National Security and Intelligence Review Agency

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



NSIRA

Canada's independent expert review body for all national security and intelligence activities.

2019 Annual Report

Canada

© Her Majesty the Queen in Right of Canada, as represented by the National Security and Intelligence Review Agency, 2020.
ISSN 2563-5778
Catalogue No.: PS106-9E-PDF

November 20, 2020



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 first annual report. Consistent with subsection 38(1) of the *National Security and Intelligence Review Agency Act*, the report includes information about our activities in 2019, as well as our findings and recommendations. Pursuant to transitional provisions 12(1) and 12(2) of the *National Security Act, 2017*, this report also includes information that our predecessor organizations, the Security Intelligence Review Committee and the Office of the Communications Security Establishment Commissioner, had not yet reported on publicly.

In accordance with paragraph 52(1)(b) of the *National Security and Intelligence Review Agency Act*, our report was prepared after consultation with the deputy heads concerned 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 or the professional secrecy of advocates and notaries or to litigation privilege.

Yours sincerely,

The Honourable Dr. Ian Holloway, P.C., C.D., Q.C.
Acting Chair
National Security and Intelligence Review Agency



NSIRA

Canada's independent expert review body for all national security and intelligence activities.

2019 Annual Report

Table of Contents

Committee message ii
Executive summary v
Introduction 14
Part 1: Institution building 16
Review 16
Complaints investigations 17
NSIRA's values 18
Part 2: Review 20
Section I — The information continuum 20
Section II — Collection 22
Section III — Safeguarding 34
Section IV — Sharing 40
Section V — Action 47
Part 3: Complaints 52
Section I — NSIRA's complaints investigation mandate 52
Section II — Synopsis of trends and key themes 54
Section III — Whistleblower protection 55
Section IV — Priorities for the year ahead 56
Part 4: Engagement and transparency 58
Section I — Engagement 60
Section II — Transparency 60
Conclusion 62
Annex A: Summaries of NSIRA reviews finalized during the reporting period 63
Annex B: Summaries of unreleased SIRC and OCSEC reviews up to July 2019 73
Annex C: Summaries of complaints investigations 77
Annex D: Statistical tables on complaints 82
Annex E: NSIRA corporate organization, achievements and priorities 84
Annex F: List of abbreviations 87
Endnotes 88

Committee message

We are proud to present the first annual report of the National Security and Intelligence Review Agency (NSIRA) for work undertaken in 2019. Our enabling legislation requires us to present a report to Parliament each year with respect to our activities during the previous calendar year, including any reviews not yet made public by our predecessor organizations, the Security Intelligence Review Committee, and the Office of the Communications Security Establishment Commissioner. In doing so, our report discusses our activities within a framework that addresses the complex, multi-agency and interwoven approach to national security that exists in Canada.

We are primarily a retrospective body, meaning we generally look at activities that have already taken place and make conclusions regarding their compliance with the law and ministerial direction. We also examine the reasonableness and necessity of a department's exercise of its powers. We are very conscious of the need for timely access to our findings by parliamentarians and all Canadians. NSIRA is committed to releasing redacted reviews as soon as possible after they are provided to the appropriate minister(s). We hope that our annual report will be a mechanism to reflect on broader trends and themes that cut across the full range of our work. We feel strongly that this approach is embedded in our mandate, and is supported by the government's own push for greater transparency in national security.

Openness also means deepening the dialogue with Canadians on national security. We have broadened our exposure to a diverse set of viewpoints to ensure our review plan reflects the concerns and priorities of all Canadians. This is particularly important in the context of anti-racism movements that are taking place around the world. We hope that engagement with diverse communities will help our organization learn about how we can best contribute to the fight against racism and discrimination in the national security and intelligence field. Engagement with Canadian experts, with cultural communities and with civil society has already begun as we build our social media presence and our capacity to organize videoconferences and in-person meetings. We have met several stakeholders in Ottawa, Victoria, Toronto and Calgary — and more activities are planned in the year ahead. Internationally, we work with and share our experiences with parallel review bodies as a member of the Five Eyes Intelligence Oversight and Review Council, which is made up of our partners in Australia, New Zealand, the United Kingdom and the United States.

We are mindful of the need to avoid overlap with other review bodies and to make the best use of resources within the national security community that are in place to facilitate our work. We know that for many departments and agencies, external review is a new endeavour that will take time to adjust to. We are very pleased with the level of cooperation and support we are seeing. We have developed and shared our three-year review plan, which we hope will clarify our work priorities and give the organizations that we will be reviewing time to adjust and prepare. Our legislation is unequivocal as to our access to information: we are entitled to timely access to anything that is in the possession or under the control of a department in relation to our reviews (except only Cabinet confidences). The integrity of our work demands this access. Our public reports will accordingly record any shortcomings in this regard. To avoid duplication and to enhance the quality of Canada's system of national security accountability, we are committed to cooperating with other oversight and review bodies, including the Intelligence Commissioner's Office, the National Security and Intelligence Committee of Parliamentarians, the Office of the Privacy Commissioner of Canada (OPC), the Civilian Review and Complaints Commission for the RCMP and the Office of the Auditor General of Canada[1].

