reasonableness and necessity of the exercise of CSIS's powers.

20. In 2021, NSIRA completed four reviews of CSIS, summarized below. NSIRA also began two more reviews: one of CSIS's Justification Framework and the other of CSIS's Dataset Regime. Several other ongoing NSIRA reviews contain a CSIS component.

Review arising from the Federal Court's decision in *2020 FC 616*, Rebuilding Trust: Reforming the CSIS Warrant and Department of Justice Legal Advisory Processes

21. In a 2020 decision (2020 FC 616), the Federal Court recommended that a "comprehensive external review be initiated to fully identify systemic, governance and cultural shortcomings and failures that resulted in CSIS engaging in operational activity that it has conceded was illegal and the resultant breach of candour." Based on that recommendation, the Minister of Public Safety and Minister of Justice referred the review to NSIRA pursuant to paragraph 8(1)(*c*) of the *NSIRA Act*. Acting on this reference and relying on its own jurisdiction, NSIRA therefore reviewed the manner in which CSIS seeks and receives legal services from the Department of Justice and prepares and executes the warrants it needs to collect information.

22. This review found an intelligence service and its counsel who struggle to organize themselves in a manner that enables them to meet their legal obligations, including to the Federal Court. NSIRA also found a failure at CSIS to fully and sustainably professionalize the warrant application process as a specialized trade requiring training, experience and

investment. This review also demonstrated the need to transform the relationship between CSIS and its legal counsel.

23. This review was led by NSIRA members Marie Deschamps and Craig Forcese. One or both members were directly involved in every aspect of the review including review process management, briefings, interviews and document review. This included dozens of confidential interviews with Department of Justice and CSIS employees whose perspectives were essential for "ground-truthing" the knowledge NSIRA had gained from documents and formal briefings.

24. In organizing these interviews, NSIRA ensured robust representation covering the range of functions in the warrant and legal advice giving processes. The interviews raised issues and concerns that would have otherwise been unavailable to NSIRA. This assisted NSIRA in making recommendations on governance, systemic and cultural issues that contribute to inefficiencies threatening the ability of CSIS and the Department of Justice to fulfil their mandates.

25. NSIRA heard repeated concerns from interviewees that these problems put at risk the ability of the intelligence service to meet the mandate Parliament has assigned to it. Addressing these challenges urgently is in the public interest. Though CSIS and the Department of Justice have made improvements, difficulties are still evident.

26. NSIRA grouped its findings and recommendations into three overarching areas:

    - the Department of Justice's provision of legal advice;
    - CSIS's and the Department of Justice's management of the warrant acquisition process; and
    - investment in people.

The Department of Justice's provision of legal advice

27. CSIS operates in often rapidly evolving and legally challenging environments. Timely, nimble and actionable legal advice is critical. The Department of Justice provides CSIS with legal advice on national security matters via the National Security Litigation and Advisory Group (NSLAG). This review highlighted factors that prevent NSLAG from providing CSIS with the legal advice it needs.

28. The Department of Justice has employed a centralized "one voice" model for delivering its legal services. The one voice model reflects a desire for uniform and consistent legal advice delivered on behalf of the Attorney General of Canada. Although the premise for the one voice approach is sound, NSIRA found that NSLAG struggled to provide timely, responsive

and useful legal advice in the CSIS context. The way the Department of Justice provides advice has often not been responsive to CSIS operations. For example, NSLAG presents its advice as a legal risk assessment using the Department of Justice-wide Legal Risk Management grid. This grid uses a colour-coded risk rating that can be compared to a "traffic light" system: a green risk rating represents a low legal risk to CSIS, a red risk rating represents a high legal risk, and, more ambiguously, a yellow risk rating represents an intermediate legal risk. Yellow light responses are reportedly the most common and the most frustrating for CSIS, especially when unaccompanied by discussions on how to mitigate the risk, the inclusion of which NSIRA heard is not currently common practice.

29. Therefore, some at CSIS perceive the Department of Justice as presenting a roadblock because of its bureaucracy, its perceived operational illiteracy and its unhelpful approach to communicating legal advice.

30. However, the problems with timely, responsive and useful legal advice do not stem from the Department of Justice alone. NSIRA heard that CSIS has not always shared all relevant information with the Department of Justice, prompting a degree of mistrust. The internal process for requesting legal advice at CSIS also contributes to delays and lack of relevance. The advice that sometimes comes back to operational investigators at CSIS filtered through bureaucratic hierarchies may be of limited relevance.

31. NSIRA heard that the laborious advice-seeking and -receiving process has sometimes caused [discussion of detrimental effects on and risks to operations].

32. CSIS and the Department of Justice often operate in a situation of legal doubt because of lack of clarity in the law. Clarifying legal standards often requires judicial case law. However, an unwieldy warrant process, discussed below, makes that prospect more difficult.

33. The Department of Justice is aware of the need for change. Broad, recent initiatives include the Vision Project, which promises client-centric strategic partnerships. New procedures have been implemented at NSLAG to address internal silos between advisory and litigation counsel, and to improve training, improve access to legal advice and facilitate consistent legal opinions. NSLAG also appears to recognize the desire for a different approach to providing legal advice, including moving toward legal advice that promotes collaborative and iterative engagement with CSIS in order to achieve its operational goals, within the bounds of the law. However, as of fall 2021, it did not appear that CSIS and the Department of Justice had systematically put this model into effect.

34. To facilitate proper advice-giving, CSIS needs to provide NSLAG with all the facts, and to engage NSLAG early on, at the operational level. Earlier and ongoing involvement throughout the stages of an investigation or operation would enable counsel to provide

informal legal nudges that allow CSIS to course-correct before too much time has been spent. A more iterative process of incorporating legal advice over the full course of an operation could address the reported challenge of operations halted due to untimely or ambiguous legal advice.

Management of the warrant process

35. CSIS organizes the process of seeking a warrant around a system of internal preparation and approvals before proceeding to the statutory step of seeking ministerial approval of the warrant application. A number of legal concepts and expectations enter into the warrant process, including the "duty of candour" owed to the Court.

36. The Federal Court duty of candour concerns fit into two categories: disclosure of information material to the credibility of the sources who supply information used in the application; and disclosure of information material to matters of potential concern about the broader context of the warrant and how it will be executed.

37. Despite past attempts at reforms, the current warrant process adopted by CSIS and supported by the Department of Justice has repeatedly failed to meet these candour obligations. Many reforms appear to have contributed to the bureaucratic complexity of the warrant process, without addressing candour issues.

38. CSIS has especially struggled to ensure that all information material to the credibility of sources is properly included in warrant applications. NSIRA heard repeatedly that CSIS officers involved in the early stages of preparing warrant applications do not clearly understand the legal expectations surrounding the duty of candour. Deficient information management systems related to human sources at CSIS have also resulted in important omissions, violating duty of candour obligations. These challenges produce what NSIRA calls the "recurring omissions" problem.

39. In 2019, CSIS sought to professionalize affiant work by creating an Affiant Unit. CSIS's establishment of the Affiant Unit is a critical development and, properly resourced and staffed, it would be well positioned to respond to long-standing problems with the duty of candour. However, when created, the Affiant Unit was placed [Name of Branch]. [Name] has a broad mandate that does not align with the Affiant Unit's functions in preparing legally robust warrant applications. This governance anomaly may explain the Affiant Unit's present administrative and human resource challenges. The Affiant Unit's sustainability is in question, and indeed NSIRA heard that the unit could currently be described as being in a state of crisis. CSIS has not supported the unit with resources commensurate with the importance of this unit in fulfilling CSIS's mission.

40. Warrants counsel at NSLAG have several key roles in the warrant application process and are intimately implicated in ensuring adherence to the duty of candour. Fostering a strong, collaborative and productive relationship with CSIS is key. Morale among NSLAG warrants counsel may have suffered in light of the recent Federal Court decision that prompted this review. With recent staffing increases, it appears that NSLAG currently has the requisite complement to manage the number of annual warrant applications expected from CSIS, but recruitment challenges remain an ongoing issue. NSLAG should be staffed to ensure that CSIS's operations are not stalled due to the lack of availability of warrants counsel.

41. The warrant application process is meant to be strengthened through a review of the near-final affidavit by an "independent counsel" (IC) – in practice, a lawyer drawn from the Department of Justice's National Security Group. The role was originally envisioned as performing a rigorous challenge of the warrant application. However, the primary role of the IC appears to be more clerical than substantive, designed to cite check rather than assertively perform a devil's advocate function.

42. NSIRA believes that the presence of a rigorous challenge function performed by a knowledgeable, adequately supported lawyer distant from the warrant application is valuable and necessary. However, NSIRA proposes that the current IC model be abandoned in favour of a challenge function performed at Public Safety Canada, whose precise role is that of oversight of the CSIS warrant application process.

43. Working with the Public Safety Canada unit charged with warrant review, an experienced and specialized warrant counsel could perform a genuine challenge role to the warrant, analogous to the role a defence lawyer would play were warrants subject to an adversarial process. NSIRA believes that a testing review of this sort will help forestall duty of candour shortcomings stemming from a failure to disclose fully information material to matters of potential concern about the broader context of the warrant and how it will be executed.

44. Once a judge issues a warrant, CSIS may execute the warrant. That execution must comply with the scope and terms of the warrant. However, the CSIS regional warrant coordinators have not received sufficient training to enable the contents of warrants to be translated into advice on proper execution.

Investment in people

45. Concern about inadequate training at CSIS was a recurring theme in this review. This concern was noted in internal CSIS documents. CSIS acknowledges that it is currently not a learning organization and does not have a learning culture. There are too few training

opportunities required to sustain a modern professional intelligence service operating in a complex environment.

Conclusions

46. This report concluded with observations on cross-cutting cultural and governance challenges that stem, at least in part, from challenges characterizing the provision of legal advice and the warrant process. NSIRA divides these broad, cross-cutting phenomena into two categories: morale and attitudes; and performing the mission.

47. Low morale at CSIS was a common theme throughout this review. The systemic problems in the warrant application process are likely one cause of this problem: morale is affected when a warrant acquisition system repeatedly prevents CSIS officers from performing their mandated duties and is the source of regular reputational crises stemming from failures to meet the duty of candour.

48. Meanwhile, a failure to correct problems with the warrant process impairs CSIS's and the Department of Justice's abilities to fulfil their mandates. The Department of Justice must go from being perceived as a roadblock to a frank and forthright advisor fully attuned to operational objectives.

49. Within CSIS, the warrant application process was sometimes likened to winning a lottery — not because the Federal Court declines to issue warrants, but because of the resources required to prepare and complete the application. The current, laborious warrant application process is preventing some collection activities from moving forward.

50. In sum, this review was sparked by a compliance failure in a duty of candour matter. It concludes that repeated failures in this area are both caused by, and cause, deep-seated cultural and governance patterns. This vicious cycle has compounded the challenges of reform in the warrant acquisition process.

51. Cherry-picked or paper-based reforms that mask without addressing the overarching systemic, cultural, and governance challenges will suffer the fate of prior reforms: the problems will continue.

52. NSIRA intends to launch a follow-up review within two years that will measure progress at CSIS, the Department of Justice and Public Safety Canada in resolving the systemic problem with the warrant process addressed by this review. Moreover, in other regular reviews implicating warrants, NSIRA will document recurrences of systemic problems. In the meantime, since this review originated with a decision of the Federal Court, it is vital that the Minister and CSIS share it in its full form with the designated judges of that court. NSIRA's full redacted report can be read on its website.[4]

Response to NSIRA's recommendations

53. NSIRA's recommendations, the management response of CSIS, Public Safety Canada and the Department of Justice, and other details about this review are found in Annex D of this report.

Study of CSIS Technical Capabilities

54. Canada's national security threat landscape is constantly evolving and changes in technology present CSIS with a variety of new investigative opportunities. Consequently, CSIS must develop and acquire new technical capabilities, as well as adapt (repurpose) existing tools to support its mandated collection activities.[5] This process presents potential compliance risk, as CSIS's existing governance and legal frameworks may not capture the new deployment or adaptation of these technical capabilities. Furthermore, certain personnel and supporting legal counsel may not fully understand how these tools are used operationally, impacting their ability to advise whether or not CSIS has the legal and policy framework required to support use of the technology. These risks require NSIRA to maintain up-to-date knowledge of CSIS's technical capabilities and related warrant powers.

55. NSIRA's survey of CSIS technical capabilities offers a first step in this endeavour by surveying CSIS's suite of capabilities, along with its associated governance structure, and identifying areas of interest or concern to which NSIRA may return in future reviews.

56. The full range of technical capabilities CSIS currently employs in support of its intelligence collection operations was examined. NSIRA reviewed relevant policy and legal frameworks as communicated by CSIS but did not conduct an independent verification or audit of the claims or activities themselves. NSIRA also examined the tripartite information/knowledge sharing and support nexus that exists between CSIS's operational branches, technological branches and CSIS's Department of Justice counsel with regard to the deployment of capabilities in support of operations.

57. In addition to the foundational knowledge NSIRA gained of CSIS's technical capabilities, NSIRA made several observations identifying areas of interest for possible future reviews. For example, NSIRA noted, and CSIS agreed, that the main policy suite related to the use of technical capabilities is outdated and under revision, though the timeline for completing this task is

Reality of the risks

NSIRA's review of CSIS's use of a geolocation tool found that the lack of "developed policies and procedures around the assessment of new and emerging collection technologies" directly contributed to the risk that CSIS had breached section 8 of the *Canadian Charter of Rights and Freedoms* while testing the tool.

- *NSIRA Study 2018-05*

unclear.[6] In the interim, the policy suite is buttressed as required by directives from senior leadership and other relevant policies and practices. The lack of up-to-date policies and procedures may result in heightened compliance risks, an issue of interest to future NSIRA reviews.

58. In addition, CSIS is currently reworking the framework it uses to assess compliance and risk in this area. CSIS indicated that greater efficiencies in addressing stakeholder needs and compliance gaps could be achieved through new initiatives such as the creation of the Operational Technology Review Committee, which was created in May 2021. This committee's objective is to review all new technologies used to collect intelligence and existing technologies that will be used in a new or different manner. The creation of the Operational Technology Review Committee suggests a positive step toward mitigating the risk of compliance breaches related to the deployment of technologies in support of operations. Most obviously, it presents a forum in which potential risks can be proactively identified and mitigated. The evolving nature of how compliance is monitored in relation to technical capabilities will be of interest to NSIRA moving forward.

59. Further questions exist regarding how CSIS monitors the operational value of technical capabilities. CSIS needs to strengthen its performance metrics program with regard to its deployment of technologies in support of operations. A performance measurement regime, currently under development, will become an important feature of the governance framework, with attendant compliance implications for possible future NSIRA reviews.

60. Overall, it will be important for NSIRA to remain up to date with respect to the technical aspects of CSIS intelligence collection operations, particularly given the speed with which technology and associated technical capabilities evolve.

61. As part of this effort, it may be possible to leverage existing reporting requirements already undertaken by CSIS. For example, Section 3 of the Ministerial Direction to the Canadian Security Intelligence Service: Accountability (September 10, 2019) requires CSIS to inform the Minister of Public Safety of operational activities in which "a novel authority, technique or technology is used." These notifications could provide NSIRA with ongoing and up-to-date knowledge of CSIS's capability suite and how/when technologies are deployed operationally. Furthermore, sharing the notifications would bolster CSIS's efforts toward proactive transparency, which are in line with commitments to provide explanatory briefings to the Federal Court on new technologies used in warranted operations.

62. NSIRA has recommended that the full, unredacted, version of this technical survey be shared with the designated judges of the Federal Court.

Review of CSIS Threat Reduction Activities: A Focus on Information Disclosure to External Parties

63. Under the *Anti-terrorism Act, 2015,* CSIS was granted the authority to undertake threat reduction measures (TRMs). NSIRA is required to review, annually, at least one aspect of CSIS's performance in the use of its threat reduction powers.[7] NSIRA recognizes that CSIS's threat reduction powers can be an effective tool to diminish a national security threat; however, these powers also command heightened responsibility, given their nature and ability to profoundly impact, not only the subject of a given TRM, but others potentially captured by its scope.

64. This year, NSIRA produced its second annual review of CSIS's TRMs. This review sought to expand on findings from the previous review by examining a larger number of TRMs, wherein CSIS disclosed information to external parties, and in doing so, provided the external party the opportunity to take action, at their discretion and pursuant to their authorities, to reduce identified threats. This review studied the characteristics of these particular TRMs but focused its examination on the extent to which CSIS appropriately identified, documented and considered any plausible adverse impacts that these measures could have on affected individuals.

65. NSIRA observed that several different kinds of external parties were involved in the TRMs. These external parties had varied levers of control through which they could take action to reduce a threat.

66. NSIRA found that CSIS's documentation of the information disclosed to external parties as part of TRMs was inconsistent and, at times, lacked clarity and specificity. NSIRA also found that CSIS did not systematically identify or document the authorities or abilities of external parties to take action, or the plausible adverse impacts of the TRM. NSIRA also found that CSIS did not always document the outcomes of a specific TRM, or the actions taken by external parties to reduce a threat.

67. Without robust documentation, CSIS is neither capable of assessing the efficacy of its measures nor appreciating the full impact of its actions related to these measures.

68. NSIRA recommended that when a TRM involves the disclosure of information to external parties, CSIS should clearly identify and document the scope and breadth of information that will be disclosed as part of the proposed measure. NSIRA recommended that CSIS should also fully identify, document and consider the authority and ability of the external party to take specific action to reduce a threat, as well as the plausible adverse impacts of the measure. Beyond recommending that CSIS comply with its record-keeping policies, NSIRA recommended that CSIS amend its TRM policy to include a requirement to

systematically document the outcomes of TRMs, including actions taken by external parties. This practice should inform post-action assessments and future decision-making.

69. In addition, NSIRA found that the current assessment framework employed as part of the TRM approval process is overly narrow and does not sufficiently consider the full impact of CSIS TRMs. NSIRA recommended that CSIS consider plausible adverse impacts resulting not only from CSIS disclosures of information, but also from the actions of external parties as part of TRMs.

70. The variety of impacts observed in this year's review, combined with the gaps identified in CSIS's understanding and assessment of these impacts, highlights the salience of a number of NSIRA's recommendations made in 2020. NSIRA reiterated its 2020 recommendation that CSIS consider more comprehensively the plausible adverse impacts of these types of measures on the affected individuals, even when they are carried out by the external party and not CSIS. These impacts should be considered not only when assessing the reasonableness and proportionality of a proposed measure, but also when determining whether a warrant is required.

71. The *Canadian Security Intelligence Service Act* (CSIS Act) is clear that when a proposed TRM would limit a right or freedom protected in the *Canadian Charter of Rights and Freedoms*, or would otherwise be contrary to Canadian law, CSIS must seek a judicial warrant. NSIRA fundamentally disagrees with CSIS's understanding of and approach to the legal analysis of determining whether a warrant is required for proposed TRMs. In 2020, CSIS responded to this recommendation by stating, "the Department of Justice will consider this recommendation and factor it into its work related to TRMs under the CSIS Act."

72. Going forward, NSIRA recommended that CSIS seeks a warrant when a proposed TRM could infringe on an individual's Charter rights, or where it would otherwise be contrary to Canadian law, regardless of whether the activity would be conducted by CSIS directly, or via an external party to whom CSIS discloses information.

73. NSIRA was able to use its direct access to CSIS information repositories to confirm information that it needed to verify and pursue necessary additional inquiries. For that reason, NSIRA has a high level of confidence in the information used to complete this review. NSIRA would also like to recognize CSIS's timeliness in responding to NSIRA's requests for information throughout the course of this review.

Response to NSIRA's recommendations

74. NSIRA's recommendations, the management response of CSIS and other details about this review are found in Annex D of this report.

NSIRA's annual review of CSIS activities

75. In accordance with the CSIS Act, CSIS is required to provide information to NSIRA on specific activities.[8] In response, NSIRA has developed a process to examine this information throughout the year and highlight any significant observations as part of NSIRA's annual reporting obligations to the Minister of Public Safety.[9] This process aims to keep NSIRA informed of key CSIS activities so that it can identify emerging issues and compliance gaps in a timely manner, and plan reviews and annual reporting obligations. Furthermore, this process facilitates additional scrutiny of these activities, as necessary, to assess for compliance, reasonableness and necessity.

76. In 2021, NSIRA formalized this process and initiated an annual review pursuant to its review mandate (paragraph 8(1)(a) of the NSIRA Act). To enhance transparency, NSIRA requested additional categories of information from CSIS, including approved warrant applications, compliance reports, internal audits and evaluations, and communications between CSIS and the Federal Court and CSIS and the Minister of Public Safety. These additional categories sought to ensure that NSIRA has the benefit of specific policy and governance information beyond that which CSIS is legislatively required to provide.

77. NSIRA found that CSIS met its legislated reporting requirements; however, these requirements do not always translate into information that can be used for assessments by NSIRA. Notably, CSIS did not provide information on the additional categories of activities requested by NSIRA. Conversations to address these gaps will continue in 2022.

78. In 2022, NSIRA will continue its review of CSIS activities with the support of the information from CSIS as required under the CSIS Act and the NSIRA Act.

Statistics

79. NSIRA requested that CSIS provide for publication statistics and data about public interest and compliance-related aspects of its activities. NSIRA is of the opinion that the following statistics will provide the public with information related to the scope and breadth of CSIS operations, as well as display the evolution of activities from year to year.

Warrant applications

80. Section 21 of the CSIS Act authorizes CSIS to make an application to a judge for a warrant if CSIS believes, on reasonable grounds, that more intrusive powers are required to investigate a particular threat to the security of Canada. Warrants may be used by CSIS, for example, to intercept communications, enter a location, and/or obtain information, records

or documents. Each individual warrant application could include multiple individuals or request the use of multiple intrusive powers.

81. NSIRA is aware that difficulties with the warrant acquisition process within CSIS persist. NSIRA's *Review on Rebuilding Trust: Reforming the CSIS Warrant and Justice Legal Advisory Process* found that the current warrant process continues to be overly burdensome, despite attempts at reform. The review found a failure at CSIS to professionalize the warrant application process fully and sustainably. The lack of clear accountability and clear communication combined with excessive complexity have contributed to the problems facing this process. The review made a number of findings and recommendations related to systemic problems with CSIS's warrant process.

Section 21 warrant applications made by CSIS, 2018 to 2021

	2018	2019	2020	2021
Approved warrants Total	24	23	15	31
New warrant	10	9	2	13
Replacements	11	12	8	14
Supplemental	3	2	5	4
Denied total	0	1	0	0

Threat reduction measures (TRMs)

82. Section 12.1 of the CSIS Act authorizes CSIS to take measures to reduce threats to the security of Canada, within or outside Canada.[10] CSIS is authorized to seek a judicial warrant if it believes that certain intrusive measures (outlined in subsection 21 (1.1) of the CSIS Act) are required to reduce the threat. To date, CSIS has sought no judicial authorizations to undertake warranted TRMs.

83. NSIRA's first two reviews of CSIS's use of threat reduction measures found that CSIS did not sufficiently consider the full impact of the measure as part of the approval process for these activities. More specifically, these impacts were not explicitly considered when determining whether a warrant may be required. As already noted, NSIRA expects that when CSIS is proposing a TRM where an individual's Charter rights would be limited or the TRM would otherwise be contrary to Canadian law, whether CSIS is undertaking the TRM directly or whether it will be executed by an external party, CSIS will seek a warrant to authorize the TRM.

Threat reduction measures approved, executed by CSIS and warranted, 2015 to 2021

	2015	2016	2017	2018	2019	2020	2021
Approved TRMs	10	8	15	23	24	11	23
Executed	10	8	13	17	19	8	17
Warranted TRMs	0	0	0	0	0	0	0

CSIS targets

84. CSIS is mandated to investigate threats to the security of Canada, including espionage; foreign-influenced activities; political, religious or ideologically motivated violence; and subversion.[11] Section 12 of the CSIS Act sets out criteria permitting CSIS to investigate an individual, group or entity for matters related to these threats. Subjects of a CSIS investigation, whether they be individuals or groups, are called "targets."[12]

CSIS targets, 2018 to 2021

	2018	2019	2020	2021
Number of targets	430	467	360	352

Datasets

85. Data analytics is a key investigative tool for CSIS, providing it with the capacity to make connections and identify trends that are not possible through traditional methods of investigations. The *National Security Act, 2017*, which was passed by Parliament in June 2019, gave CSIS a suite of new powers including a legal framework for the collection, retention and use of datasets. The framework authorizes CSIS to collect datasets (sub-divided into Canadian, foreign and publicly available datasets) that have the ability to assist CSIS in the performance of its duties and functions. It also establishes safeguards for the protection of Canadian rights and freedoms, including privacy rights. These protections include enhanced requirements for ministerial accountability. Depending on the type of dataset, CSIS must meet different requirements before it is able to use the dataset.[13]

86. The CSIS Act also requires CSIS to keep NSIRA apprised of certain dataset-related activities. Reports prepared following the handling of datasets are to be provided to NSIRA, under certain conditions and within reasonable timeframes.[14] While CSIS is not required to advise NSIRA of judicial authorizations or ministerial approvals for the collection of Canadian and foreign datasets, CSIS has been proactively keeping NSIRA apprised of these activities.

87. While this new framework has provided opportunities to execute CSIS's mandate to investigate threats, CSIS noted in its 2020 Public Annual Report that the current legislative

framework is not without its challenges. NISRA is currently reviewing CSIS's implementation of its dataset regime. The results of this review will inform Parliament's review of the *National Security Act, 2017*.

Datasets evaluated by CSIS, approved or denied by the Federal Court or Intelligence Commissioner, and retained by CSIS, 2019 to 2021

	2019	2020	2021
Publicly available datasets			
Evaluated	8	11	4
Retained	8	11	2[15]
Canadian datasets			
Evaluated	10	0	2
Retained by CSIS	0	0	0[16]
Denied by the Federal Court	0	0	0
Foreign datasets			
Evaluated	8	0	0
Retained by CSIS	0	1	1[17]
Denied by Minister	0	0	0
Denied by Intelligence Commissioner	0	0	0

Justification Framework

88. The *National Security Act, 2017*, also created a legal justification framework for CSIS's intelligence collection operations. The framework establishes a limited justification for CSIS employees, and persons acting at their direction, to carry out activities that would otherwise constitute offences under Canadian law. CSIS's Justification Framework is modelled on those already in place for Canadian law enforcement.[18] The Justification Framework provides needed clarity to CSIS, and to Canadians, as to what CSIS may lawfully do in the course of its activities. It recognizes that it is in the public interest to ensure that CSIS employees can effectively carry out its intelligence collection duties and functions, including by engaging in otherwise unlawful acts or omissions, in the public interest and in accordance with the rule of law. The types of otherwise unlawful acts and omissions that are authorized by the Justification Framework are determined by the Minister and approved by the Intelligence Commissioner. There remain limitations to what activities can be undertaken, and nothing in the Justification Framework permits the commission of an act or omission that would infringe a right or freedom guaranteed by the Charter.

89. According to subsection 20.1 (2) of the CSIS Act, employees must be designated by the Minister of Public Safety in order to be covered under the Justification Framework while committing or directing an otherwise unlawful act or omission. Designated employees are CSIS employees who require the Justification Framework as a part of their duties and functions. Designated employees are justified in committing an act or omission themselves (commissions by employees) and they may direct another person to commit an act or omission (directions to commit) as a part of their duties and functions. NSIRA is currently reviewing CSIS's implementation of the Justification Framework. The results of this review will inform Parliament's review of the *National Security Act, 2017*.

Authorizations, commissions and directions under the Justification Framework, 2019 to 2021

	2019	2020	2021
Authorizations	83	147	178
Commissions by employees	17	39	51
Directions to commit	32	84	116
Emergency designations	0	0	0

Compliance

90. CSIS's internal operational compliance program leads and manages overall compliance within CSIS. The objective of this unit is to promote a "culture of compliance" within CSIS by investing in information technology (IT) to support the process around warrants, designing an approach for reporting and assessing potential non-compliance incidents, embedding experts in operational branches to provide timely advice and guidance, and producing internal policies and procedures for employees. This program is the centre for processing all instances of potential non-compliance related to operational activities.

91. NSIRA's knowledge of CSIS operational non-compliance and associated violations of the Charter is limited to what is contained in the CSIS Director's Annual Report on Operations to the Minister of Public Safety. NSIRA notes with interest that CSIS reports Charter violations as operational non-compliance. NSIRA will continue to monitor closely instances of non-compliance that relate to Canadian law and the Charter, and to work with CSIS to improve transparency around these activities.

Non-compliance incidents processed by CSIS, 2019 to 2021

	2019	2020	2021
Processed compliance incidents[19]	53	99	85
Administrative		53	64
Operational	40[20]	19	21
Canadian law			1
Canadian Charter of Rights and Freedoms			6
Warrant conditions			6
CSIS governance			8

CSIS review plan

92. In 2022, NSIRA is commencing or conducting five reviews exclusively focused on CSIS, one review focused on CSIS and CSE operational collaboration (See 2022 CSE review plan, below), one focused on threat management by CSIS and the RCMP of ideologically motivated violent extremism, and a number of interagency reviews that contain a CSIS component.

93. In addition to NSIRA's three legally mandated reviews of the *Security of Canada Information Disclosure Act*, the *Avoiding Complicity in Mistreatment by Foreign Entities Act* and CSIS's TRMs, NSIRA has initiated or is planning the following CSIS reviews:

Justification Framework
This review will assess the implementation of CSIS's new Justification Framework for activities that would otherwise be unlawful, authorized under the *National Security Act, 2017*.
Datasets
This review will examine the implementation of CSIS's dataset regime following the coming into force of the *National Security Act, 2017*.
CSIS Cover Program
This review would be the first review of CSIS Cover Operations. It will survey the full range of CSIS cover activities and concentrate on building foundational knowledge to allow NSIRA to select specific activities for detailed review in future years.

Ideologically Motivated Violent Extremism
This is a joint CSIS-RCMP review of their respective and joint threat management of ideologically motivated violent extremism. The core of the review will be the interplay between CSIS and the RCMP in the context of ideologically motivated violent extremism, and an assessment of whether activities complied with the law, applicable ministerial directions, operational policies, and whether activities were necessary and reasonable.

94. Beyond 2022, NSIRA intends to explore reviews of CSIS on topics including, but not limited to:

    - the lifecycle of warranted information;
    - CSIS's section 16 mandate;
    - "Strictly Necessary" retention policies; and
    - CSIS's Internal Compliance Framework.

Access to CSIS Information

95. Throughout 2021, NSIRA faced differing levels of access and responsiveness in relation to CSIS. COVID-19 related restrictions resulted in considerable delays with receiving requested information and briefings and impeded direct access to NSIRA's dedicated office space within CSIS Headquarters.

96. In response to NSIRA's requests for information, CSIS was transparent in its ability to respond and communicate anticipated delays. When access and staffing levels were no longer restricted, CSIS responses to formal and informal requests related to the Study of Technical Capabilities and the TRM review were timely and complete, and briefings were well administered and provided the requested information.

97. As mentioned above, throughout 2021, NSIRA did not have consistent access to its dedicated office space within CSIS Headquarters, which is used by NSIRA review, legal and investigation staff. As a result, NSIRA's direct access to CSIS's information systems was notably limited. NSIRA was provided various temporary accommodations within CSIS headquarters during this time.

98. CSIS was able to continue to provide NSIRA members access to its regional offices across Canada throughout 2021, however. This access supported NSIRA members not based in the National Capital Region, whose work often requires secure facilities where they can safely

and securely access information relevant to reviews and investigations. NSIRA greatly appreciates the willingness and efforts of CSIS and its regional colleagues in this regard.

2.2 Communications Security Establishment reviews

Overview

99. NSIRA has the mandate to review any activity conducted by CSE. NSIRA must also submit a classified annual report to the Minister of National Defence on CSE activities, including information related to CSE's compliance with the law and applicable ministerial directions, and NSIRA's assessment of the reasonableness and necessity of the exercise of CSE's powers.

100. In 2021, NSIRA completed two reviews of CSE, and directed CSE to conduct one departmental study, all of which are summarized below. NSIRA also began five new reviews focused on CSE's activities that are scheduled for completion in 2022 (see 2022 CSE Review Plan, below). Furthermore, CSE is implicated in other NSIRA multi-departmental reviews, such as the legally mandated annual reviews of the *Security of Canada Information Disclosure Act* (SCIDA) and the *Avoiding Complicity in Mistreatment by Foreign Entities Act* (ACA), the results of which are described below (see Multi-departmental Reviews).

101. Although the pandemic and other priorities precluded NSIRA from advancing its previous commitments to redacting, translating and publishing reviews of the former Office of the CSE Commissioner, NSIRA remains committed to releasing this material, resources permitting.

Review of CSE's Governance of Active and Defensive Cyber Operations

102. The *Communications Security Establishment Act* (CSE Act) provides CSE with the authority to conduct active cyber operations (ACOs) and defensive cyber operations (DCOs). As defined by the CSE Act, an ACO is designed to "degrade, disrupt, influence, respond to or interfere with the capabilities, intentions or activities of a foreign individual, state, organization or terrorist group as they relate to international affairs, defence or security." A DCO helps protect Canadian federal government systems, or systems deemed by the Minister of National Defence to be important to Canada against foreign cyber threats. ACOs and DCOs are authorized by ministerial authorizations and, due to the potential impact on Canadian foreign policy, require the Minister of Foreign Affairs to consent to an ACO ministerial authorization or be consulted on a DCO ministerial authorization.

103. In this review, NSIRA assessed the governance framework that guides the conduct of ACOs and DCOs, and whether CSE appropriately considered its legal obligations and the foreign policy impacts of operations. NSIRA analyzed policies and procedures, governance and operational documentation, and correspondence within and between CSE and GAC. The review scope included the earliest available materials pertaining to ACOs and DCOs and ended concurrently with the validity period of the first ACO and DCO ministerial authorizations (2019–2020).

104. NSIRA incorporated GAC into this review, given the role of the Minister of Foreign Affairs in the ACO and DCO governance structure. As a result, NSIRA gained an understanding of the governance and accountability structures in place for these activities by obtaining unique perspectives from the two departments on their respective roles and responsibilities.

105. The novelty of these powers required CSE to develop new mechanisms and processes while also considering new legal authorities and boundaries. NSIRA found that both CSE and GAC made considerable efforts in building the ACO and DCO governance structure. In this context, NSIRA has found that some aspects of the governance of ACOs and DCOs could be improved by making them more transparent and clearer.

106. Specifically, NSIRA found that CSE could improve the level of detail provided to all parties involved in the decision-making and governance of ACOs and DCOs, within documents such as the ministerial authorizations authorizing these activities and the operational plans that are in place to govern their execution. Additionally, NSIRA also identified several gaps that CSE and GAC need to address, and recommended improvements relating to:

    - engaging other departments to ensure an operation's alignment with broader Government of Canada priorities;
    - demarcating an ACO from a pre-emptive DCO;
    - assessing each operation's compliance with international law; and
    - communicating with each other any newly acquired information that is relevant to the risk level of an operation.

107. The gaps observed by NSIRA, if left unaddressed, could carry risks. For instance, the broad and generalized nature of the classes of activities, techniques and targets comprising ACOs and DCOs could capture unintended higher-risk activities and targets. Additionally, given the difference in the required engagement of GAC in ACOs and DCOs, misclassifying what is truly an ACO as a pre-emptive DCO could result in a heightened risk to Canada's international relations through the insufficient engagement of GAC.

108. While this review focused on the governance structures at play in relation to ACOs and DCOs, of even greater importance is how these structures are implemented and followed in practice. NSIRA made several observations about the information contained within the governance documents developed to date and will subsequently assess how they are put into practice as part of NSIRA's forthcoming review focused on the operations themselves.

Response to NSIRA's recommendations

109. NSIRA's recommendations and other details about this review are found in Annex D of this report.

Review of Information Sharing across Aspects of CSE's Mandate

110. This review examined CSE's legal authority for sharing information obtained in the course of one aspect of its mandate for the purposes of fulfilling another aspect of its mandate. Specifically, the review focused on internal information sharing within CSE between the foreign intelligence aspect and the cybersecurity and information assurance (cybersecurity) aspect of CSE's mandate.