NSIRA also brings together under one roof the investigation of complaints related to national security that are made by members of the public. We have a mandate to investigate complaints into the activities of the Canadian Security Intelligence Service, the Communications Security Establishment and national security-related activities of the Royal Canadian Mounted Police. Additionally, we can investigate complaints arising from an individual whose security clearance is denied or revoked, as well as referrals from the Canadian Human Rights Commission[2] and certain matters under the *Citizenship Act.* We are confident that this consolidation of complaints investigations will help to ensure that Canadians' national security-related grievances can be addressed with the greatest degree of consistency, quality and timeliness possible. A particular task we are undertaking over the next year is to improve the efficiency of the complaints process.

We would be remiss if we did not address the unique and challenging environment facing us all at this moment. The COVID-19 pandemic has had far-reaching consequences the world over that we are perhaps only beginning to understand. Throughout much of 2020, NSIRA staff have been working from home, with minimal access to the office and, therefore, minimal access to classified physical and electronic documents that must be kept within a secure space. We are very proud of the extraordinary work of our staff, who have kept momentum alive during this

difficult period, and who continue to put measures in place to enhance our organizational adaptability. We also expect that organizations that are subject to our review and complaints investigations will continue to allocate personnel to these vital functions, and continue to prioritize national security accountability as they too adjust to an ever-changing situation.

At this time, we would like to express our gratitude to three NSIRA members whose terms concluded this year: the Honourable Pierre Blais, the Honourable L. Yves Fortier, and Murray Rankin, NSIRA's first Chair. Their collegiality and leadership during a time of transition were greatly appreciated, and their contributions to national security accountability in Canada continue to be deeply felt.

We are honoured to have been chosen to be the first members of NSIRA. We are committed to providing meaningful findings and recommendations on the extent to which Canada's national security community is complying with the law and on the necessity and reasonableness of its actions. We look forward to the challenge facing us in this increasingly complex environment.

The Honourable Dr. Ian Holloway, P.C., C.D., Q.C. (Acting Chair)
The Honourable Marie Deschamps, C.C.
Professor Craig Forcese
The Honourable Marie-Lucie Morin, P.C., C.M.
The Honourable Pierre Blais, P.C. (Member until May 2020)
The Honourable L. Yves Fortier, P.C., C.C., O.Q., Q.C. (Member until October 2020)
Murray Rankin, Q.C. (Member and Chair until September 2020)

Executive summary

- Information pertaining to the transition from the Security Intelligence Review Committee (SIRC) to the National Security and Intelligence Review Agency (NSIRA), corporate milestones, organizational values and objectives, and other relevant elements, are briefly described in the introduction, and are supplemented with more detailed material in various annexes as well as on NSIRA's website.[3]

- Review findings and themes discussed in this report reflect NSIRA's work over the first several months of our mandate, beginning in July 2019. They also build on work done by SIRC and the Office of the Communications Security Establishment Commissioner (OCSEC), including reviews that these organizations had not yet released prior to the establishment of NSIRA. Summaries of these reviews are found in Annexes A and B. We discuss findings and themes in this report according to the "information continuum": collection, safeguarding, sharing and action.

- A key challenge for departments and agencies in Canada is to ensure that their use of new technology conforms to privacy laws and respects Canadians' rights under the *Canadian Charter of Rights and Freedoms* (the Charter). NSIRA is aware of instances where an agency used technology in ways that exceeded legal authorities. Notably, one of NSIRA's first reviews concerned the Canadian Security Intelligence Service's (CSIS) use of publicly available geolocation data. NSIRA concluded that CSIS's use of this data without a warrant risked breaching section 8 of the Charter, which protects against unreasonable search and seizure. NSIRA submitted a report under section 35 of the NSIRA Act, to the Minister of Public Safety and Emergency Preparedness regarding the possible unlawful activity.[4]

- The report provides an overview of some longstanding issues with regard to the failure of CSIS to meet its duty of candour to the Federal Court, most recently in relation to its human source activities.[5] Specifically, CSIS did not inform the Court that CSIS's warrant applications were based on intelligence that had likely been collected by illegal means. The Court also observed failings with regard to the Department of Justice's role in the situation. In response, the Government referred the matter to NSIRA for review under paragraph 8(1)(c) of the NSIRA Act. Over the next year, NSIRA will dedicate significant resources to a review stemming from this Federal Court decision.

- NSIRA has prioritized safeguarding (i.e., how the government protects people, information and assets) as a review theme we will examine on a yearly basis. In our first year, NSIRA completed one safeguarding review of CSIS, and commenced another within the Department of National Defence (DND). Of note, our observations with regard to the polygraph (i.e., "lie detector test") during the security clearance process, highlight a number of shortcomings, including:

- CSIS was unable to justify the capacity of examiners — who are not medical practitioners — to ask medical-related questions of the examinees.
- There were unequal outcomes or consequences for polygraph exams conducted on external applicants to CSIS vs. current employees.

- This finding raises broader issues. Although the Treasury Board Secretariat (TBS) Standard on Security Screening, created in 2014, cites the use of the polygraph as an appropriate tool for assessing candidates seeking an Enhanced Top Secret clearance, TBS was unable to provide any policy rationale for the use of this tool. NSIRA brought a number of shortcomings to the attention of TBS. The standard is currently under internal review at TBS, and we are awaiting the results.

- NSIRA made several findings and corresponding recommendations for the Communications Security Establishment (CSE) to improve its documentation, mitigation and privacy protection practices in relation to its Privacy Incidents File.

- In 2019, NSIRA launched our first interagency review, an assessment of the implementation of the 2017 Ministerial Direction on Avoiding Complicity in Mistreatment by Foreign Entities by: the Canada Border Services Agency, CSE, CSIS, DND, Global Affairs Canada, and the Royal Canadian Mounted Police. NSIRA found significant variation among the six departments and agencies in terms of their success in implementing the 2017 ministerial direction. While some departments or agencies, such as CSIS and CSE, had fairly advanced procedures for implementing the ministerial direction, the review highlighted some shortcomings. Some departments and agencies face challenges in operationalizing this direction. Some also face challenges in establishing decision-making mechanisms that are independent from the operational front line in cases where there is a risk of mistreatment. One

of the key issues that NSIRA's review identified was the inconsistent application of the "substantial risk of mistreatment" threshold across departments – under the 2017 directions and their successors, sharing is prohibited where there is a "substantial risk of mistreatment of an individual by a foreign entity". How departments and agencies assess this standard will be a future area of inquiry.

- In 2020–21, NSIRA is modernizing the process for addressing complaints. Our goal will not change: to provide a just and efficient investigation and resolution of complaints. Two priorities will guide the modernization: access to justice for self-represented complainants, and the need for a broader spectrum of tools to streamline the resolution of complaints.

- In previous correspondence to the Attorney General, NSIRA identified legislative gaps related to whistleblower protections in Canada's national security community and the corresponding negative implications resulting from these gaps.[6] In the interim, NSIRA will be implementing internal procedures to address concerns brought forward by members of the security and intelligence community.

- In 2019, NSIRA launched a series of public engagements to increase awareness of our new organization, expand our network, and deepen our understanding of Canadians' concerns relating to national security and intelligence activities. Over the coming year NSIRA intends to continue our outreach and engagement program, with a focus on four key areas: expanding our network to help us address issues related to new and emerging technologies (including artificial intelligence); broadening our dialogue with stakeholders to inform NSIRA's future review priorities; building new relationships with community groups, in an effort to demystify the complaints investigation process; and scaling up recruitment efforts to ensure NSIRA continues to build an elite workforce with a diverse set of skills and backgrounds.

- To enhance transparency, NSIRA also intends to proactively redact and release future NSIRA reports as they are approved throughout the year, rather than waiting for the release of our annual report to disclose our findings and recommendations. The organization is working with departments and agencies to ensure that this new approach is as timely and efficient as possible, and both protects vital national security and intelligence information, and provides the public with as much insight as possible into the results of NSIRA's reviews.

Introduction



01

The National Security and Intelligence Review Agency (NSIRA)[7] began operations July 12, 2019, as part of the transformation of Canada's national security accountability framework. As a result, this inaugural annual report covers only a six-month period, from July to the end of the 2019 calendar year.[8] During that time and continuing into 2020, NSIRA did a great deal of work to ensure the successful transition from the Security Intelligence Review Committee (SIRC),[9] to a larger organization with a much broader mandate.



02. Because the NSIRA website provides detailed information relating to NSIRA's mandate, the types of reviews undertaken, the process and lifecycle of a review, and the complaints investigation process, this report does not discuss these topics.

03. Instead, it focuses on NSIRA's initial work on reviews, our complaints investigations, and our public engagement and transparency efforts. The emphasis on analysis of recent findings and trends in review draws on previously unreleased SIRC and Office of the Communications Security Establishment Commissioner[10] reviews going back to 2018 and 2019, respectively, as well as NSIRA reviews completed in the first several months of operation. Summaries of these individual reports are available in Annexes A and B.