111. NSIRA examined whether CSE's internal sharing of information relating to a Canadian or a person in Canada (IRTC) is consistent with the *Privacy Act,* which limits how collected personal information can be used by a federal institution, and the CSE Act*,* which applies to CSE's incidental collection and use of IRTC. NSIRA concluded that from the descriptions of the aspects in sections 16 and 17 of the CSE Act*,* sometimes information acquired under one aspect can be used for the same, or a consistent purpose, as another. This would satisfy *Privacy Act* requirements for sharing information internally. However, this principle cannot simply be assumed to apply as the purposes of the aspects differ within the CSE Act. CSE must conduct case-by-case compliance analysis that considers the purpose of the collection and sharing.

112. NSIRA considers it necessary for the Chief of CSE's application for a ministerial authorization to fully inform the Minister of National Defence of how IRTC might be used and analyzed by CSE, including the sharing of IRTC to another aspect, and for what purpose. With one exception, the Chief's applications for the period of review appropriately informed the Minister that retained IRTC might be used to support a different aspect. Moreover, the foreign intelligence applications appropriately informed the Minister how CSE assessed "essentiality" for IRTC collected under the foreign intelligence aspect.

113. Under CSE policy, an assessment of IRTC's relevance, essentiality or necessity to each aspect is required for sharing information across the aspects. CSE policy offers definitions

and criteria for assessing and applying these thresholds to the information. NSIRA found that CSE's policy framework with regards to the internal sharing of information between the foreign intelligence and cybersecurity aspects of the mandate is compliant with the CSE Act.

Response to NSIRA's recommendations

114. NSIRA's recommendations, CSE's management response and other details about this review are found in Annex D of this report.

CSE Departmental Study on Disclosures of Canadian Identifying Information

115. Following a 2020 review of CSE's disclosures of Canadian identifying information (CII),[21] NSIRA concluded that CSE's implementation of its disclosure regime under the *National Defence Act* may not have been in compliance with the *Privacy Act*. On November 25, 2020, following the release of the review, NSIRA submitted a compliance report to the Minister of National Defence.[22] NSIRA was of the opinion that CSE, as the custodian of incidentally collected CII, has the responsibility to assure itself and to document that both a collection and disclosure authority exist before sharing it with third-party recipients. NSIRA then directed CSE to conduct a departmental study of its disclosure of CII from August 1, 2019, to March 1, 2021.[23]

116. The purpose of the departmental study was to ensure that disclosures of CII conducted by CSE were conducted in a manner that complies with the CSE Act, and that all disclosures of CII were essential to international affairs, defence, security or cybersecurity.[24]

117. CSE provided the completed departmental study to the Minister of National Defence on October 8, 2021, with a copy to NSIRA, on November 1, 2021. NSIRA is satisfied that CSE provided a complete accounting of its disclosure regime for the requested period of review and provided a report that meets the objectives detailed in NSIRA's terms of reference. In doing so, CSE defined its process for assessing and disclosing CII requests to Government of Canada and foreign clients under the CSE Act while also providing an update on relevant changes that have been made to its disclosure regime based on NSIRA's recommendations from the last CII review.

118. The production of the departmental study also provided an opportunity for CSE to review the CII disclosure regime from CSE's own perspective. This process provides NSIRA with a clearer understanding of how CSE manages its program and evaluates its relevant legal authorities. In addition to contributing to NSIRA's current understanding of CSE's disclosure

regime, the study will also assist in identifying avenues of inquiry for the planned follow-up review of CII scheduled for 2023.

Statistics

119. To achieve greater public accountability, NSIRA recommends that CSE publish statistics and data about public interest and compliance-related aspects of its activities. NSIRA is of the opinion that the following statistics will provide the public with information related to the scope and breadth of CSE operations, as well as display the evolution of activities from year to year.

Ministerial authorizations and ministerial orders

120. Ministerial authorizations are issued by the Minister of National Defence and authorize specific activities conducted by CSE pursuant to one of the aspects of the CSE mandate. The following table lists the ministerial authorizations issued between 2019 and 2021.

CSE ministerial authorizations, 2021

Type of ministerial authorization	Enabling section of the CSE Act	Number issued in 2019	Number issued in 2020	Number issued in 2021
Foreign intelligence	26(1)	3	3	3
Cybersecurity — federal and non-federal	27(1) and 27(2)	2	1	2
Defensive cyber operations	29(1)	1	1	1
Active cyber operations	30(1)	1	1	2

Note: This table refers to ministerial authorizations that were issued in the given calendar years and may not necessarily reflect ministerial authorizations that were in effect at a given time. For example, if a ministerial authorization was issued in late 2020 and remained in effect in parts of 2021, it is counted above solely as a 2020 ministerial authorization.

121. Ministerial orders are issued by the Minister of National Defence and designate people or organizations with whom CSE can work and share information. For instance, a ministerial order designating non-federal information infrastructures as being of importance to the Government of Canada is required for CSE to carry out certain aspects of its cybersecurity and defensive cyber operations mandate. A ministerial order is also required to designate recipients of CII. The following table lists the three ministerial orders in effect in 2021.

CSE ministerial orders, 2021

Name of ministerial order	In effect in 2021	Enabling section of the CSE Act
Designating electronic information and information infrastructures of importance to the Government of Canada	1	21(1)
Designating recipients of information relating to a Canadian or person in Canada acquired, used or analyzed under the cybersecurity and information assurance aspects of the CSE mandate	1	44(1) and45
Designating recipients of Canadian identifying information used, analyzed or retained under a foreign intelligence authorization pursuant to section 45 of the CSE Act	1	43 and 45

Foreign intelligence reporting

122. Pursuant to section 16 of the CSE Act, CSE is mandated to acquire information from or through the global information infrastructure,[25] and to use, analyze and disseminate the information for the purpose of providing foreign intelligence in accordance with the Government of Canada's intelligence priorities.

123. According to CSE, it released 3,050 foreign intelligence end-product reports to 1,627 clients across 28 departments or agencies of the Government of Canada in 2021.

Information relating to a Canadian or a person in Canada

124. As discussed in NSIRA's Review of Information Sharing Across Aspects of CSE's Mandate, IRTC includes information about Canadians or persons in Canada that may be incidentally collected by CSE while conducting foreign intelligence or cybersecurity activities under the authority of a ministerial authorization.[26] According to CSE policy, IRTC is any information recognized as having reference to a Canadian or person in Canada, regardless of whether that information could be used to identify that Canadian or person in Canada.

125. CSE was asked to release statistics or data about the regularity with which IRTC or "Canadian-collected information" is included in CSE's end-product reporting. CSE responded that "as this type of information has not previously been disclosed publicly, CSE is carrying out an injury assessment to determine if information can be provided for publication." CSE subsequently advised that "The impact assessment for disclosure of information requested … is a longer-term endeavour that is unlikely to be resolved in time for the 2021

NSIRA public annual report. Please consider [CSE's response] as 'no releasable information' for the purpose of this year's report."

Canadian identifying information

126. CSE is prohibited from directing its activities at Canadians or persons in Canada. However, given the nature of the global information infrastructure and CSE's collection methodologies, such information may be incidentally acquired by CSE. When used in CSE foreign intelligence reporting, incidentally collected information potentially identifying a Canadian or a person in Canada is suppressed in order to protect the privacy of the individual(s) in question. CSE may release unsuppressed CII to designated recipients when the recipients have the legal authority and operational justification to receive it and when it is essential to international affairs, defence or security (including cybersecurity).

127. The following table shows the number of requests CSE received for disclosure of CII in 2021.

Number of requests for disclosure of Canadian identifying information, 2021

Type of request	Number
Government of Canada requests	741
Five Eyes[27] requests	90
Non-Five Eyes requests	0
Total	**831**

128. CSE was also asked to release the number of instances where CII is suppressed in CSE foreign intelligence or cybersecurity reporting. CSE indicated that "as this type of information has not previously been disclosed publicly, CSE is carrying out an injury assessment to determine if information can be provided for publication." CSE subsequently advised that "The impact assessment for disclosure of information requested … is a longer-term endeavour that is unlikely to be resolved in time for the 2021 NSIRA public annual report. Please consider [CSE's response] as 'no releasable information' for the purpose of this year's report."

Privacy incidents and procedural errors

129. A privacy incident occurs when the privacy of a Canadian or a person in Canada is put at risk in a manner that runs counter to, or is not provided for, in CSE's policies. CSE tracks such incidents via its Privacy Incidents File,[28] Second-party Privacy Incidents File[29] and Minor Procedural Errors File.[30]

130. The following table show the number of privacy incidents and procedural errors CSE tracked in 2021.

CSE privacy incidents and procedural errors, 2021

Type of incident	Number
Privacy incidents	96
Second-party privacy incidents	33
Minor procedural errors	18

Cybersecurity and information assurance

131. Pursuant to section 17 of the CSE Act, CSE is mandated to provide advice, guidance and services to help protect electronic information and information infrastructures of federal institutions, as well as non-federal entities which are designated by the Minister as being of importance to the Government of Canada.

132. CSE was asked to release statistics or data characterizing CSE's activities related to the cybersecurity and information assurance aspect of its mandate. CSE responded that:

> Generally, the Canadian Centre for Cyber Security does not comment on specific cyber security incidents, nor do we confirm businesses or critical infrastructure partners that we work with or provide statistics on the number of reported incidents. Statistics on cyber incidents, including cybercrime, are predicated upon victims coming forward, which is not an accurate reflection of the Canadian environment.
>
> CSE and its Canadian Centre for Cyber Security work every day to defend Government of Canada systems from cyber attacks. On any given day, CSE's dynamic defence capabilities block up to seven billion reconnaissance scans on these systems.

Defensive and active cyber operations

133. Pursuant to section 18 of the CSE Act, CSE is mandated to conduct DCOs to help protect electronic information and information infrastructures of federal institutions, as well as non-federal entities that are designated by the Minister of Defence as being of importance to the Government of Canada from hostile cyber attacks.

134. Pursuant to section 19 of the CSE Act, CSE is mandated to conduct ACOs against foreign individuals, states, organizations or terrorist groups as they relate to international affairs, defence or security.

135. CSE was asked to release the number of DCOs and ACOs approved during 2021. CSE responded that it is "not in a position to provide this information for publication by NSIRA, as doing so would be injurious to Canada's international relations, national defence and national security."

Technical and operational assistance

136. As part of the assistance aspect of CSE's mandate, CSE receives Requests for Assistance from Canadian law enforcement and security agencies, as well as from the DND/CAF.

137. The following table shows the number of requests for assistance CSE received and acted on in 2020 and 2021.

CSE requests for assistance received and acted on, 2020 and 2021

Requests for assistance	2020	2021
Number received	24	35
Number acted on	23	32

2022 CSE review plan

138. In addition to NSIRA's two legally mandated reviews of the *Security of Canada Information Disclosure Act* and the *Avoiding Complicity in Mistreatment by Foreign Entities Act*, both of which implicate CSE, NSIRA has initiated or is planning the following five reviews of CSE:

Review of CSE's Internal Security Program (Safeguarding)
This review will examine how CSE safeguards its employees, information and assets. It will explore the ways in which CSE mitigates internal security risks through inquiries and investigations, and in particular, the use of the polygraph as a tool in the security screening process. This review will also assess CSE's compliance with Treasury Board security policies and directives, as well as the adequacy of, adherence to and effectiveness of CSE's internal processes used to address potential or actual security incidents, violations and breaches of security.
Review of Cybersecurity — Network-Based Solutions
This will be NSIRA's first review focused on the cybersecurity and information assurance aspect of CSE's mandate. It will explore the use of a specific tool: Network Based Solutions as outlined within the cybersecurity ministerial authorization.

Review of Active and Defensive Cyber Operations — Part 2 (Operations)
This review is the continuation of NSIRA's examination of CSE's active and defensive cyber operations conducted prior to July 30, 2021. The first review focused on the internal policies and procedures governing CSE's use of active and defensive cyber operations. This review builds on NSIRA's previous work and will focus on the implementation of these governance structures in actual operations.
Review of a Program under the Foreign Intelligence Mandate
This is a review of a classified program under the foreign intelligence aspect of CSE's mandate. This program is authorized by a ministerial authorization, which also sets out its parameters.
Review of CSE-CSIS Operational Collaboration
This review will examine operational collaboration between CSE and CSIS, both under the assistance aspect of CSE's mandate, but also as it relates to joint operational activities coordinated between them under each agency's respective mandates.

139. Beyond 2022, NSIRA intends to review topics including, but not limited to:

- an annual compliance review of CSE;
- CSE's signals intelligence(SIGINT) retention practices;
- a CSE collection program conducted under a ministerial authorization; and
- CSE's Equities Management Framework.

Access to CSE information

140. In its 2020 Public Annual Report, NSIRA noted that it was seeking to formalize CSE's provision of specific categories of information on a regular basis, such as ministerial authorizations, orders and directives, which would be used to ensure compliance of activities and to inform the conclusions NSIRA provides in the annual classified report to the Minister of National Defence. NSIRA will commence this review, called the annual compliance review of CSE, in 2022. NSIRA is pleased to report that CSE has already begun the process of providing the requested information.

141. NSIRA also previously reported that a lack of comprehensive and independently verifiable access to CSE's information repositories posed a significant challenge to NSIRA's ability to review CSE's activities. In 2021, this challenge persisted.

142. In 2021, NSIRA sought to develop direct access to CSE information repositories, further to NSIRA's "trust but verify" review model.[31] With the exception of dedicated office space, which NSIRA continues to utilize at CSE's Headquarters, NSIRA and CSE have been unable to achieve a workable trust-but-verify model for any reviews of CSE to date, despite several proposals for test cases brought forward by NSIRA throughout the year. NSIRA remains committed to developing a greater degree of verifiable access to CSE information so as to ensure the robustness of its findings and recommendations and, in turn, provide greater transparency of CSE activities to Parliament and the Canadian public.

143. In lieu of direct access to CSE information repositories, NSIRA has to rely on CSE External Review staff to collect relevant information held by CSE on its behalf. CSE External Review organizes briefings by subject matter experts, solicits responses to specific questions, and coordinates searches by CSE staff through information repositories for documents and other materials relevant to reviews. NSIRA recognizes the work of CSE External Review staff and thanks them for their contribution to the work of review.

144. However, reliance on CSE to locate, collate and curate information for NSIRA is not a proper long-term alternative to direct access. Currently, and on receipt of a request for information, CSE conducts a lengthy process to locate and collect information, followed by an internal review of this information to determine relevance prior to releasing materials to NSIRA. CSE's predetermination of relevance of information undercuts NSIRA's authority to decide whether information relates to its reviews and contributes to significant delays in the provision of information to NSIRA. Furthermore, this process creates a burden on CSE staff to coordinate responses to NSIRA's information requirements. This workload could be substantially reduced by allowing NSIRA to conduct its own searches in CSE's information repositories. Concurrently, it would serve as an element of verification that could strengthen NSIRA's confidence in the completeness of information reviewed.

145. Beyond the issues related to limitations on NSIRA's ability to trust but verify are ongoing concerns related to CSE's responsiveness. As mentioned above, significant delays in the provision of information continued to pose a disruptive challenge to all NSIRA reviews of CSE activities in 2021.[32] Although the COVID-19 pandemic interrupted life everywhere, it alone could not account for the extent of delays experienced during 2021. The timely provision of information required for a review not only facilitates the work of NSIRA, but is a legal requirement to which NSIRA expects CSE to adhere.

146. The sole exception to NSIRA's right of access to information under the control of CSE is a confidence of the Queen's Privy Council for Canada, otherwise known as a Cabinet confidence. Information subject to the *Privacy Act*, or any other act of Parliament, for that matter, as well as highly classified or Exceptionally Controlled Information (ECI) must be

made available to NSIRA in a timely manner, when it relates to a review. This was not always the case in 2021.

147. In light of the ongoing challenges to NSIRA reviews of CSE activities, NSIRA continues to be of the opinion that the only mechanism to ensure a high degree of confidence, reliability and independence in its work is to have direct access to information relevant to its reviews. One important way by which CSE can continue to increase the level of transparency for its activities is to facilitate greater direct access for external review. For NSIRA to be able to conduct its work with a high degree of confidence, it must be able to verify the accuracy and completeness of the information on which it bases its findings and recommendations. NSIRA will continue to work with CSE to identify ways it can begin to implement additional elements of NSIRA's trust but verify methodology in a more comprehensive and meaningful manner.

2.3 Other government departments

Overview

148. Beyond CSIS and CSE, NSIRA initiated reviews of the following departments and agencies in 2021:

- the Department of National Defence / Canadian Armed Forces (DND/CAF);
- the Royal Canadian Mounted Police (RCMP);
- Immigration, Refugees and Citizenship Canada (IRCC);
- the Canada Border Services Agency (CBSA); and
- Transport Canada.

149. As well, through the annual reviews of the *Security of Canada Information Disclosure Act* and the *Avoiding Complicity in Mistreatment by Foreign Entities Act*, NSIRA has engaged with all departments and agencies that make up the Canadian national security and intelligence community.

150. The following sections outline reviews completed or initiated in 2021, by department or agency, as well as some planned future reviews.

Department of National Defence and the Canadian Armed Forces

Study of the Defence Intelligence Enterprise of the Department of National Defence and the Canadian Armed Forces

151. The purpose of this study was threefold. The primary objective focused on understanding the concept of the Defence Intelligence Enterprise (DIE), the umbrella under which DND/CAF conducts its intelligence activities. The second objective focused on developing an understanding of the compliance and oversight functions within the DIE, as well as the reporting of instances of non-compliance. Finally, the information gathered through the two primary objectives of this review provided NSIRA with prerequisite knowledge to help design future reviews.

152. Although comprising only a small percentage of the work of DND/CAF, the intelligence function is growing both in how DND/CAF perceives its importance, as well as in resource allocation. All of DND/CAF's intelligence activities and structures fall within the DIE and without an understanding of this enterprise, NSIRA's review plan would lack focus and organization. The DIE represents a large and complex structure with widely varied activities and functions. Successive reviews will build on NSIRA's knowledge and experience, as well as developing the required expertise to proactively identify areas of future review. In addition, having a more complete understanding of the DIE will help NSIRA better situate DND/CAF in the broader security and intelligence community, so it can identify more opportunities for horizontal review activities.

153. This study also helped to highlight and identify some of the challenges NSIRA may face in reviewing DND/CAF moving forward. Notably, DND/CAF represents a large and complex structure with widely varied activities and functions. Reporting structures are complex. For example, DND senior management structures report directly to the Deputy Minister, CAF Commands report directly to the Chief of the Defence Staff, and some accountability structures require reporting to both. NSIRA also observed that information collection and storage procedures vary across the organization and that it has over 180 independent electronic repositories. The combination of these elements emphasizes the importance of maintaining strong working relationships with DND/CAF to help navigate access to timely information and assets. NSIRA is working closely with DND/CAF on how to overcome these challenges, including the possibility of providing detailed search strings and follow-up briefings to attest to the reliability, completeness and specificity of the provided documentation.

Review of the Canadian Forces National Counter-Intelligence Unit — Operational Collection and Privacy Practices

154. This review was a follow up to last year's review of the Canadian Forces National Counter-Intelligence Unit (CFNCIU). This year's review focused on how IT searches were used to support counter-intelligence investigations. NSIRA assessed whether IT searches and the collection of information in support of counter-intelligence investigations interfered with individuals' reasonable expectation of privacy in the circumstances.

155. Over the course of the review, NSIRA identified three areas of concern tied to the requests for, and conduct of, counter-intelligence internal IT network searches. These are arranged under the following categories: (1) CFNCIU's search of a subject's email, internet and removable device activity; (2) the CFNCIU checklist used to identify and restrict search parameters, and how applicable stakeholders define search parameters; and (3) the use acquired information to expand supplementary searches.

156. NSIRA believes that DND employees and CAF members have a reasonable expectation of privacy when using work computers for personal use. CFNCIU requires the assistance of police or security agencies to obtain search warrants or technical intercept services, under Level II and Level III investigations. NSIRA found that CFNCIU may be inappropriately relying on DND/CAF policies as lawful authority to interfere with a subject's reasonable expectation of privacy.

157. NSIRA observed that information obtained by CFNCIU via the checklist has the potential to capture intimate and personal information that touches on a subject's biographical core. NSIRA found that the checklist risks capturing information that is protected by section 8 of the Charter. NSIRA also found that DND/CAF is applying a definition of metadata that captures information that could be subject to a reasonable expectation of privacy.

158. NSIRA observed that CFNCIU IT inquiries used broad search parameters, which may include information not relevant to the investigation. These parameters were applied as broad approvals with no specific internal controls or oversight at both the operational and working levels. Collection techniques, due in part to the limitations of IT audit tools and broad search parameters, resulted in a wide net being cast. NSIRA found that the investigative IT system practices observed in the context of CFNCIU's counter-intelligence investigations have insufficient legal oversight to ensure that they are as minimally invasive as possible.

159. As a result of these findings, NSIRA recommended that DND/CAF suspend investigative IT system practices in the context of CFNCIU counter-intelligence investigations until a reasonable legal authority has been established. Once a reasonable legal authority has

been established, DND/CAF should create a new policy framework that is reflective of the noted findings.

Response to NSIRA's recommendations

160. NSIRA's recommendations, DND/CAF's management response and other details about this review are found in Annex D of this report.

Reviews planned or in progress

161. NSIRA has several reviews planned for DND/CAF and will conduct further work on two in 2022. The first one in progress is NSIRA's review of DND/CAF's human intelligence (HUMINT) program. This review will examine the entirety of the human source handling program used by DND/CAF.

162. Second, NSIRA is currently examining the domestic open-source collection activities of DND/CAF. More specifically, this review will take a closer look at legal authorities and the policy framework, program support and training, information and technology management systems, collection activities, intelligence production and dissemination, and oversight and accountability mechanisms.

Access to DND/CAF information

163. DND/CAF is the largest federal government department, both in terms of personnel (127,000 including regular and reserve forces) and number of physical locations occupied (42 in the National Capital Region alone). Given its domestic and international breadth, information collection and storage varies across the organization, with 180+ independent electronic repositories. NSIRA primarily accesses information through DND/CAF's liaison body, the National Security and Intelligence Review and Oversight Coordination Secretariat (NSIROCS).

164. To help ensure that NSIRA receives timely and complete access to requested information, DND/CAF has formalized processes for responding to requests for information that includes a Level 1 (assistant deputy minister or equivalent) approval and attestation. Therefore, when NSIROCS receives a request for information, it coordinates with internal stakeholders to provide the requested information and submit it for Level 1 approval, after which the assistant deputy minister (or equivalent) provides a managerial attestation verifying the completeness and accuracy of the information provided.

165. NSIRA has also established direct access to specific DND/CAF IT systems for an ongoing review, and is working on a "proxy access" model for future reviews. Ultimately, the nature

and scope of the review will dictate the access and verification model to be applied. NSIRA remains committed to working with NSIROCS to ensure that access and verification processes meet review requirements.

Royal Canadian Mounted Police

Reviews in progress or planned

166. NSIRA is currently working on three reviews focused exclusively on the RCMP. One of these reviews assesses the RCMP's use of human sources in national security criminal investigations. Another review examines how the RCMP bypasses encryption when it intercepts private communications in national security criminal investigations. Lastly, NSIRA'S review of the Operational Research Unit of the RCMP will be examining the unit's access to and use of security intelligence. The RCMP is also implicated in one multi-departmental review that is discussed below.

Access to RCMP information

167. NSIRA began reviewing the RCMP in 2020 and does not yet have direct access to the RCMP's IT systems. The decentralized nature of the RCMP's information holdings, COVID-19-related restrictions, and limitations resulting from other emergencies have resulted in delays in the RCMP providing NSIRA with requested information. NSIRA is committed to working with the RCMP's National Security External Reviews and Compliance (NSERC) team to establish approaches for the timely provision of information.

168. In lieu of direct access to RCMP IT systems, NSIRA currently relies on the RCMP's NSERC team to collect relevant information. NSIRA thanks the NSERC team for its contribution to the work of review but looks forward to working toward direct access to RCMP IT systems or alternate independent verification processes that provides NSIRA with independent confidence in the reliability and completeness of the information it has access to.

Canada Border Services Agency

169. In 2021, NSIRA completed its review of the Government of Canada's use of biometrics in the border continuum that, while also examining IRCC and Transport Canada, had a strong CBSA component. The summary of this review can be found in the multi-departmental review section below.

170. NSIRA also made considerable progress on two CBSA-focused reviews. The first review is of air passenger targeting and examines the CBSA's use of predictive analysis to identify inbound air travellers for further scrutiny in relation to national security threats. The second review assesses the CBSA's use of confidential human sources, building on prior work in this area by National Security and Intelligence Committee of Parliamentarians.[33]

Financial Transactions and Reports Analysis Centre of Canada

171. NSIRA is currently working on its first review of the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC). NSIRA will examine FINTRAC's existing regime for sharing information with its domestic and international partners by looking at queries and disclosures to foreign financial intelligence units.

2.4 Multi-departmental reviews

Study of the Government of Canada's Use of Biometrics in the Border Continuum

172. Biometrics play a fundamental role in the border continuum, which includes the screening of foreign nationals seeking admission to Canada and the identification of passengers travelling internationally by air.[34] In the course of this review, NSIRA examined activities conducted by the CBSA, IRCC and Transport Canada. The review also extended to the RCMP, which plays a supporting role in one of the major IRCC-led programs using biometrics.

173. Biometrics are sensitive personal information. The identification of persons by virtue of their biological characteristics raises privacy and human rights concerns. There is public apprehension about the government's use of biometric analysis, as reflected in discussions regarding the use of facial recognition technology and, relatedly, its possible disparate impact on marginalized groups. At the same time, identifying individuals entering the country — and consequently determining whether they have a right to enter, or what risks they might pose — serves a national security function. In this way, the use of biometrics requires an assessment of the balance between security and privacy.

174. The immediate objective of this review was to map the nature and scope of biometric activities occurring in this space. This included examining the collection, retention, use and disclosure of biometric information, as well as the legal authorities under which these activities occur. This review also considered the reasonableness and necessity of these activities, studying the accuracy and reliability of biometrics.

175. This review identified a set of observations linked to nine overarching themes:

- *Biometrics and national security.* The centrality of national security as a justification for biometric activities has waned over time relative to other objectives, such as identity management and traveller facilitation. This makes it challenging to assess biometric activities in general as national security activities. Future NSIRA reviews may focus more narrowly on biometric activities that directly engage national security.
- *The steady-state activities.*[35] The steady-state biometric activities in the border continuum are generally well-supported by current legal authorities and are consistent with international practice.
- *Expanding use of biometrics over time.* The use of biometrics in the border continuum has significantly expanded over the last three decades and is likely to continue expanding in the future. New biometric activities must be justified according to the necessity and proportionality of collecting and using biometrics for particular, intended objectives.
- *Pilot projects.* Pilot projects and initiatives raise more concerns than do steady-state activities, as they risk being implemented without sufficient legal analysis or policy development. Despite the temporary or experimental nature of a project, NSIRA expects that departments will conduct the analysis necessary to ensure that legal authority is in place for the conduct of the activity, and that the attendant collection, use, retention and disclosure of personal information is well-governed by policy.
- *Evolving legal and societal norms.* The public debate surrounding legal authorities questions whether existing standards and protections are sufficient for regulating biometric activities or whether new standards and protections are required. The border is, comparatively, a space in which greater intrusiveness is considered reasonable — but the boundaries of those justifications are not limitless, and will require careful calibration moving forward.
- *The dual use of biometrics.* NSIRA observed several instances of possible dual use of biometric information in the activities examined in this report. Even where new uses of biometrics offer demonstrable benefits, new uses must be carefully considered to ensure their reasonableness and proportionality. In addition, all new uses must be justified and well-authorized in law. The principle of "purpose limitation" may be a way of guarding against dual use in the context of biometric activities.[36]
- *Technical systems.* There is significant overlap between the technical systems and databases used across the steady-state biometric activities. The overall architecture of the systems is complex, though not necessarily problematic.

- *Visibility into algorithms.* Departments and agencies have limited ability to see how the algorithms they use for biometric analysis operate. Each department and agency did, however, demonstrate that performance metrics are known and tested, and that custom thresholds are used when appropriate.
- *Preventing bias and discrimination.* IRCC and the CBSA have conducted preliminary analyses to explore how their biometric activities may impact diverse groups of people, though the implementation of possible mitigation strategies was not always apparent. In some contexts, technological advancements have helped to reduce, but not eliminate, differential impacts. More work remains in terms of mitigating differential impacts on segments of the population. At the same time, the departments and agencies under review have demonstrated their awareness of possible systemic inequalities and their commitment to addressing them.

176. Public debate about the government's application of biometric technology will continue to evolve, driving change in the legal and regulatory frameworks associated with such activities. As such, continued scrutiny from NSIRA is warranted, particularly in those instances where the collection and use of biometric information is justified by explicit reference to national security outcomes.

Review of Federal Institutions' Disclosures of Information under the *Security of Canada Information Disclosure Act* in 2020

177. In November 2021, NSIRA and the Office of the Privacy Commissioner of Canada (OPC) completed a joint review of the 215 disclosures made under the *Security of Canada Information Disclosure Act* (SCIDA) in 2020 — NSIRA's first joint review with another review body.

178. SCIDA encourages and facilitates the sharing, or disclosure, of information within the federal government to protect against activities that undermine or threaten national security, subject to certain conditions.[37] SCIDA permits disclosures of information where the disclosing federal institution satisfies itself that the information will contribute to the exercise of the recipient federal institution's jurisdiction or responsibilities in respect of activities that undermine the security of Canada, and will not affect any person's privacy interest more than is reasonably necessary.[38] This is called the disclosure test.

179. The review found that 212 of the 215 disclosures (approximately 99%) appeared to meet both parts of the disclosure test. In the remaining three disclosures, the information appeared speculative, with no clear connection to activities that undermine the security of Canada. All three of the disclosures of concern were proactive disclosures by the RCMP. Of

particular interest was the RCMP's disclosure of the identities and biometric information about approximately 2,900 individuals to the CAF. NSIRA and the OPC recommended that the RCMP update its policies and practices to support compliance with the disclosure test, that the institution that received the disclosure of concern from the RCMP delete or return the information unless they can demonstrate a valid reason not to,[39] and that any institution disclosing personal information about a large number of individuals (bulk disclosure) exercise heightened due diligence.

180. The records reviewed also highlighted one case of a verbal disclosure made to CSIS months prior to a formal SCIDA disclosure and without an apparent source of legal authority. NSIRA and the OPC recommended that institutions with national security expertise ensure that when they request personal information for national security purposes from other federal institutions, they make it clear that their request, in and of itself, does not constitute or confer authority on the other institution to disclose personal information.

181. Based on CSE's and IRCC's information-sharing patterns under SCIDA, NSIRA and the OPC recommended that these two institutions enter into an information-sharing arrangement, and that GAC and CSIS update their information-sharing arrangement to incorporate SCIDA's guiding principles.[40]

182. Finally, the review examined the federal government's SCIDA policies. The review found that Public Safety Canada developed a SCIDA guide for federal institutions, led an interdepartmental working group, and provided training that included all 17 of the federal institutions listed in SCIDA. The review also found that 16 of the 17 federal institutions listed in SCIDA — the exception being the Canadian Food Inspection Agency — have policies to support compliance with SCIDA. NSIRA and the OPC recommended that the Canadian Food Inspection Agency develop a similar framework to implement a SCIDA policy.

Response to NSIRA's recommendations

183. NSIRA's recommendations, the management response of reviewees and other details about this review are found in Annex D of this report.

Review of Departmental Implementation of the *Avoiding Complicity in Mistreatment by Foreign Entities Act* for 2020

184. The *Avoiding Complicity in Mistreatment by Foreign Entities Act* (ACA) and directions issued according to the ACA seek to prevent the mistreatment of any individual as a result of information exchanged between a department of the Government of Canada and a foreign entity. At the heart of the directions is the consideration of substantial risk, and whether that

risk, if present, can be mitigated. To do this, the ACA and the directions lay out a series of requirements that need to be met or implemented when handling information.

185. This review covered the implementation of the directions sent to 12 departments and agencies[41] from January 1, 2020, to the end of the calendar year, December 31, 2020. It was conducted under subsection 8(2.2) of the NSIRA Act, which requires NSIRA to review, each calendar year, the implementation of all directions issued under the ACA.

186. This was the first ACA review to cover a full calendar year. Many of the reviewed departments noted that the COVID-19 pandemic impacted their information-sharing activities, such as the number of cases requiring further review as per the ACA. As such, NSIRA found that from January 1, 2020, to December 31, 2020, no cases under the ACA were issued to deputy heads in any department.

187. While NSIRA was pleased with the considerable efforts made by many departments new to the ACA in building their frameworks, the CBSA and Public Safety Canada had not finalized their policy frameworks in support of the directions received under the ACA within the review period.

188. Mitigation measures used by departments were also reviewed this time, since they are an integral part in the information-sharing process for departments.

189. NSIRA believes that it is now in a position to conduct in-depth case study assessments of individual departments' adherence to the ACA and directions, irrespective of whether a department reported any cases to its deputy head. Finally, future reviews will follow up on the ongoing implementation of NSIRA's past recommendations.

Reviews planned or in progress

190. In the future, NSIRA intends to continue to take advantage of its mandate to "review any activity carried out by a department that relates to national security or intelligence"[42] by pursuing more multi-departmental reviews and avoiding examinations in siloes. In addition to the mandated annual SCIDA and ACA reviews, NSIRA plans to work on two more reviews involving multiple departments. The first one is a review of how CSIS and the RCMP manage threats posed by ideologically motivated violent extremism. The second review will study the relationship between CSE and CSIS on operational activities.

2.5 Technology in review

Integration of technology in review

191. Traditionally associated with the systems and software responsible for the administrative support of an organization, IT plays an increasingly large role in the operational activities of Canada's national security and intelligence community. By taking advantage of rapid advances in cutting-edge technologies, Canada's security and intelligence community is operationalizing advancements in technology to a degree greater than ever before. Modern national security and intelligence agencies must not only use new technologies to enhance their respective mandates, but they also do so to keep abreast of new opportunities, as well as new threats.

192. These advancements happen quickly, are complex and are often unique to each institution. Furthermore, emerging technologies, while ostensibly developed for one purpose, often have unforeseen implications on civil liberties and privacy, especially when used in an intelligence or security capacity. It is essential for an accountability body like NSIRA to keep pace with the use of developing technologies in Canada's national security and intelligence community to ensure that the organizations it is responsible to review are discharging their mandates lawfully, reasonably and appropriately.

193. The vision for NSIRA's Technology Directorate is to enhance the review landscape to incorporate an appropriate focus on the use and implementation of technology by security and intelligence agencies in Canada. By extending its reach into the practical applications of technology, and by entrusting this new focus to an in-house team of engineers, computer scientists and experienced review professionals, NSIRA will be well placed to ensure that the departments and agencies are held accountable for the decisions they make in leveraging the various aspects of emerging technology.

194. The development of this capacity at NSIRA will also provide a unique opportunity to build a review model that will put us on equal footing within the Five Eyes and the international review community. Without dedicated in-house technology expertise, NSIRA's work will not stay current with contemporary national security legal and compliance risks or issues.

195. To that effect, NSIRA's Technology Directorate will:

- lead the review of IT systems and cutting-edge technical advancements;
- conduct independent technical investigations;
- support assigned NSIRA members in the investigation of complaints against CSIS, CSE or the RCMP requiring technological expertise to assess the evidence;

- produce reports explaining and interpreting sophisticated technical subjects;
- assess the risk of a reviewed entity's IT compliance with applicable laws and policy;
- recommend IT system and data safeguards to minimize the risk of legal non-compliance;
- lead the integration of technology themes into yearly NSIRA review plans; and
- leverage external expertise in the understanding and assessment of IT risks.

Future of technology in review

196. In 2022, NSIRA will continue to increase the number of employees working in the Technology Directorate as it takes an increasingly active and significant role. It will also lead the first technology-focused reviews of the lifecycle of CSIS information collected by technical capabilities pursuant to a Federal Court warrant. NSIRA is also scheduled to review CSE's SIGINT retention practices in 2023.