04. Part 1 outlines our organizational values and NSIRA's approach to building a new institution.

05. Part 2 provides detailed analysis of themes that cut across many of these reviews, drawing linkages and establishing a platform for future work.

06. Part 3 deals with our complaints investigations and briefly discusses themes from 2019 and priorities for the year ahead, with an emphasis on modernizing the complaints investigation process to ensure greater timeliness and accessibility. Summaries and statistics relating to complaints investigations are available in Annexes C and D.

07. Part 4 outlines NSIRA's efforts and our vision in addressing engagement and transparency, which are key priorities for the organization.

08. Key accomplishments and ongoing priorities with respect to NSIRA's corporate services, including measures taken to adapt to an expanded mandate, are detailed in Annex E. [11]

09. This is NSIRA's first annual report, and we have structured it in a way that aims to be useful and engaging for the reader, while it serves its intended function, namely, to make an important contribution to Canadians' dialogue on national security and intelligence issues. We are interested in feedback on how to make it as helpful and accessible as possible in achieving this aim.

Institution building

10. The creation of NSIRA, following the proclamation of the *National Security Act, 2017,* represented a considerable step forward in the development of national security and intelligence accountability in Canada. Over the past two decades, national security and intelligence operations have become increasingly interconnected within the Government of Canada. This resulted in a number of departments and agencies that had not traditionally been part of the security and intelligence community now playing key roles in this area. However, review bodies' powers did not evolve with the changing national security and intelligence landscape, and their ability to review agencies and make contributions remained compartmentalized.

11. NSIRA's creation remedies these long-standing gaps in Canada's national security architecture and significantly strengthens the framework for national security accountability. NSIRA has taken over the mandates of our predecessors to review the operations of the Canadian Security Intelligence Service (CSIS) and the Communications Security Establishment (CSE), respectively, but we also have an additional and novel mandate to review any activity in the federal government that relates to national security or intelligence. Alongside this expanded mandate, NSIRA has unfettered access to classified information in the possession or under the control of any department or agency (except Cabinet confidences). This allows NSIRA to break down the previously compartmentalized approach to review and accountability, and replace it with horizontal, in-depth interagency review. As such, Canada now has one of the world's most extensive systems for independent review of national security in the world.

12. Since July 2019, the NSIRA Secretariat has focused on ensuring a successful and effective transition to a much larger organization with a much broader mandate. This included emphasis on the following: securing new accommodations; effective staffing and knowledge development; establishing strong working relationships with departments and agencies, as well as other Canadian review bodies; and delivering on our mandatory reporting requirements. NSIRA absorbed a staff complement from the Security Intelligence Review Committee (SIRC), who had expertise in review and complaints investigation related to CSIS. Sustained effort to recruit staff and build knowledge of the broader security and intelligence community will continue in the year ahead.

Review

13. In the early months of our mandate, NSIRA developed a three-year review plan. This plan will help develop a systematic approach to deciding what to review and how to set priorities. Besides helping to guide resource allocation and staffing decisions in the medium term, the review plan provides clarity to the departments and agencies we review and prevents overlap with other review bodies.

14. Part of the challenge inherent in NSIRA's mandate is thinking differently about how to organize and undertake reviews. The interagency mandate allows for reviews to be planned and undertaken in a horizontal manner, involving several departments and agencies from the start. Similarly, NSIRA is also working in a horizontal manner internally, to incorporate legal and technical experts into reviews more systematically, so that considerations in these areas are built into reviews from the start.

15. Within this plan, in-depth review of CSIS and CSE remain organizational priorities. NSIRA is also developing foundational knowledge of national security and intelligence activities conducted in federal government institutions that have not traditionally been subject to review. Through a series of increasingly complex and in-depth reviews conducted over the upcoming years, NSIRA will seek to provide a holistic and detailed picture of activities, programs or key themes in the national security and intelligence community.

16. When conducting reviews, whether simple scoping exercises or more complex projects, NSIRA considers a number of elements to develop conclusions, findings and recommendations. These include the lawfulness, compliance with directives and policies, reasonableness, necessity, and proportionality of security and intelligence activities. These considerations help NSIRA ensure that Canadians are confident that national security and intelligence activities undertaken by the Government of Canada are thoroughly reviewed and assessed.

Complaints investigations

17. In addition to NSIRA's review mandate, the organization has the responsibility to investigate national security-related complaints. This includes hearing complaints from the public regarding actions taken by CSIS and CSE, national security-related complaints regarding the Royal Canadian Mounted Police (RCMP),[12] and complaints related to the revocation or denial of security clearances.

18. NSIRA acknowledges that the complaints investigation framework inherited from SIRC has been far too slow and too complex. An analysis of the number of complaints filed annually and the number outside NSIRA's jurisdiction to investigate also reveals a clear knowledge gap with respect to NSIRA's role in this regard. For these reasons, NSIRA has begun to reform the complaints process, including increasing access, timeliness and accountability.

NSIRA's values

19. NSIRA inherited a number of values, practices and expertise from the review agencies that came before. Nonetheless, NSIRA is dedicated to undertaking our work in a new way — one that emphasizes outreach, engagement and transparency. As such, NSIRA has begun a comprehensive program of engagement with civil society, community groups, academics and others, based on a number of objectives including but not limited to:

- informing NSIRA's review plan;
- raising awareness of and demystifying the complaints investigation process;
- leveraging and creating communities of interest on key issues (for instance, on artificial intelligence); and
- recruiting talented Canadians.

20. The new organization wants to break with previous practices that resulted in findings and recommendations being publicly reported only once per year. To increase transparency, NSIRA is committed to the release of unclassified versions of reviews as they become available after redaction and translation. By making our reviews available to the public, NSIRA hopes to increase transparency and accountability, and to open the door to extensive discussions and debate in the public sphere. Consequently, a priority is to draft reports that avoid classified information because the intent is to release them; this "write to release" approach will facilitate the redaction process, where necessary, and ensure more timely and effective release of information.[13]

21. NSIRA is committed to:

- openness and transparency, in an effort to better connect with Canadians;
- methodological excellence to ensure the quality of our work; and
- forward thinking and innovation, including how we consider the impacts of new technology and an ever-changing national security environment.

22. To achieve our numerous and complex objectives, NSIRA relies on a skilled and experienced workforce. As the organization grows, NSIRA will continue to recruit talented candidates that reflect Canada's diverse and inclusive nature.

23. NSIRA understands the importance of organizational health and wellness as fundamental to success. The organization wishes to be an employer of choice that promotes and provides a healthy work environment. Although the COVID-19 pandemic has raised unprecedented challenges, NSIRA remains focused on further adapting to the sweeping changes brought by the pandemic. Ensuring the physical and mental health and wellness of our staff remains a cornerstone of the organization's strategy as we develop creative ways to maintain effectiveness and efficiency while working in a distributed manner.

24. In addition to maintaining a broad expertise within the organization, NSIRA has been focusing on building a strong network of partnerships to help define our research priorities and deliver on our mandate. NSIRA has been working with other organizations within the Canadian review and accountability system, such as the National Security and Intelligence Committee of Parliamentarians (NSICOP)[14] and the Office of the Privacy Commissioner of Canada (OPC),[15] on issues of common interest to maximize both the effectiveness and efficiency of national security review agencies, while limiting duplication of efforts.

25. NSIRA made a great deal of progress in all aspects of our mandate throughout the first few months of operation in 2019. Many ambitious projects are under way for the year ahead, in order to progress on building an institution that is fit to play a broad and constructive role in Canada's system for national security accountability.