197. In terms of important considerations for ongoing reviews, NSIRA Technology Directorate has identified the following three technology-related topics as priorities for consideration:

    - dual-use technologies;
    - data warehousing, bulk data and data analytics; and
    - automated decision-making.

198. As Canada's security and intelligence community continues to grow its technical collection and analytic capacity, NSIRA must develop its own expertise in technical review in tandem. Over the next year, NSIRA intends to establish domestic and international partnerships and develop working relationships with academics, civil society and commercial leaders to ensure key technological issues factor into its approaches. NSIRA's Technology Directorate will also support the NSIRA complaint investigations team to understand where and when technology advancements could be applied to NSIRA investigations.

2.6 Review policies and processes

Method for assessing timeliness

Guidelines for assessing timeliness in reviews

199. To ensure greater accountability and predictability, NSIRA will be using the following guidelines to assess the timeliness of reviewee responses to requests for information (RFIs) during the review process, and will comment both privately and publicly on the outcomes. Notably, NSIRA's annual report will track timeliness each year. These guidelines provide clear, standardized expectations on this important aspect of the review process.

Standard request for information (RFI) timelines

200. Much of the information requested by NSIRA falls into two categories: "off-the-shelf," readily available material, and material requiring additional work to compile. Off-the-shelf material may include items such as policy documents, ministerial directives, operational policies, legal opinions and standard operating procedures. Information that requires additional work to compile may include things such as material that requires data manipulation or explanations and material in certain specialized databases and emails. RFIs will clearly state which type of material they pertain to, and standard timelines of 15 or 30 days, respectively, will be provided for responses.

Non-standard RFI timelines

201. NSIRA may deem it necessary to provide longer response times for information requests, for example, when the review covers new subject matter, the request is expected to return a large amount of information or documentation, or the reviewee has other ongoing reviews or other operational considerations. Non-standard timelines are at NSIRA's discretion and will be applied based on the judgment of the review team.

202. NSIRA recognizes that extraordinary factors and extenuating circumstances may affect responses to requests for information and documentation. To accommodate this, reviewees may present, with significant justification, an alternative RFI timeline to the one originally provided. This should be done on receipt and review of the request, if possible. The decision to grant an extension is made by the NSIRA review team, and other arrangements, such as providing the requested information in tranches, can be considered. Regardless, RFI's will always have an associated response timeline attached to them. This timeline will determine whether subsequent remedial steps are required.

Remedial steps

203. NSIRA will implement a three-stage approach to engage reviewees when no response is received to an RFI within the associated timeline. When a deadline is missed with no satisfactory response, NSIRA will escalate its concerns progressively by sending a series of letters to the assistant deputy minister, deputy minister and, finally, the responsible minister.

204. The letters will be attached as an annex to the related review and will inform an overall assessment of timeliness of the reviewee in NSIRA's public annual report. The above guidelines will also be reviewed annually and may be updated based on the outcome of their ongoing implementation to ensure they meet their objectives.

Implementation of recommendations

205. The key outcomes of the work flowing from NSIRA's review mandate are typically captured and distilled in the recommendations NSIRA provides based on its findings. In most NSIRA reviews completed since its inception, NSIRA has issued recommendations to the departments and agencies under review. In turn, reviewees have provided responses to these recommendations, which may include a plan for implementation. With a little over two years since recommendations for the first NSIRA reviews were issued, NSIRA believes enough time has elapsed to begin seeing the results of the implementation of these recommendations reflected in reviewees' activities and policies. Therefore, NSIRA will begin considering the most appropriate means to track and evaluate the implementation of the recommendations issued in past reviews.

206. NSIRA will discuss with agencies and departments that were reviewed how to evaluate the implementation of past recommendations. For example, if issues and challenges remain unaddressed, NSIRA may initiate follow-up reviews. NSIRA's public annual report may also raise issues in the implementation of recommendations as needed.

Verification

207. As noted above, verification is a fundamental component of credible and professional independent review. NSIRA must be able to test the completeness or accuracy of information it may receive as a matter of course during every review. This component is key to NSIRA's ability to assure its stakeholders that it has confidence in the information it receives during a review, and thereby in the findings and conclusions of the review.

208. During a review, NSIRA is entitled to receive all information it deems relevant, except for Cabinet confidences. This feature of the NSIRA Act is critical for the success of NSIRA's mandate. For NSIRA to assure Parliament and Canadians that it has a high level of confidence in the information it receives, departments and agencies under review are expected to support processes that satisfy NSIRA's requirement to independently verify the completeness and accuracy of information provided by the department or agency. For example:

    - provide NSIRA, in support of each review, an index of documents provided, and an indication as to whether any information has been altered or removed and why; and
    - include a record of how searches of information are conducted, including which search terms were used, and which databases were queried.

209. Reviewees should always expect an element of verification as a regular part of each review. In keeping with its commitment to transparency and methodological rigour, NSIRA reviews now contain a "confidence statement." This statement reflects NSIRA's ability to verify information during a review. The confidence statement also provides important additional context to the review, apprising readers of the extent to which NSIRA has been able to verify necessary or relevant information during the review, and whether its confidence was impacted as a result of this exercise.

03 //

Complaints investigations

3.1 Overview

210. In the course of the year, NSIRA continued to adapt in conducting its complaints investigations by using innovative approaches. This included the use of videoconference technology for its hearings and investigative interviews, as well as finding procedural efficiencies such as proceeding with some investigations in writing. In part due to challenges inherent to the COVID-19 pandemic, NSIRA experienced delays in its investigations stemming from reduced responsiveness in accessing information and evidence. Annex E contains statistics for NSIRA's complaints investigations in 2021.

211. Advancing the investigations and obtaining evidence presented issues for both NSIRA and the federal government parties to investigations that were obligated to provide information to NSIRA. In several ongoing matters, NSIRA granted adjournments and extensions of deadlines for procedural steps, including the filing of submissions and evidentiary material. In addition to pandemic-related delays, NSIRA notes that federal government parties to investigations cited other reasons for their requests for extensions of deadlines to file material, such as issues related to availability of witnesses and shortage of resources. Furthermore, NSIRA had to ask for additional information in response to incomplete initial disclosures in more than one investigation, which also created delays.

212. As to NSIRA's investigation caseload in 2021, NSIRA dealt with a continued substantial increase in its inventory of cases. This increase resulted from 58 complaints referred in April 2021 to NSIRA for investigation by the Canadian Human Rights Commission, pursuant to subsection 45(2) of the *Canadian Human Rights Act*. This high-volume caseload has impacted NSIRA's overall management of its cases.

213. NSIRA has also been focusing on strengthening its program delivery by working on strategies for the collection, analysis and use of race-based and demographic data in the context of the complaints investigation process. Working closely with its partner, the Civilian Review and Complaints Commission for the RCMP, NSIRA has been developing strategies of common interest in improving procedures to take into account considerations of diversity and inclusion. The specific objective is to improve access to justice by improving awareness

and understanding of the investigation process. The intent is also to document the different racial groups among civilian complainants and determine:

- whether there are significant racial disparities;
- whether there are racial differences with respect to the types of complaints made against national security organization members based on different groups;
- the frequency of complaints that include allegations of racial or other forms of bias; and
- whether complaint investigation outcomes vary by racial group.

214. Looking to the year ahead, NSIRA will analyze procedural data with respect to the timelines of its investigations in order to inform the establishment of new service standards, continuing its efforts to ensure efficiency and transparency in the process. NSIRA is mindful that service standards are based on time commitments in normal circumstances. As the public health situation with respect to the COVID-19 pandemic continues to improve, NSIRA looks forward to the cooperation of federal government parties in increasing their responsiveness to advance investigations. In light of NSIRA's objective of developing service standards, it will be adopting a measured approach to requests for adjournments and extensions of deadlines, which will be permitted in exceptional circumstances. Also for the year ahead, NSIRA will continue to improve its website to promote accessibility to and relevance of processes in the investigation of complaints.

3.2 Status of complaints investigation process reform

215. In 2021, NSIRA completed its investigation process reform initiative after a complex consultation with multiple stakeholders. In July 2021, NSIRA launched its new process that included the implementation of its new rules of procedure, aiming to provide greater accessibility as well as greater efficiency in NSIRA's investigation mandate. Investigations under this new model show early signs of efficiency in that NSIRA has set timelier dates for the conduct of investigative interviews.

3.3 Investigations

Final report summaries

Investigation Concerning Allegations Against the Canadian Security Intelligence Service (1500-516)

Background

216. The Complainant filed a complaint against the Canadian Security Intelligence Service (CSIS) regarding its involvement in different incidents with airport authorities while the Complainant was travelling.

217. In addition, the Complainant alleged harassment, possible interference with employment opportunities, interference with a passport application, intercepting and reviewing mail, and disrupting personal relationships.

Investigation

218. During the investigation, the Complainant raised several separate incidents that led to the filing of their complaint. NSIRA reviewed the evidence before it to determine whether CSIS's actions were reasonable and proportionate in the circumstances; whether CSIS's actions constituted harassment; and whether it had acted lawfully.

219. NSIRA considered the evidence given by witnesses, the documentation submitted by the parties, as well as other relevant material made available during the course of the investigation of the complaint. NSIRA also heard evidence provided by the Complainant.

220. With respect to one specific incident in dealing with airport authorities while travelling, NSIRA heard evidence by witnesses regarding section 8 of the *Canadian Charter of Rights and Freedoms* (Charter). Section 8 of the Charter provides that everyone has the right to be secure against unreasonable search and seizure.

Conclusion

221. With respect to all allegations, NSIRA determined that the complaint is unsupported. However, concerning events related to CSIS participating in a Canada Border Services Agency search of the Complainant's cell phone at an airport on one occasion, NSIRA found that CSIS breached section 8 of the Charter.

222. NSIRA concluded that CSIS did not take the Complainant's privacy interests casually and did not deliberately disregard privacy considerations in relation to the search. The breach of section 8 of the Charter was not egregious and constituted an error in judgment.

Reopened Investigation Concerning Allegations Against the Canadian Security Intelligence Service (1500-471)

Background

223. NSIRA issued a supplemental final report resulting from a reopened investigation that was concluded by its predecessor, the Security Intelligence Review Committee (SIRC).

224. The Complainant alleged that CSIS had violated his constitutional rights due to his race and religion as well as his refusal to work as a human source. He further alleged that CSIS agents were harassing him by stopping him in airports and following him. Lastly, the Complainant alleged that CSIS had disclosed false information to a foreign entity, which resulted in him being held for eight hours without food in a foreign country's airport.

225. In SIRC's final report, SIRC concluded that the Complainant's allegations of discrimination and harassment were unsupported. SIRC also concluded that the actions of CSIS officials had violated section 12 of the CSIS Act, ministerial directions, policies and operational procedures, and that these actions resulted in adverse consequences for the Complainant.

226. NSIRA's reopened investigation was strictly limited to two questions of law: (1) whether the reasonable grounds to suspect standard under section 12 of the CSIS Act must be met when CSIS makes initial inquiries of its operational holdings; and (2) whether CSIS was required to obtain an individual targeting authority against the Complainant.

Investigation

227. The investigation of the reopening was deemed to be continued before NSIRA pursuant to subsection 11(1) of the *National Security Act*. NSIRA considered the documentation submitted by the parties, including classified submissions and documents filed by CSIS. NSIRA also considered the submissions filed by the Complainant as well as any other relevant material made available during the course of the investigation of this reopening.

228. With respect to whether the reasonable grounds to suspect standard under section 12 of the CSIS Act must be met when CSIS makes initial inquiries of its operational holdings, CSIS conceded during the investigation that it requires reasonable grounds to suspect that activities constitute a threat to the security of Canada, as described in section 2 of the CSIS Act, to conduct such initial inquiries of its operational holdings.

229. On the facts of this case, NSIRA determined that SIRC had correctly found that CSIS did not possess objective facts about activities that met the requisite reasonable grounds to suspect standard.

230. With regard to whether CSIS was required to obtain an individual targeting authority against the Complainant, NSIRA concluded that SIRC's findings of fact regarding the extent and manner in which CSIS investigated the Complainant would not be revisited by NSIRA. NSIRA found that SIRC's conclusion that there is a point in the CSIS investigation where CSIS agents were specifically investigating the activities of the Complainant was unequivocal, and, therefore, it was clear that CSIS should have obtained an individual targeting authority against him, yet failed to do so.

Conclusion

231. NSIRA determined that SIRC's report and the findings were affirmed.

04 //

Conclusion

232. In 2021, NSIRA delivered on its mandate by completing reviews on a wide array of federal departments and agencies involved in national security and intelligence activities. Similarly, despite the challenges of the COVID-19 pandemic for complaints investigation proceedings and a large increase in its workload, NSIRA adapted its methods and continued its efforts to improve its program delivery.

233. NSIRA aims to increase its capacity to review technology and its practical use in national security and intelligence activities. The ongoing growth in NSIRA's staff complement will also help the organization review a greater variety of national security and intelligence activities and continue to progress in its investigation of a large number of complaints.

234. NSIRA remains committed to engage with non-government stakeholders. NSIRA took note of feedback on its prior annual report and will continue to aim to improve its usefulness.

235. Once again, NSIRA members are very grateful for the excellent work of the Secretariat staff and their dedication to the organization's mission of promoting greater accountability in the Canadian security and intelligence community and improving the confidence of Canadians in their oversight institutions.

05 //

Annexes

Annex A: Abbreviations

Abbreviation	Full name
ACA	*Avoiding Complicity in Mistreatment by Foreign Entities Act*
ACO	active cyber operation
CAF	Canadian Armed Forces
CBSA	Canada Border Services Agency
CFNCIU	Canadian Forces National Counter-Intelligence Unit
CII	Canadian identifying information
CSE	Communications Security Establishment
CSIS	Canadian Security Intelligence Service
DCO	defensive cyber operation
DIE	Defence Intelligence Enterprise
DND	Department of National Defence
FINTRAC	Financial Transactions and Reports Analysis Centre of Canada
GAC	Global Affairs Canada
HUMINT	Human Intelligence
IRCC	Immigration, Refugees and Citizenship Canada
IRTC	information relating to a Canadian or a person in Canada
NSIRA	National Security and Intelligence Review Agency
NSLAG	National Security Litigation and Advisory Group (of the Department of Justice)
OPC	Office of the Privacy Commissioner of Canada
RCMP	Royal Canadian Mounted Police
SCIDA	*Security of Canada Information Disclosure Act*
SIGINT	Signals Intelligence
TRM	threat reduction measure

Annex B: Administrative and financial overview

Financial overview

1. NSIRA is organized according to three main business lines: Legal Services, Reviews and Internal Services. The following table presents a comparison of spending between 2020 and 2021 for each of the three business lines.

Expenditures by business line, 2020 and 2021

(in dollars)	Expenditures (2020)	Expenditures (2021)
Legal services and complaint investigations	1,859,924	3,051,611
Reviews	3,094,323	4,471,941
Internal services	4,625,860	8,926,178
Total	**9,580,107**	**16,449,730**

2. In the 2021 calendar year, NSIRA spent $16.4 million, a $6.9 million (72%) increase from 2020. This spending increase is mainly attributed to continued growth in personnel, progress in the fit-up of secure facilities to house employees, and investments in infrastructures for information management and information technology (IT), such as classified network access, secure video teleconferencing and equipment to permit NSIRA personnel to work remotely.

Staffing

3. Over the course of the year, NSIRA's personnel grew from 58 to 73, a net employee increase of 15. The impact of the pandemic lockdowns on security screening activities combined with a more competitive labour market and the need, at least partly, for NSIRA employees to work from a secure site, led to staffing delays, an increase in attrition, and an overall lower net intake of employees compared with the previous year.
4. While NSIRA continues to use modern and flexible staffing strategies, procedures and practices, it is also working with employees to implement a post-pandemic flexible hybrid work model as a means to attract and retain talent and compete with other federal employers offering employees the opportunity to work from home.
5. In 2021, NSIRA took the initial step of implementing a custom employee onboarding program including the introduction of training roadmaps. Based on employees' feedback,

NSIRA will be making further investments in 2022 to define core positional competency requirements, and will continue to strengthen, document and develop review methodologies and practices in a bid to support employees' effective integration. These activities are key to attracting and retaining talent in a competitive labour market.

Pandemic

6. Again in 2021 and as discussed throughout this report, the pandemic continued to have an impact on NSIRA operations and activities throughout the year. The NSIRA Secretariat's first priority was the safety of its employees. The Secretariat responded quickly to lockdowns and in communicating COVID-19 working protocols as well as implementing its own vaccination policy following the Government of Canada call for mandatory vaccination for public service employees.

7. In 2021, NSIRA recognized that a modern and flexible approach to work was necessary for the conduct of its mandated activities during the pandemic. NSIRA developed an evergreen COVID-19 guide where employees and managers could turn for up-to-date information on COVID-19 and on flexible work arrangements.

8. NSIRA continued to focus on increased digital communication and virtual contacts with staff through regular newsletters, pandemic updates, virtual get-togethers and promotion of employee assistance programs.

Cyber incident

9. As mentioned in last year's report, NSIRA was affected in March 2021 by a cyber incident involving the network used to house unclassified and protected information (up to Protected B). This network was not used to store classified information (Secret or Top Secret).

10. With the help of its federal partners, such as the Privy Council Office, the Canadian Centre for Cyber Security and Shared Services Canada, NSIRA was able to address the issue and resume normal business operations. However, this incident did exacerbate delays NSIRA was already dealing with because of the pandemic.

11. NSIRA worked with the Office of the Privacy Commissioner of Canada and Treasury Board of Canada Secretariat to address a privacy breach that resulted from the cyber incident. NSIRA informed partners, notified the public through its website and social media, and issued direct notifications in accordance with requirements and recommendations of the Office of

the Privacy Commissioner. Ensuring the privacy of Canadians and the protection of NSIRA's information remain NSIRA's top priorities.