Review

Section I
— The information continuum

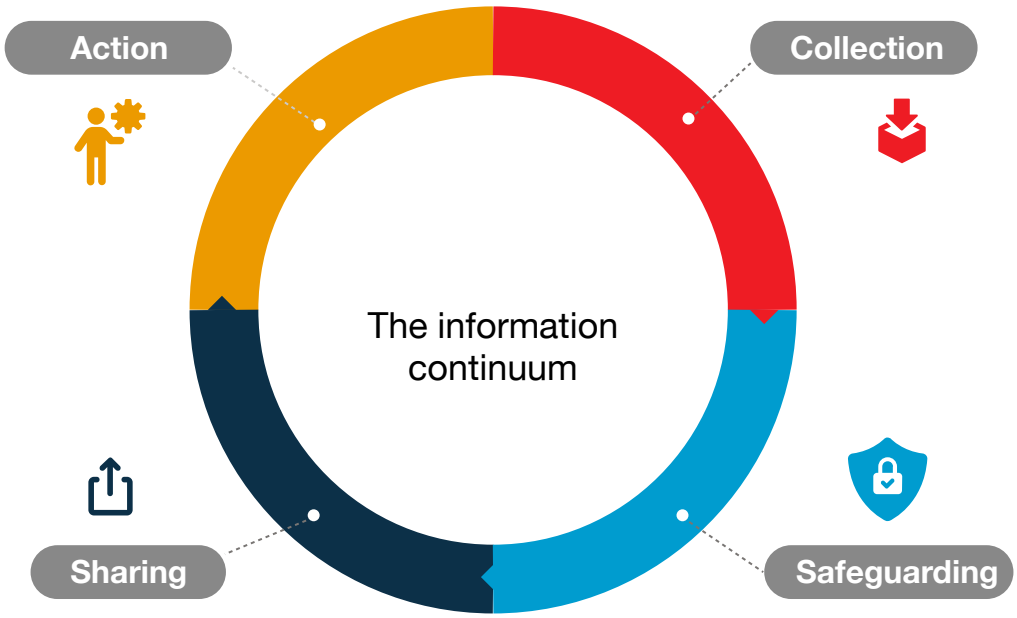
02

This part outlines NSIRA's framework for discussing findings and trends in review, and provides detailed analysis according to the four categories within this framework. This part does not go into detail about review methodology and prioritization. In short, as we expand our knowledge base of national security and intelligence activities across the Government of Canada, NSIRA aims to undertake increasingly complex reviews over the next three years.



27. Members of NSIRA are planning to proactively redact and publicly release full reviews, along with unclassified executive summaries, as they are approved and translated, rather than having to wait for the annual report to showcase the organization's review work. This new practice opens up opportunities for the annual report to discuss and dissect lessons learned throughout the year in new and interesting ways. Rather than discussing the findings and recommendations of each review individually (or vertically), as had been done in the Security Intelligence Review Committee (SIRC) and Office of the Communications Security Establishment Commissioner (OCSEC) annual reports, NSIRA will focus on the entire body of work horizontally, and ask what broad lessons, trends or themes emerge. NSIRA believes that this will allow for a more comprehensive analysis of findings and will help to develop more holistic and interconnected review planning.

28. The following discussion is organized according to what NSIRA calls the "information continuum." This continuum is meant to reflect the lifecycle of information, from how it is collected and safeguarded, to how it is shared and, ultimately, how it is used to inform real-world actions undertaken for national security or intelligence purposes.



29. NSIRA acknowledges that the information continuum differs from the national security and intelligence information cycle. The continuum is not a unidirectional process, and all concepts mentioned in it are intertwined. However, we hope that presenting our findings within this framework will facilitate a reader's understanding of key themes and priorities within the national security and intelligence environment. Future annual reports might adopt a different structure depending on the recommendations NSIRA receives and the information we wish to communicate.

Section II
— Collection

30. Collection is the first step in the information continuum described in this report. It refers to all forms of information gathering by the Government of Canada's departments and agencies that relates to national security or intelligence. It covers information that is gathered directly by these federal institutions, in Canada and abroad, as well as information received from other federal entities and other orders of government, such as information from provincial or municipal law enforcement. The receipt of information from foreign entities is also a form of collection, but given the special human rights considerations governing such activity, this report discusses this topic in the section on information sharing.

31. Departments and agencies collect information using a range of techniques. Some recruit human sources to collect information on the agency's behalf. Others intercept telecommunications through a variety of technical means, such as wiretaps. Telecommunications, in this context, refers to both the gathering of communications content (e.g., intercepting a voice conversation or email) and metadata (e.g., telecommunications subscriber information or information related to Internet connections). Importantly, collection here refers to information that is gathered by Government of Canada institutions both covertly and overtly, and includes publicly available information. The distinction between what is publicly available and what is not has been controversial, and it is a subject that NSIRA will review in the future. Often, the information collected relates only to one person or a handful of people; in other instances, departments and agencies collect data in bulk.[16]

32. Obviously, the collection of certain information by departments and agencies can intrude into the private affairs of Canadians. Indeed, of the many types of national security and intelligence activities that NSIRA is mandated to review, collection is the area with the most potential to impinge on the privacy rights of Canadians. Nonetheless, Canadians expect their private lives, communications and online activities to remain free from state surveillance unless the intrusion complies with the law (including, where required, pre-authorization by an independent judicial officer), and that the collection is reasonable, and goes no further than necessary to achieve a legitimate goal, such as the investigation of a criminal offence or the investigation of a threat to the security of Canada. For these reasons, scrutinizing the government's collection of information will be a permanent area of focus for NSIRA.

Legal frameworks

33. The legal frameworks governing information collection by government departments and agencies are complex, and vary from department to department, and agency to agency. There are a few overarching principles, however. In simple terms, all departments and agencies are subject to the *Canadian Charter of Rights and Freedoms* (the Charter) and must ensure that their collection of information is "reasonable" under section 8 of the Charter, which protects against "unreasonable search and seizure" of their persons, property and information. This means that where state action intrudes on a person's reasonable expectation of privacy, the search must generally be pre-authorized by an independent judicial officer — typically a judge issuing a warrant. In limited circumstances, however, warrantless collection of information in which a person has a reasonable expectation of privacy is permissible, so long as it is authorized by a law that is considered reasonable in striking an appropriate balance between privacy and the state interest being pursued, and the search is conducted reasonably.