Foundational initiatives

12. Building from having named a Champion and establishing a committee to take action on systemic employment equity, diversity and inclusion issues in 2020, NSIRA continued to work hard to create a culture of inclusion by holding staff discussions on anti-racism and themes related to diversity. In response to the Call to Action from the Clerk of the Privy Council,[43] NSIRA completed a maturity assessment of its policies, programs, and practices related to human rights, accessibility, employment equity, diversity and inclusion, and developed a three-year action plan to guide its efforts.

13. NSIRA is also taking steps to analyze complaints data from previous years to look at demographic trends, including race. In this regard, it is working jointly with another review body to leverage relevant academic expertise to assist NSIRA in collecting the right kind of data in future complaints investigations to assist with this analysis. The aim is to gain insight into communities most impacted by national security activities, which can assist NSIRA in guiding its outreach and engagement priorities.

14. In light of the current and planned growth in personnel and the pandemic physical distancing requirements, it was critical to the success of the organization to increase its access to secure office space to conduct work of a classified nature. In 2021, NSIRA was able to increase its footprint by opening a temporary office site. At the same time, the plans for a permanent NSIRA site were also completed and construction of additional secure office space began in April 2022.

15. NSIRA completed the implementation of a corporate services strategy through the formalization of service agreements with the Privy Council Office and with Public Services and Procurement Canada with respect to IT networking services, security screening activities, finance and compensation services support.

16. In 2021, NSIRA focused on assessing gaps in its security and information management practices. The conduct of a security governance and controls assessment led to the approval and the implementation of the Agency Security Plan recommendations in September 2021.

17. NSIRA also published a policy on information management to ensure that roles, responsibilities and expectations regarding information management were defined, communicated, understood and adhered to throughout the organization. Since information and information management are critical in the conduct of NSIRA's mandate, a new

classification plan was developed, information retention plans established with strategies for destruction, storage, digitization, transport and transfer of information.

18. NSIRA continues promoting transparency by dedicating resources to redact, declassify and release previous reports from the Security Intelligence Review Committee in addition to proactively releasing NSIRA's reviews. During 2021, NSIRA completed a privacy impact assessment of most of its program activities and is in the process of implementing recommendations aimed at ensuring the protection of privacy while communicating in a transparent and open manner.

Annex C: 2021 reviews at a glance

This annex presents a concise list of reviews that NSIRA completed, initiated or conducted during 2021. In the tables below, "start date" refers to the month in which NSIRA sent a notification letter for a given review, while "completion date" refers to the month that the final review report was approved by the NSIRA members.[44]

Reviews completed in 2021

Name of review	Start date	Completion date
Canadian Security Intelligence Service (CSIS) reviews		
Review on Rebuilding Trust: Reforming the CSIS Warrant and Justice Legal Advisory Processes	Jun 2020	Jan 2022
Review of CSIS Threat Reduction Activities: A Focus on Information Disclosure to External Parties	Feb 2021	Dec 2021
Study of CSIS Technical Capabilities	Sep 2020	Oct 2021
Communications Security Establishment (CSE) reviews		
Review of CSE's Governance of Active and Defensive Cyber Operations	Aug 2020	Oct 2021
Review of Information Sharing across Aspects of CSE's Mandate	Jan 2020	Sep 2021
Department of National Defence and the Canadian Armed Forces		
Study of the Defence Intelligence Enterprise of the Department of National Defence and the Canadian Armed Forces	Jun 2021	Oct 2021
Review of the Canadian Forces National Counter-Intelligence Unit — Operational Collection and Privacy Practices	Apr 2021	Dec 2021
Multi-departmental		
Review of the Government of Canada's Use of Biometrics in the Border Continuum	Jul 2020	Oct 2021
Review of Federal Institutions' Disclosures of Information under the *Security of Canada Information Disclosure Act* in 2020	May 2021	Nov 2021
Review of Departmental Implementation of the *Avoiding Complicity in Mistreatment by Foreign Entities Act* for 2020	Jul 2021	Dec 2021

Annex D: Review findings and recommendations

This annex lists NSIRA's full findings and recommendations for the reviews discussed in this annual report, as well as reviewees' management responses to NSIRA's recommendations, to the fullest extent possible at the time of publication.[45] NSIRA intends to publish and track such information from all reviews on its website.

Canadian Security Intelligence Service reviews

Review arising from the Federal Court's decision in *2020 FC 616*, Rebuilding Trust: Reforming the Canadian Security Intelligence Service Warrant and Justice Legal Advisory Processes

NSIRA's findings

1. NSIRA finds that the legal advice-seeking and giving process, and resource constraints at NSLAG contribute to considerable delays, [description of timeline].
2. NSIRA finds that Justice legal opinions have sometimes been prepared without sufficient attention to the audience that needs to understand and act on them. Opinions have been focused on assessing legal risk, often late in the development of a CSIS activity, with limited effort made to propose alternative and legally sustainable means of arriving at the intended objective.
3. NSIRA finds that the Justice Legal Risk Management Framework is misunderstood at the working level at CSIS and further that it does not provide an appropriate framework for the unequivocal communication of unlawful conduct to CSIS.
4. NSIRA finds that difficulties in acquiring prompt and relevant legal advice have contributed [discussion of detrimental effects on and risk to operations] that may require legal advice. In consequence, the manner in which Justice has provided legal advice to CSIS does not always meet the needs of CSIS operations.
5. NSIRA finds that Justice does not generate the necessary business analytics to track its service delivery performance to CSIS.
6. NSIRA finds that Justice has acknowledged that internal silos at NSLAG between the advisory and litigation wings have sometimes left warrant counsel unaware of emerging legal issues and that Justice has taken steps to resolve these issues.

7. NSIRA finds that Justice has committed to improve its advice-giving to CSIS, including moving toward "road map" style legal advice that involves working collaboratively and iteratively with CSIS to achieve operational goals within the bounds of the law.

8. NSIRA finds that CSIS has not always shared all relevant information with NSLAG, prompting a degree of mistrust and limiting Justice's ability to provide responsive legal advice.

9. NSIRA finds that CSIS has a history of quick reforms, followed by neglect, high turnover of personnel leading to a loss of institutional knowledge, and resourcing that did not match stated priorities. CSIS does not track or measure the outcome of past reforms adequately and has no performance metrics for assessing success.

10. NSIRA finds that CSIS policies have not kept pace with operational reality, as they are often vague, dated, overlapping and contradictory. The absence of clear policy creates legal doubt or concerns, and gives rise to disparate interpretations of legal and operational standards.

11. NSIRA finds that there is little common understanding regarding the process or basis on which a warrant is prioritized. Frequent shifts in this process of prioritization have added to operational uncertainty. The prioritization process has made it very difficult to bring novel issues to the Court with the goal of addressing legal ambiguities through court decisions.

12. NSIRA finds that the actors involved in the warrant process do not have a common understanding of the rationale for each of the [multiple] of steps in the overarching warrant application scheme and are not always sure what role each approval step plays.

13. NSIRA finds that the proliferation of process in seeking warrants has created a system of diluted accountability widely regarded as slow and unwieldy, with delays caused by multiple levels of approval.

14. NSIRA finds that there is no regular feedback process in which explanations for warrant-related decisions made at one level filter back to other levels. The absence of feedback is especially acute for the regional investigators.

15. NSIRA finds that often, the sole means to address legal uncertainty is to bring legal questions to the Federal Court through warrant applications. In consequence, an unwieldy warrant process makes resolution of legal doubt more difficult.

16. NSIRA finds that CSIS has struggled to ensure that all information material to the credibility of sources is properly contained in warrant applications. This "recurring omissions" problem stems from a misunderstanding of the Federal Court's role in assessing the credibility of sources and from the presence of multiple, siloed information management systems. NSIRA acknowledges that CSIS has undertaken reforms, but work remains to implement successfully long-term sustainable solutions.

17. NSIRA finds that the Affiant Unit (AU) constitutes a vital and laudable reform within CSIS. However, the AU is currently at risk of collapse. CSIS has not supported the unit with resources commensurate with the importance of this unit in fulfilling CSIS's mission. The benefits of the AU are currently in jeopardy because of governance, human resource, and training deficiencies.

18. NSIRA finds that the AU's placement in the [Name] branch is not commensurate with its functions and importance. This governance anomaly most likely contributes to administrative hurdles and resource challenges faced by the AU.

19. NSIRA finds that without a functional AU able to produce timely and accurate warrant applications, CSIS puts at risk access to warrants and the information collected under them.

20. NSIRA finds that the "Independent Counsel" (IC) role as performed by NSG counsel falls short of creating a rigorous challenge function.

21. NSIRA finds that the CSIS regional warrants coordinators have not received sufficient training enabling them to translate the contents of the warrants into advice on proper warrant execution.

22. NSIRA finds that CSIS lacks long-term training programs for Intelligence Officers.

23. NSIRA finds that CSIS has failed to provide systematic training programs for "non-Intelligence Officers".

24. NSIRA finds that the CSIS's Learning and Development Branch has not been sufficiently resourced to develop and administer comprehensive training programs, especially in specialized areas not covered by the training offered for Intelligence Officers early in their career.

25. NSIRA finds that CSIS and Justice are at risk of not being able to fulfill their respective mandates. No one reform is likely to succeed unless each is pursued as part of a coherent package. No package will succeed unless backed by prioritization at senior levels, and the stable provision of resources, including people with the means and institutional knowledge to see reforms through, and no reform initiative will succeed unless accompanied by clear performance indicators, measured and analyzed regularly to track progress.

NSIRA's recommendations and departmental responses

Recommendation	Departmental response (March 29, 2022)
Recommendation 1: NSIRA recommends that Justice pursue its commitment to reforming the	**Agree.** Prior to NSIRA issuing its report, Justice Canada has been working on a number of

Recommendation	Departmental response (March 29, 2022)
manner of providing legal advice to CSIS, and its stated commitment to "road map"-style advice as a best practice. In support of this objective and the provision of timely, operationally relevant advice, NSIRA further recommends that Justice implement the following: • Whether through an expanded "office hours" and liaison counsel program or otherwise, NSLAG must develop a legal support service operating full time, staffed by experienced lawyers empowered to provide operational advice in real time on which CSIS officers can rely, on the basis of settled Justice positions on recurring legal issues, accessible directly to CSIS officers across all regional offices and at all levels. • NSLAG develop a concise reference tool with its position on recurring issues and most common legal authorities invoked and make the tool accessible to counsel to support their real-time advice. • To minimize the need to resort to the formalized legal advice-seeking process, NSLAG (in coordination with CSIS) must involve counsel with CSIS officers at the early stage of the planning of key or novel operations and throughout their entire operational lifecycle to case-manage an iterative legal guidance process.	measures concerning policies and practices in the provision of legal services to CSIS. These measures include activities related to the duty of candour and the warrant acquisition process, best practices in the delivery of legal services, advising CSIS on legal risks associated with its operations, the sharing of information in the national security context, and tracking and responding to key performance indicators related to the delivery of legal services. Justice is committed to improving the manner of providing legal services and ensuring practical and timely legal services. The measures undertaken to date and further measures underway support a coordinated approach for legal services, striking the right balance of resources across corporate and operational priorities. This includes providing legal advice in a more accessible, iterative manner, and supporting Counsel through interactive training to better understand and support their work in a proactive manner. Justice and CSIS working together in an integrated fashion ensures that counsel are involved throughout an operation's life-cycle, including the early stages. Early integration into operational planning supports the provision of timely and relevant legal advice as operations progress. Justice has already modified its liaison counsel model. Liaison counsel are experienced counsel designated to support CSIS officers across regional offices and particular operations. Enhancements to the role have resulted in liaison counsel providing timely and focused advice, supporting operational imperatives, and identifying trends and issues of concern to develop guidance documents and other practical tools. Justice is developing a suite of practical tools and legal service delivery mechanisms to support CSIS. These include:

Recommendation	Departmental response (March 29, 2022)
	• a user-friendly blog that describes relevant legal issues and concepts in plain-language and with a practical application to CSIS' work; • a field guide for the practical application of legal concerns to CSIS' operations that can be used by officers in the field and in real time; • interpretation and guidance documents; and, • knowledge management tools ensuring counsel can access legal precedents and interpretations.
Recommendation 2: NSIRA recommends that NSLAG (in coordination with CSIS) develop Key Performance Indicators to measure the delivery of legal services to CSIS.	**Agree.** Justice has developed business metrics to measure service delivery performance. Justice will continue to work with CSIS to invest in resources to conduct detailed business analytics to enhance the provision of legal services and make improvements to the existing system. Client feedback surveys are undertaken regularly.
Recommendation 3: NSIRA recommends that CSIS and Justice should include in their training programs interactive scenario-based training developing the operational intelligence activities expertise of NSLAG counsel and the legal knowledge of CSIS operational staff.	**Agree.** Justice has worked with CSIS to develop and deliver interactive scenario-based training and is committed to continuing that involvement. Cross-reference recommendations 14 and 18.
Recommendation 4: To ensure Justice is able to give meaningful and responsive legal advice as recommended in recommendation #1, NSIRA recommends that CSIS invite Justice counsel to sit at the table at all stages of the lifecycle of key and novel operations, and that it fully and frankly brief counsel on operational objectives, intent, and details.	**Agree.** As set out above, Justice is working with CSIS to be involved sooner and more continuously across the lifecycle of operations to provide timely, focused and iterative legal services.
Recommendation 5: NSIRA recommends that Justice's advice-giving must clearly and unequivocally communicate advice on the unlawfulness of client conduct, whether criminal or otherwise.	**Agree.** Justice is currently undertaking a review of its legal risk framework in order to improve both how legal risk is assessed, and also how risks are communicated to clients.

Recommendation	Departmental response (March 29, 2022)
Recommendation 6: NSIRA recommends that CSIS adopt, and share internally, clear criteria for the warrant prioritization process.	**Agree.** CSIS will further refine the warrant prioritization process and work to set clear criteria.
Recommendation 7: NSIRA recommends that CSIS establish a new warrant process eliminating steps that do not make a significant contribution to a more accurate application. The process should assign clear lines of responsibility for the production of accurate applications. The reformed system should ensure that delays associated with managerial approvals are minimized, and that time is reallocated to those steps contributing to the preparation of the accurate applications.	**Agree.** Work on implementation is underway. CSIS and Justice are committed to streamlining warrant applications, templates, and requests as part of broader modernisation objectives.
Recommendation 8: NSIRA recommends that CSIS integrate the regional stakeholders (including the implicated investigators) at every key milestone of the warrants process.	**Agree.** CSIS has already undertaken related improvements to address this recommendation, including through the updated Affiant Unit (AU) business approach to warrant acquisition, which now includes regional stakeholders.
Recommendation 9: NSIRA recommends that CSIS adopt policies and procedures governing the reformed warrant process that clearly outlines the roles and responsibilities of each participant and the objective of each step in the warrant process and that these policies be kept current as the process evolves.	**Agree.** The revised CSIS Justice Joint Policy on Duty of Candour and the associated guidance document outline the role of all CSIS employees (not just the affiants) in ensuring that disclosure obligations to the Court are met. In addition, CSIS has developed a s.21 warrant policy and the drafting of the related procedure is underway. In 2020 and 2021, CSIS provided Duty of Candour training to all operational employees through a special project.
Recommendation 10: To address the seeming inevitability of "recurring omissions", NSIRA recommends that CSIS prioritize the development of [an improved] system for human source information management. CSIS should also continue initiatives meant to ensure that source handlers are assiduous in documenting and then reporting in source precis information going to credibility. Even with these reforms, the Affiant Unit should adopt procedures for verifying the information prepared by the regions.	**Agree.** The recommendation endorses a CSIS initiative already underway. An Action Plan approved by the Executive in January 2021 identified the requirement, and CSIS stakeholders are advancing this initiative. CSIS developed a comprehensive requirements package, and identified a potential technical solution. The complexity of the technical development process means this will be a long process.