34. In Canada, the police and other peace officers seek a number of different authorizations permitting intrusive searches and seizures that implicate a person's reasonable expectation of privacy. These "lawful access" authorizations include search warrants, production orders to obtain documents or records, and warrants authorizing the interception of private communications. The Canadian Security Intelligence Service (CSIS)[17] can seek warrants from the Federal Court authorizing the interception of any communication or the obtaining of any information, record, document or thing.[18] The procedures followed for obtaining these authorizations vary depending on the statute governing the agency seeking it, and also depend on the search's intrusiveness. The Communications Security Establishment (CSE),[19] for its part, collects information outside of Canada in accordance with its various mandates related to foreign intelligence and cybersecurity. Where those collection activities might otherwise contravene an act of Parliament or interfere with the reasonable expectation of privacy of a Canadian or any person in Canada, CSE must obtain ministerial authorizations from the Minister of National Defence.[20] Before they come into effect, CSE's ministerial authorizations under its foreign intelligence mandate and its cybersecurity and information assurance mandate must be approved by the Intelligence Commissioner, who is a retired judge.[21]

35. Regardless of the sensitivity of the information being collected, a department or agency must have a legal authority to collect it. Departments and agencies receive such legal authority from their enabling statutes (for example, the CSIS Act for CSIS; the CSE Act for CSE), as well as from common law powers, especially for the RCMP.

36. These statutes also set important limits, often by spelling out what information departments are permitted to collect, when and to what extent. For instance, CSE is prohibited from directing its collection against Canadians or persons in Canada. But it is not always possible to know in advance which information involves Canadians and which does not. As a result, CSE may sometimes collect information relating to Canadians and persons in Canada incidentally — that is, without deliberately seeking it. CSE must handle this information in accordance with the CSE Act and the ministerial authorizations that it has received from the Minister of National Defence.[22]

Ministerial direction and policy

37. The collection of information by the Government of Canada is guided not only by the law, but also by a range of ministerial directions and internal policies. Ministerial direction represents the formal guidance issued by a minister to a department or agency.[23] Though not a statutory instrument, a ministerial direction has a more robust legal status than mere departmental internal policy, and often serves to set out a minister's expectations regarding how a department should function, and how it should interpret its legal powers. These directions are used, for example, to implement the Government of Canada's Intelligence Priorities, which are periodically approved by Cabinet. The Intelligence Priorities set out those areas that the Government of Canada has identified as requiring the greatest need for information. Ministers then direct departments to allocate collection resources accordingly, although they must always remain within the scope of their legal collection mandates. When NSIRA reviews a collection activity related to national security or intelligence, we review not just compliance with the law, but also compliance with ministerial direction and internal policy.

2019 collection by the numbers:

CSIS collection warrants

April 1, 2018 – December 31, 2018



New: 10

Replacement: 11

Supplemental: 3

Total: 24

Applications Denied: 0

January 1, 2019 – December 31, 2019



New: 9

Replacement: 12

Supplemental: 2

Total: 23

Applications Denied: 1

CSIS targets

April 1, 2018 – December 31, 2018: 430

January 1, 2019 – December 31, 2019: 467

CSIS datasets

CSIS Canadian datasets retained after authorization by the Court:	0
CSIS applications to the Court to retain a Canadian dataset:	0
CSIS foreign datasets retained after approval by the Minister and Intelligence Commissioner:	0
CSIS applications to the Intelligence Commissioner to retain a foreign dataset:	0

CSE ministerial authorizations, 2019

Ministerial authorizations issued under the following sections of the CSE Act:

subsection	26(1),	foreign intelligence:	x
subsection	27(1),	cybersecurity - federal:	x
subsection	27(2),	cybersecurity - non-federal:	x
subsection	29(1),	defensive cyber operations:	x
subsection	30(1),	active cyber operations:	x

CSE has confirmed that, in 2019, ministerial authorizations were signed under each subsection listed in this table. However, CSE is of the view that releasing the specific numbers would be injurious to national security. NSIRA disagrees with this view. As of November 20, 2020, this issue could not be resolved. NSIRA will continue to work with CSE with a view to finding a compromise.

Collection challenges

Technology and privacy

38. Criminals and those who pose a threat to national security are constantly adopting the latest technologies to shield their activities from scrutiny. This places pressure on investigative agencies, in Canada and abroad, to maintain their capacity to collect usable information. As a result, Canada's national security and intelligence agencies must employ new technologies quickly to circumvent or get ahead of the capabilities of their subjects of investigation.