Recommendation	Departmental response (March 29, 2022)
Recommendation 11: NSIRA recommends that CSIS recognize the importance of the Affiant Unit by assigning affiants and analysts an employment classification congruent with their responsibilities.	**Agree.** CSIS has addressed this recommendation by classifying affiants at one level above the Intelligence Officer working level to recognize the complexity of their work and to attract/retain candidates. A competitive competition process is underway to staff the affiant positions and is anticipated to be completed by the end of March 2022.
Recommendation 12: NSIRA recommends that CSIS should create an Affiant Branch reporting directly to the CSIS Director.	**Disagree.** The Service notes the concerns raised by the committee in its report regarding the Affiant's Unit current placement in the organization's hierarchy. This said, throughout the course of this review, CSIS has invested heavily in the Affiant Unit and its employees and has made significant changes to the warrant process and its governance. The Service is confident that these changes will be sufficient to address the concerns that resulted in this finding and recommendation, particularly as it relates to observations related to administrative and human resource challenges. In addition, the current placement of the Affiant Unit with other units with corresponding responsibilities for warrant acquisition best facilitates the provision of ongoing guidance and advice throughout the warrant lifecycle to ensure compliance and duty of candour obligations are met. Given its importance, CSIS commits to ongoing monitoring and evaluation of the Affiant Unit to ensure the concerns highlighted in the report do not re-occur.
Recommendation 13: NSIRA recommends that CSIS urgently resource the Affiant Unit to meet its responsibilities and ensure its sustainability. In deciding the size of the AU, CSIS should assess how many warrants an affiant team might reasonably complete every year.	**Agree**. In line with the recommendation, CSIS already increased the resourcing of the Affiant Unit and approved changes to the organizational chart in March 2021. As noted above, a staffing action is currently underway that aims to create a pool of qualified candidates which can be leveraged to help increase the Affiant Unit's capacity.
Recommendation 14: NSIRA recommends that CSIS, in consultation with Justice, develop a	**Agree**. CSIS intends to provide fulsome training to the affiant unit, as recommended. In late 2021,

Recommendation	Departmental response (March 29, 2022)
comprehensive training course for all affiants and analysts, codifying best practices and methods for members of the AU.	initial consultations were held to identify appropriate training. Unfortunately, the pandemic has disrupted training efforts. Justice is supporting CSIS in the development and delivery of all comprehensive and practical training for all those working on warrant applications. Cross-reference recommendations 3 and 18.
Recommendation 15: NSIRA recommends that NSLAG be staffed by a complement of counsel and support personnel sufficient to ensure that CSIS operations are not impeded by resource limitations at NSLAG.	**Agree**. Justice and CSIS will continue to work together on resources and staffing issues.
Recommendation 16: NSIRA recommends that the function of the Independent Counsel as performed by NSG counsel at the Department of Justice should be eliminated, in favour of a new challenge function, analogous to the role a defence lawyer would play were warrants subject to an adversarial process, situated at Public Safety and supported by the Public Safety vetting team, and performed by a knowledgeable lawyer from the Public Prosecution Service of Canada, the private sector, or elsewhere, who is independent from Justice management and not otherwise involved in CSIS warrant applications.	**Agree**. Public Safety will develop an enhanced vetting function, housed in Public Safety Canada, that reflects the principles and objectives set out by NSIRA. Public Safety Canada will develop the enhanced vetting function as part of the CSIS warrant acquisition process such that it provides a meaningful challenge function without adding undue complexity or delay. While this work is underway, Public Safety Canada will take steps to strengthen warrant vetting on an interim basis.
Recommendation 17: NSIRA recommends that CSIS regional warrants coordinator positions receive adequate training, and that CSIS professionalize the position and enable warrant coordinators to more effectively translate the content of warrants into advice on warrant execution.	**Agree**. CSIS acknowledges the importance of training and of centers of expertise. CSIS is determining training requirements.
Recommendation 18: NSIRA recommends that CSIS adequately resource and regularly deliver evergreen scenario-based training programs for all CSIS employees, including;	**Agree**. CSIS is committed to improving the training offered to all of its employees, as recommended. Scenario-based training, which helps employees understand the application of policies and procedures, is now an integral part of operational

Recommendation	Departmental response (March 29, 2022)
• annual, comprehensive, warrant training for all operational employees; • specialized onboarding training for all employees not part of the Intelligence Officer program; and • continued long-term training for all specialized personnel.	training, which includes the development of an annual operational workshop. A recently approved business case will significantly increase staffing in Learning & Development to further enable training of CSIS employees. This business case includes the creation of a new position responsible for developing an enhanced onboarding for all newly hired employees, as well as the creation of new positions to create and deliver additional learning opportunities for all operational employees. Cross-reference recommendations 3 and 14.
Recommendation 19: The recommendations within this review should be treated as a coherent package and that progress and outcomes in implementing these recommendations be tracked, allowing management, the Ministers of Public Safety and of Justice, and NSIRA, to assess the efficacy of reforms and course-correct if necessary.	**Agree.** PS, CSIS, and Justice are committed to taking a holistic approach to the implementation of the recommendations and will track and course correct as required in this complex operating environment.
Recommendation 20: The full classified version of this report be shared with the designated judges of the Federal Court.	**Partially agree.** The Attorney General of Canada has shared the full report, redacted for solicitor-client privilege, with the designated judges of the Federal Court of Canada.

Review of CSIS Threat Reduction Activities: A Focus on Information Disclosure to External Parties

NSIRA's findings

1. NSIRA finds that CSIS's documentation of the information disclosed to external parties as part of TRMs was inconsistent and, at times, lacked clarity and specificity.
2. NSIRA finds that CSIS does not systematically identify or document the external parties' authority and ability to take action, or plausible adverse impacts of the measure.
3. NSIRA finds that CSIS did not systematically document the outcomes of the TRMs and that post-action reports often excluded the actions taken by external parties.

NSIRA's recommendations and CSIS response

Recommendation	CSIS response (June 2022)
Recommendation 1. NSIRA recommends that when a TRM involves CSIS disclosing information to external parties, CSIS should clearly identify and document the scope and breadth of information that will be disclosed as part of the proposed measure.	**Agree.** CSIS agrees with this recommendation. As an organization committed to being fully transparent with Canadians, CSIS benefits from review and leverages recommendations where possible to update its procedures, policies and practices and ensure that any measures it undertakes, including the disclosure of information to external parties, are fully documented in scope and breadth.
Recommendation 2. NSIRA recommends that CSIS fully identify, document and consider the authority and ability of the external party to take action, as well as the plausible adverse impacts of the measure.	Partially agree. CSIS partially agrees with this recommendation. While CSIS fully accepts the recommendation to document the external parties' authority and ability to take action, or the plausible adverse impacts of the measure, this information does not originate from CSIS and, therefore, it may not always be available nor be available at a standard consistent across the implicated external parties.
Recommendation 3. NSIRA recommends that CSIS should amend its TRM policy to include a requirement to systematically document the outcomes of TRMs, including actions taken by external parties. This practice should inform post-action assessments and future decision-making.	Partially agree. CSIS partially agrees with this response. CSIS policy includes reporting requirements such as documentation of TRMs. The actions taken by external parties are included in documentation when available. However, actions undertaken by third parties are voluntary just as discussions and engagement with CSIS are voluntary.
Recommendation 4. NSIRA recommends that CSIS comply with its record-keeping policies related to documenting the outcomes of TRMs.	Agree. CSIS agrees with this recommendation. However, the recommendation is not accurate as it is based on reviews of historic reporting. Indeed, since early 2019 CSIS has been fully documenting the outcomes of TRMs in a manner consistent with its record-keeping policies.

Recommendation	CSIS response (June 2022)
Recommendation 5. NSIRA recommends that CSIS appropriately consider the impacts resulting from external party actions when determining whether a warrant is required.	Disagree. CSIS disagrees with NSIRA's position on leveraging third parties in support of TRMs. CSIS works closely with the Department of Justice to assess whether a warrant is required for each of its TRM initiatives in accordance with the legislative regime and, when applied to TRM initiatives involving third parties.

Communications Security Establishment reviews

Review of CSE's Governance of Active and Defensive Cyber Operations

NSIRA's findings

1. The Active and Defensive Cyber Operations Ministerial Authorization Applications do not provide sufficient detail for the Minister(s) to appreciate the scope of the classes of activities being requested in the authorization. Similarly, the Ministerial Authorization does not sufficiently delineate precise classes of activities, associated techniques, and intended target sets to be employed in the conduct of operations.
2. The assessment of the foreign policy risks required by two conditions within the Active and Defensive Cyber Operations Ministerial Authorizations relies too much on technical attribution risks rather than characteristics that reflect Government of Canada's foreign policy.
3. The current governance framework does not include a mechanism to confirm an Active Cyber Operation's (ACO) alignment with broader Government of Canada (GC) strategic priorities as required by the CSE Act and the Ministerial Authorization. While these objectives and priorities that are outside CSE and GAC's remit alone, the two departments govern ACOs without input from the broader GC community involved in managing Canada's overarching objectives.
4. CSE and GAC have not established a threshold to determine how to identify and differentiate between a pre-emptive Defensive Cyber Operation and an Active Cyber Operation, which can lead to the insufficient involvement of GAC if the operation is misclassified as defensive.

5. CSE's internal policies regarding the collection of information in the conduct of cyber operations are not accurately described within the Active and Defensive Cyber Operations Ministerial Authorizations.

6. The Target Submission process, which occurs after planning documents have been approved, contains information that is pertinent to CSE's broader operational plans. The Target Submission at times contained pertinent information absent from these other documents, even though it is approved at a lower level of management.

7. CSE has provided its employees with high-level learning opportunities to learn about its new authorities to conduct Active and Defensive Cyber Operations (ACO/DCOs). However, employees working directly on ACO/DCOs may not have the requisite understanding of the specifics of CSE's new legal authorities and parameters surrounding their use.

8. CSE and GAC have not sufficiently developed a clear and objective framework with which to assess Canada's obligations under international law in relation to Active and Defensive Cyber Operations.

9. CSE expects GAC to provide notification of any changes to foreign policy risks, but has not sufficiently considered the need to communicate other risks that may arise during an operation to GAC. Further, information critical to GAC's assessment of foreign policy risks has also been excluded in materials CSE uses to engage GAC on an operation. As such, within the current consultation framework, CSE may not sufficiently communicate relevant information to GAC in support of its foreign policy assessment, and to manage ongoing changes in the risk associated with a cyber operation.

NSIRA's recommendations

Recommendation
Recommendation 1. CSE should more precisely define the classes of activities, associated techniques, and intended target sets to be undertaken for Active and Defensive Cyber Operations as well as their underlying rationale and objectives, both in its Applications and associated Ministerial Authorizations for these activities.
Recommendation 2. GAC should include a mechanism to assess all relevant foreign policy risk parameters of active and defensive cyber operations within the associated ministerial authorizations.
Recommendation 3. CSE and GAC should establish a framework to consult key stakeholders, such as the National Security and Intelligence Advisor to the Prime Minister and other federal departments whose mandates intersect with proposed active cyber operations, to ensure that they align with broader Government of Canada strategic priorities and that the requirements of the CSE Act are satisfied.

Recommendation
Recommendation 4. CSE and GAC should develop a threshold that discerns between an active cyber operation and a pre-emptive defensive cyber operation, and this threshold should be described to the Minister of National Defence within the applicable Ministerial Authorizations.
Recommendation 5. In its applications to the Minister of National Defence, CSE should accurately describe the potential for collection activities to occur under separate authorizations while engaging in active and defensive cyber operations.
Recommendation 6. CSE should include all pertinent information, including targeting and contextual information, within all operational plans in place for a cyber operation, and in materials it presents to GAC.
Recommendation 7. CSE should provide a structured training program to its employees involved in the execution of active and defensive cyber operations (ACO/DCOs), to ensure that they have the requisite knowledge of CSE's legal authorities, requirements, and prohibitions, as required by the associated Ministerial Authorizations.
Recommendation 8. CSE and GAC should provide an assessment of the international legal regime applicable to the conduct of active and defensive cyber operations. Additionally, CSE should require that GAC conduct and document a thorough legal assessment of each operation's compliance with international law.
Recommendation 9. CSE and GAC should communicate to one another all relevant information and any new developments relevant to assessing risks associated with a cyber operation, both in the planning phases and during its execution.

Review of Information Sharing across Aspects of CSE's Mandate

NSIRA's findings

1. CSE's internal sharing of information between the FI and cybersecurity aspects of the mandate has not been sufficiently examined for compliance with the *Privacy Act.*
2. With one exception, the Chief of CSE's applications for Ministerial Authorizations issued in 2020 appropriately informed the Minister of National Defence that retained information might be used to support a different aspect.
3. The applications for foreign intelligence authorizations by the Chief of CSE for the period of review appropriately informed the Minister of National Defence how the essentiality condition in paragraph 34(2)(*c*) is met for IRTC collected under the FI aspect.

4. CSE's policy framework with regards to the internal sharing of information between the foreign intelligence and cybersecurity aspects of the mandate is compliant with the CSE Act.

NSIRA's recommendations, and CSE response

Recommendation	CSE Response (May 26, 2022)
Recommendation 1. CSE should obtain additional legal advice on its internal sharing of information between the foreign intelligence and cybersecurity aspects of the mandate, explicitly in relation to compliance with the *Privacy Act*, which thoroughly addresses the following two issues: 1) Whether the internal sharing of information between the foreign intelligence and cybersecurity aspects of the mandate is a use or a disclosure of information for the purposes of the *Privacy Act*; and 2) Whether uses and disclosures are done in accordance with sections 7 and 8 of the *Privacy Act*.	**Disagree.** CSE does not accept recommendation 1. CSE has already received comprehensive and clear legal advice on this matter from the Department of Justice and has relied on that advice in the conduct of its activities (which NSIRA has found lawful).
Recommendation 2. All foreign intelligence and cybersecurity applications from the Chief of CSE should appropriately inform the Minister of National Defence that retained information might be used to support a different aspect.	CSE has already implemented the recommended action. CSE notes that it had and continues to inform the Minister about the use of information for other aspects of its mandate. Applications for all foreign intelligence and cybersecurity Ministerial Authorizations in 2021-2022 included wording to clearly reflect that information collected under one aspect of CSE's mandate could be used to support a different aspect.

Department of National Defence and the Canadian Armed Forces

Review of the Canadian Forces National Counter-Intelligence Unit — Operational Collection and Privacy Practices

NSIRA's findings

1. NSIRA found that CFNCIU is inappropriately relying on DND/CAF policies as lawful authority to interfere with a Subject's reasonable expectation of privacy.
2. NSIRA found that the DND/CAF checklist applied as a standard investigative operating procedure risks capturing information that is protected by s. 8 of the *Charter*.
3. NSIRA found that DND/CAF is applying a definition of metadata that captures information that could be subject to a reasonable expectation of privacy.
4. NSIRA found that CFNCIU risks breaching protected privacy interests by not having clear policy guidance based on lawful authority for IT searches, and by expanding IT searches beyond the approved search parameters.
5. NSIRA found that the investigative IT system practices it observed in the context CFNCIU's CI investigations have insufficient oversight to ensure that they are as minimally invasive as possible.

NSIRA's recommendations

Recommendation
Recommendation 1. NSIRA recommends that DND/CAF suspend investigative IT system practices in the context of CFNCIU CI investigations until a reasonable legal authority has been established.
Recommendation 2. Once a reasonable legal authority has been established DND/CAF should create a new policy framework that is reflective of the noted findings, namely, the multi-point checklist, the categorization of metadata, and that IT searches be as minimally invasiveness as possible.

Department of National Defence / Canadian Armed Forces Response to NSIRA Annual Report (2021)

The Department of National Defence / Canadian Armed Forces (DND/CAF) acknowledges and welcomes the 2021 Annual Report produced by the National Security Intelligence Review Agency (NSIRA). DND/CAF recognizes the importance of independent, external review of Government of Canada national security and intelligence activities to ensure that they are lawful, reasonable and necessary.

Furthermore, DND/CAF remains committed to having open and transparent discussions about these national security and intelligence activities as external reviews enhance the manner by which the department carries out its activities on behalf of Canadians. DND/CAF will continue to take into consideration all recommendations made by NSIRA in their external reviews and looks forward to receiving further reports from them.

Multi-departmental reviews

Review of Federal Institutions' Disclosures of Information under the *Security of Canada Information Disclosure Act* in 2020, a Joint Review with the Office of the Privacy Commissioner

Findings

1. National security-related personal information can be disclosed in situations where federal institutions are not conscious of the requirements for lawful authority to do so.
2. Almost all (approximately 99%) of the disclosures of information made under the *Security of Canada Information Disclosure Act* (SCIDA) in 2020 satisfied the disclosure test under paragraph 5(1)(a) based on information reviewed.
3. Almost all (approximately 99%) of the disclosures of information made under SCIDA in 2020, appear not to affect any persons' privacy interest more than was reasonably necessary in the circumstances based on information reviewed. However, the one non-compliant disclosure by the RCMP represents the vast majority of all confirmed personal information that was disclosed under SCIDA in 2020.
4. Almost all of the disclosures (nearly 98%) included accuracy and reliability statements, although there were inconsistencies with respect to the sufficiency and specificity of statements.
5. The record keeping of one institution which used SCIDA for the first time did not meet SCIDA's record-keeping requirements.
6. Most records were well organized with no discrepancies, although some were provided in a manner that was difficult to understand and review.
7. The review found instances where records kept for disclosures did not contain a sufficient description, as required under paragraph 9(1)(e), of the information that was relied on to satisfy the disclosing institution that the disclosure was authorized under SCIDA.
8. Almost all disclosures (over 97%) included caveats, which supported originator control and responsible information sharing.

9. IRCC and CSE, as well as GAC and CSIS, regularly exchange information under SCIDA of a nature and in a manner that warrants information sharing arrangements, as encouraged by subsection 4(c) of SCIDA.

10. Public Safety Canada coordinates the implementation of SCIDA among federal institutions, and all 17 federal institutions listed in SCIDA have staff who have taken Public Safety Canada's SCIDA training.

11. The Canadian Food Inspection Agency did not have policies or procedures to support compliance with SCIDA.

NSIRA's recommendations and departmental responses

Recommendation	Response (February 2022)
Recommendation 1. In light of the restrictions under section 8 of the *Privacy Act* for all disclosures of personal information, NSIRA and the OPC recommend that institutions with national security expertise ensure that when they request personal information for national security-related purposes from other federal institutions, they make it clear that their requests, in and of themselves, do not constitute or confer authority for the other institution to disclose personal information.	**Agree.** Since requests for information do not, in and of themselves, authorize federal institutions to disclose personal information, several Government of Canada departments and agencies have already developed and implemented internal policies to set clear expectations, consistent guidelines and record-keeping practices for the disclosure of personal information for national security purposes in accordance with lawful authorities. Importantly, each federal institution is responsible for knowing and implementing its obligations, and each Deputy Head is responsible for ensuring that directives and resources are put in place to fulfil these obligations. Public Safety Canada will continue to work with partner departments and agencies to provide federal institutions with access to training, guidance and other useful resources on national security information sharing that help to explain what the requirements are for disclosing this type of information in a lawful manner. Public Safety Canada will also update its SCIDA Guide and related templates for requesting and disclosing information under the SCIDA to support federal institutions in understanding their authorities for

Recommendation	Response (February 2022)
	requesting and disclosing national security information.
Recommendation 2. NSIRA and the OPC recommend that the RCMP finish updating its SCIDA policy to support compliance with the disclosure test in SCIDA, and provide guidance to its decision-makers empowered to make SCIDA disclosures on the analysis required to satisfy themselves that the disclosure test is met; and, ensure that these decisions are properly documented.	**Agree.** The RCMP has made significant progress towards completing its SCIDA policy modernization since April 2021. This updated SCIDA policy will provide an RCMP-specific complement to Public Safety's broader guidance to federal partners on SCIDA disclosures. The RCMP's updated policy tailors SCIDA guidance to a law enforcement environment and will serve to empower RCMP decision-makers to confidently share national security information in a compliant manner and aid in ensuring that decisions to disclose personal information are properly documented.
Recommendation 3. First, NSIRA and the OPC recommend that the RCMP provide fulsome and accurate information to DND/CAF about the non-compliant disclosure. Second, NSIRA and the OPC recommend that consistent with section 5.1 of SCIDA, DND/CAF assess the necessity of retaining the personal information received in light of this new information, our findings, associated DND/CAF directives and other applicable policies.	**Partially agree.** The RCMP does not agree that it failed to provide fulsome and accurate information to DND-CAF. The RCMP disclosed information that they were satisfied would contribute to the responsibility of the Department of National Defence and the Canadian Armed Forces to identify potential threats to military personnel and to provide strategic warning of emerging threats, in support of their counter-terrorism mandate. At the time of the disclosure, the RCMP were satisfied that the disclosure would not affect any person's privacy interest more than was reasonably necessary in the circumstances. DND-CAF will assess the necessity of retaining the personal information received in light of any new information provided by the RCMP, NSIRA and the OPC's findings, and associated DND-CAF directives and policies. As indicated in the SCIDA report, DND/CAF received the information from the RCMP based on its counter-terrorism mandate.
Recommendation 4. NSIRA and the OPC recommend that the federal institutions listed in SCIDA avoid formulaic language in statements of	**Agree.** Several departments and agencies have existing internal policies which request that statements of accuracy and reliability be tailored

Recommendation	Response (February 2022)
accuracy and reliability when the nature and source of information disclosed is not derived from a routine process.	to the specific disclosure and avoid the use of formulaic language. To further bolster this recommendation across federal institutions using the SCIDA to share information, Public Safety will update its SCIDA Guide, training and related guidance materials to reflect the fact that federal institutions should provide specific and clear statements of accuracy and reliability in circumstances where the information being disclosed is obtained through a non-routine process. Public Safety will equally encourage federal partners to include this guidance on statements of accuracy and reliability in their own internal policies where applicable.
Recommendation 5. NSIRA and the OPC recommend that institutions listed in Schedule 3 of SCIDA that request information from institutions not listed in SCIDA, inform the disclosing institution of their legal obligations with respect to disclosing information under SCIDA, including record-keeping requirements, and encourage the disclosing institution to seek advice from the Department of Justice and Public Safety Canada.	**Agree.** In the interest of furthering compliance with SCIDA among federal institutions, it is considered a best practice for requesting institutions listed in Schedule 3 of the Act to inform disclosing institutions not listed in the SCIDA of their legal obligations with respect to any disclosures made under SCIDA, including record-keeping requirements. It is also considered a best practice for federal institutions to encourage partners that are not as familiar with the disclosure authorities under the SCIDA to seek out the resources available from the Department of Justice and Public Safety, as appropriate. While recognizing that these are best practices and not legal obligations of recipients, Public Safety will encourage partners to implement these best practices by including related guidance in its updated SCIDA guide.
Recommendation 6. NSIRA and the OPC recommend that federal institutions that routinely disclose or receive in accordance with SCIDA standardize their record keeping in accordance with the latest Public Safety guidance.	**Agree.** Several institutions have already, or are currently in the process of, standardizing their record-keeping policies to reflect the latest Public Safety guidance. Continued work through the Public Safety-led working groups will further help to bring record-keeping practices in line with

Recommendation	Response (February 2022)
	standard guidelines for institutions that have yet to do so. Additionally, several partners have internal naming conventions or file reference systems which aid in record keeping standardization. Where such a system is not in place, Public Safety pioneered a common 'File Reference Number' system for institutions to use in their disclosures and receipts in the aim of standardizing their record keeping practices.
Recommendation 7. NSIRA and the OPC recommend that institutions ensure that records kept for bulk disclosures include an appropriately robust description of the information relied on to satisfy itself that the disclosure of all elements of the dataset meets section 5 of SCIDA, and that the level of internal oversight is commensurate with the privacy risk.	**Agree.** Records kept for bulk disclosures must contain sufficient information to demonstrate that the disclosure of all elements of the dataset meet the contribution and proportionality thresholds contained in the disclosure test of section 5 of the Act, and the level of internal oversight must be commensurate with the privacy risk. In certain cases, however, operational exigencies may require immediate action and follow-up oversight commensurate with the level of risk related to a threat that undermines the security of Canada. To assist departments and agencies in implementing this recommendation, further clarification from NSIRA and the OPC would be greatly appreciated regarding what constitutes an "appropriately robust description" of this information. Similarly, further clarification from NSIRA and the OPC on what constitutes a "bulk disclosure" would be equally appreciated as there is currently no standard Government of Canada definition for this term. Once these elements have been clarified, Public Safety will update the SCIDA guidance materials accordingly and share this information through their related interdepartmental working groups.
Recommendation 8. NSIRA and the OPC recommend that federal institutions include	**Agree.** Several institutions already include or request that information describing how the

Recommendation	Response (February 2022)
information about how the disclosure will contribute to their jurisdiction or responsibilities in respect of activities that undermine the security of Canada, and other information relevant to the disclosure test, in their written requests for information under SCIDA, even if this information was verbally communicated prior to the request to enable appropriate record keeping by disclosing institutions under SCIDA.	disclosure will contribute to recipient institutions' jurisdiction or responsibilities in respect of activities that undermine the security of Canada be provided in writing. In order to assist in implementing this recommendation across all institutions, Public Safety will update its templates for requesting and disclosing information under the SCIDA to emphasize the importance of including this information in the written request or disclosure letter. Institutions which do not currently have a practice in place of including this information agree to review their internal policies in accordance with the updated SCIDA guidance materials once published.
Recommendation 9. NSIRA and the OPC recommend that IRCC and the CSE enter into an information-sharing arrangement that structures their disclosure of information under SCIDA.	**Agree.** IRCC and the CSE will begin discussions to explore the best solutions for creating an information sharing agreement between both institutions that structures the disclosure of information under the SCIDA.
Recommendation 10. NSIRA and the OPC recommend that CSIS and GAC update their information-sharing arrangement, previously agreed upon under SCISA, to account for SCIDA.	**Agree.** CSIS and GAC will explore how best to update their information sharing agreement, previously agreed to under the SCISA, to account for the SCIDA. Both institutions will endeavour to begin the process of updating the information sharing arrangement within a reasonable timeframe and complete updates as soon as feasibly possible working within the constraints of existing priorities, emerging operational emergencies, and other complications which affect timelines.
Recommendation 11. NSIRA and the OPC recommend that the Canadian Food Inspection Agency consult Public Safety Canada, and develop and implement policies and procedures to support compliance with SCIDA.	**Agree.** Although the Canadian Food Inspection Agency (CFIA) has not yet disclosed or received information under the SCIDA, it will work collaboratively with Public Safety to develop and implement policies and procedures to support SCIDA compliance. CFIA staff will therefore feel empowered to disclose or receive national security

Recommendation	Response (February 2022)
	information under the SCIDA should the need arise.
Recommendation 12. NSIRA recommends that Immigration, Refugees and Citizenship Canada and other institutions which routinely receive requests for information under SCIDA, put into written policy the practice of keeping information received in requests for information separate from the rest of its databanks and watch lists.	**Agree.** IRCC has an existing operational practice of separating requests for information from the rest of its databanks and watch lists. Although this practice is included in its Standard Operating Procedures document, for added clarity, IRCC will also add this policy into their Information Sharing Policy guide. Public Safety Canada will also include this guidance in its updated SCIDA guidance materials to encourage broader uptake of this best practice by other institutions which routinely receive requests for information under SCIDA.

Review of Departmental Implementation of the *Avoiding Complicity in Mistreatment by Foreign Entities Act* for 2020

NSIRA's findings

1. NSIRA found that CBSA and Public Safety have yet to finalize their policy frameworks in support of Directions received under the ACA.
2. NSIRA found that from January 1, 2020 to December 31, 2020, no cases under the ACA were escalated to deputy heads in any department.
3. NSIR-A found that even when departments employed similar methodologies and sources of information to inform their determination of whether or not a case involving the same country of concern should be escalated, significant divergences in the evaluation of risk and the required level of approval emerge.
4. NSIRA found that in a case study regarding the disclosure of information, the risk of mistreatment was substantial, and the decision should have been referred to the Deputy Minister of Foreign Affairs as the accountable deputy minister for this request.

Annex E: Statistics on complaint investigations

January 1, 2021, to December 31, 2021

Intake Inquiries	**67**		
New complaints filed	**86**		
NSIRA Act, section 16 (CSIS complaints)	14		
NSIRA Act, section 17 (CSE complaints)	3		
NSIRA Act, section 18 (security clearances)	4		
NSIRA Act, section 19 (RCMP referred complaints)	5		
NSIRA Act, section 19 (*Citizenship Act*)	0		
NSIRA Act, section 45 (CHRC referrals)	60		
Decision on jurisdiction to investigate	**7**		
	Accepted	**Declined**	**Withdrawn**
NSIRA Act, section 16 (CSIS complaints)	3	14	2
NSIRA Act, section 17 (CSE complaints)	0	2	0
NSIRA Act, section 18 (security clearances)	4	5	1
NSIRA Act, section 19 (RCMP referred complaints)	0	1	0
Total	7	22	3
Active investigations	**81**		
NSIRA Act, section 16 (CSIS complaints)	12		
NSIRA Act, section 17 (CSE complaints)	0		
NSIRA Act, section 18 (Security clearances)	5		
NSIRA Act, section 19 (RCMP referred complaints)	4		
NSIRA Act, section 45 (CHRC referrals)	60		

Informal resolution		**3**	
NSIRA Act, section 16 (CSIS complaints)		2	
NSIRA Act, section 18 (security clearances)		1	
NSIRA Act, section 19 (RCMP referred complaints)		0	
NSIRA Act, section 45 (CHRC referrals)		0	
Total investigations closed		**3**	
	Final report	**Resolved informally**	**Withdrawn**
NSIRA Act, section 16 (CSIS complaints)	1	0	0
NSIRA Act, section 18 (security clearances)	0	0	0
NSIRA Act, section 19 (RCMP referred complaints)	0	0	0
NSIRA Act, section 45 (CHRC referrals)	0	0	2
Total	1	0	2
Investigations carried to the next calendar year		**78**	
NSIRA Act, section 16 (CSIS complaints)		11	
NSIRA Act, section 18 (security clearances)		5	
NSIRA Act, section 19 (RCMP referred complaints)		4	
NSIRA Act, section 45 (CHRC referrals)		58	

Note: Abbreviations are spelled out in Annex A.

Endnotes

[1] National Security and Intelligence Review Agency (NSIRA), *2019 Annual Report:* https://www.nsira-ossnr.gc.ca/wp-content/uploads/2020/12/AR-NSIRA-Eng-Final.pdf

[2] *National Security and Intelligence Review Agency Act* (S.C. 2019, c. 13, s. 2) (NSIRA Act): https://laws-lois.justice.gc.ca/eng/acts/N-16.62/page-1.html

[3] Civilian Review and Complaints Commission for the RCMP website: https://www.crcc-ccetp.gc.ca

[4] NSIRA reviews, https://nsira-ossnr.gc.ca/reviews

[5] **Terms and definitions:** *Capability* — Anything that enables the Canadian Security Intelligence Service (CSIS) to conduct operations. Capabilities include technologies and techniques. In some cases, more than one technology or technique can produce a capability. *Technique* — A way of carrying out a particular task or operation. *Technology* — Equipment (both hardware and software) developed from the application of scientific knowledge.

[6] In March 2022, CSIS advised that the updated policy suite was published on December 17, 2021.

[7] *NSIRA Act*, s. 8(2).

[8] The CSIS Act requires CSIS to provide NSIRA with certain information regarding the following activities; threat reduction measures (section 12.1 (3.5)), datasets (section 11.25), justification for acts or omissions that would otherwise constitute an offence (subsection 20.1 (26)), unlawful activities (subsection 20(4)), cooperation arrangements (section 17), ministerial direction (subsection 6(2)) and the CSIS Director's Report (subsection 6(4)).

[9] Where possible, observations will also be included in NSIRA's public annual report to Parliament.

[10] *Anti-terrorism Act,* SC 2015, c. 20.

[11] CSIS Act, section 2 defines threats to national security.

[12] Report of the Events Related to Maher Arar, Factual Background Vol I, note 10, http://www.sirc-csars.gc.ca/pdfs/cm_arar_bgv1-eng.pdf.

[13] Amendments to the CSIS Act — Data Analytics Backgrounder, CSIS, July 18, 2020, https://www.canada.ca/en/security-intelligence-service/news/2020/06/amendments-to-the-csis-act—data-analytics.html

[14] For more information on CSIS's legislative requirements to provide NSIRA with information on key CSIS activities, please see endnote 8.

[15] In 2021, CSIS evaluated four publicly available datasets and retained two. Of the other two datasets, it was found that one had been sent late for evaluation so it was deleted with no information retained and the other was found to be administrative and not subject to section 11 of the CSIS Act.

[16] Applications to retain the two Canadian datasets evaluated by CSIS in 2021 are pending decisions by the Federal Court.

[17] In 2019, CSIS sought ministerial authorization to retain eight foreign datasets. While no foreign datasets were evaluated in 2021, one foreign dataset was retained following ministerial authorization (by the Director as designate) and ratification by the Intelligence Commissioner, further to an application made in 2019.

[18] CSIS Justification Framework, https://www.canada.ca/en/security-intelligence-service/news/2020/06/amendments-to-the-csis-act–justification-framework.html

[19] The number of instances of non-compliance processed by CSIS includes instances of non-compliance as well as those instances that were deemed compliant on review by CSIS.

[20] The total number of incidents of non-compliance were not further broken down in 2019 and 2020. This number represents the number of incidents of non-compliance with requirements such as the CSIS Act, the *Canadian Charter of Rights and Freedoms*, warrant terms and conditions, or CSIS internal policies or procedures.

[21] Review of the Communications Security Establishment's (CSE's) Disclosures of Canadian Identifying Information (CII) (NSIRA Review 08-501-3).

[22] Pursuant to section 35 of the NSIRA Act, if, in the opinion of the Agency, a national security or intelligence activity carried out by a department may not be in compliance with the law, NSIRA must submit a compliance report to the responsible minister, with a copy sent to the deputy head concerned. CSE maintains that it acted in compliance with the law.

[23] Pursuant to section 31 of the NSIRA Act, NSIRA may direct a department to conduct a study of an activity in order to ensure that a department's activities are compliant with the law and applicable ministerial direction, and are reasonable and necessary.

[24] Section 43 of the CSE Act requires CSE to ensure that disclosures of CII are "essential to international affairs, defence, security or cybersecurity." This departmental study examined CSE disclosures of CII to Government of Canada departments other than CSIS, the Royal Canadian Mounted Police (RCMP) and the Canada Border Services Agency (CBSA). This study also examined all disclosures to foreign partners.

[25] The global information infrastructure is defined in the CSE Act as including electromagnetic emissions, any equipment producing such emissions, communications systems, information technology systems and networks, and any data or technical information carried on, contained in or relating to those emissions, that equipment, those systems or those networks.

[26] Incidental collection, in the context of the acquisition of information by CSE, refers to information acquired that was not itself deliberately sought, and that the activity that enabled the acquisition of this information was not directed at a Canadian or a person in Canada.

[27] Five Eyes refers to the formal cooperation agreements between the signals intelligence agencies of the governments of Canada, the United States, the United Kingdom, Australia and New Zealand.

[28] The Privacy Incidents File is a record of incidents attributable to CSE involving information about a Canadian (person or business), or any person in Canada, that was handled in a manner counter to, or is not provided for, in existing policy. This type of mishandling is labelled a "privacy incident."

[29] The Second Party Incident File is a record of privacy or compliance incidents that involve a Canadian or a person in Canada, and are attributable to a second party partner or a domestic partner. These incidents may be identified by partners or by CSE. This type of mishandling is also labelled a "privacy incident." Second party partners are the national cryptologic agencies of Australia (Australian Signals Directorate), the United Kingdom

(Government Communications Headquarters), New Zealand (Government Communications Security Bureau), and the United States of America (National Security Agency).

[30] The Minor Procedural Errors File is a log of operational compliance incidents where CSE improperly handled information about a Canadian or a person in Canada, but the information was contained within CSE. This type of mishandling is labelled a procedural error.

[31] NSIRA 2020 Annual Report, Section 1.5, "Trust but verify."

[32] CSE delays in fulfilling NSIRA's information requests precede the COVID-19 pandemic. NSIRA has tracked response times for information requests through internal memos, spreadsheets and briefing notes since NSIRA's inception in August 2019.

[33] National Security and Intelligence Committee of Parliamentarians, *2019 Annual Report*, Chapter 3: Canada Border Services Agency, https://www.nsicop-cpsnr.ca/reports-rapports-en.html

[34] The term border continuum is used here to refer to the activities and processes associated with the international movement of individuals, including foreign nationals coming to Canada (immigration applicants, refugees, and asylum claimants), and Canadian citizens and permanent residents travelling internationally with Canadian-issued travel documents (e.g., passports).

[35] The term steady-state is used to refer to activities undertaken as part of established, ongoing policies and programs, as opposed to activities undertaken as part of developmental or pilot projects with defined timelines.

[36] Purpose limitation involves explicitly stipulating the specific purpose for which the collected biometrics will be used, with a commitment to not use them for any additional purposes in the future.

[37] *Security of Canada Information Disclosure Act* (SCIDA), S.C. 2015, c. 20, s. 2, https://laws.justice.gc.ca/eng/acts/S-6.9/. SCIDA came into force on June 21, 2019. SCIDA's predecessor, the *Security of Canada Information Sharing Act* (SCISA), was in force from August 1, 2015, to June 20, 2019.

[38] SCIDA, ss. 5(1)

[39] SCIDA, s. 5.1

[40] SCIDA, para. 4(*c*)

[41] For the 2019 review period, the 12 departments that received directions under *Avoiding Complicity in Mistreatment by Foreign Entities Act* were the CBSA; Canada Revenue Agency; CSIS; CSE; Fisheries and Oceans Canada; Department of National Defence and Canadian Armed Forces; Financial Transactions and Reports Analysis Centre of Canada; Global Affairs Canada; Immigration, Refugees and Citizenship Canada; Public Safety Canada; the RCMP; and Transport Canada.

[42] NSIRA Act, paragraph 8(1)(*b*)

[43] Call to Action on Anti-Racism, Equity, and Inclusion in the Federal Public Service, https://www.canada.ca/en/privy-council/corporate/clerk/call-to-action-anti-racism-equity-inclusion-federal-public-service.html

[44] Note that sometimes work on reviews, including requests for information, began prior to finalizing the terms of reference.

[45] For some reviews, NSIRA was unable to publish some or all such information in this year's annual report. Full executive summaries of most reviews discussed in this annual report are available on request, should they not already be published at https://nsira-ossnr.gc.ca/reviews at the time of this report's publication.