39. Unfortunately, many new technologies can be used in ways that erode privacy. The rise of the Internet and mobile communications means that individuals now generate far more information and metadata about themselves than in the past. At the same time, intelligence collectors are facing a progressive loss of direct access to private communications stemming from the increasing ubiquity of strong encryption. In part for these reasons, there has been heightened interest worldwide in the bulk collection of information and metadata in recent decades. This raw material is then sifted and analyzed to glean insights and patterns. For example, use of smartphones leaves digital traces that, particularly when assembled or later identified, can reveal contacts, patterns of movement and other intimate details. A key difference between bulk collection and more traditional techniques, such as wiretaps, is that the vast majority of the information collected relates to ordinary citizens who are not subjects of investigation. The risks that such techniques pose for personal privacy are clear.[24]

40. A major challenge for departments and agencies in Canada is to ensure that their use of new technology conforms to privacy laws and respects Charter rights. Generally, this requires departments and agencies to engage the federal Department of Justice to obtain advice on the legal parameters that govern the use of the technology, and then to put in place a strong policy framework and obtain the necessary authorizations before beginning to use a new technology. Often this is exactly what happens. But NSIRA is also aware of instances where technology was used in ways that exceeded legal authorities. These are described below. Some of these examples are drawn from NSIRA's reviews to date, while others are drawn from SIRC's history of reviewing CSIS.

41. On a few occasions in recent years, CSIS used new collection techniques without first fully understanding and addressing their legal and policy implications. In these cases, legal and policy work lagged behind the operational imperative to maintain and improve collection capabilities. This risked — and at times compromised — the lawfulness of the collection activity and the privacy of Canadians. The first example is from an NSIRA review:

- **a** **Geolocation:** One of NSIRA's first reviews concerned CSIS's use of publicly available geolocation data. This review raised pressing questions regarding the use of data that is publicly available, but that nevertheless engages a person's reasonable expectation of privacy. NSIRA concluded that CSIS's use of this data without a warrant risked breaching section 8 of the Charter, which protects

against unreasonable search and seizure. NSIRA's review examined the decision-making process that led CSIS to use this data without a warrant, and found that CSIS lacked the policies or procedures to ensure that before the data was used CSIS sought legal advice to avoid unlawful use of the data. On March 16, 2020, we submitted a report under section 35 of the NSIRA Act[25] to the Minister of Public Safety and Emergency Preparedness describing the possible unlawful activity. Under section 35, NSIRA must refer to the relevant minister any national security or intelligence activity that might not be in compliance with the law. The minister is then required to forward the report to the Attorney General.

42. Other examples can be drawn from the period before NSIRA was created, which were reported by the former review bodies, SIRC and OCSEC:

a **CSIS metadata:** A 2014 SIRC review[26] assessed whether CSIS's collection, use and retention of metadata collected under the authority of a Federal Court warrant was carried out lawfully and appropriately. At the time, CSIS warrants required any communications or metadata collected incidentally (i.e., not related to the subjects of the warrant) to be destroyed, unless certain conditions were met, including if there were reasonable grounds to believe that the information "may assist" in the investigation of a threat to the security of Canada. CSIS concluded that the words "may assist" established a low threshold, and accordingly retained and used the metadata, despite the data having been collected incidentally. SIRC was given no indication that CSIS had informed the Federal Court of the nature and scope of its activities. SIRC therefore recommended that CSIS make the Court aware of the extent of its retention and use of metadata collected under warrant. Alerted by SIRC's recommendation, the Federal Court concluded in October 2016 that CSIS could not retain the information unless it was related to a threat to the security of Canada, because CSIS's collection mandate in section 12 of the CSIS Act includes the qualifier that CSIS can collect information or intelligence only "to the extent that it is strictly necessary." The Court found that CSIS's authority to retain information was informed by this limit. Therefore, it held that CSIS had exceeded its lawful authority in retaining much of the metadata collected under warrant. The Court also found that CSIS had failed in its duty of candour to the Court. As discussed below, the question of retention of electronic "datasets" is a matter now more fully regulated by the CSIS Act, following amendments made by the *National Security Act, 2017.*

b **CSE metadata:** Technological advances have created vast amounts of information in the digital realm. Agencies often turn to automation to apply privacy protection measures to large amounts of information efficiently. In 2013, CSE notified its previous review body, OCSEC, that metadata containing Canadian identity information had not been properly minimized by software.[27] This software failure resulted in Canada's Five Eyes allies receiving data that Canadian laws prohibit CSE from sharing. CSE suspended sharing certain types of metadata while it developed a solution to rectify this problem. Although this was the only instance in which CSE was found by OCSEC not to have complied

with the law, related issues arose periodically, including the incomplete reporting on private communications. OCSEC found this to be the result of human and system error. Many of the observations raised historically by OCSEC centred on the interaction of human and technical elements involved in collection and subsequent reporting activities.

c **Datasets:** In 2016, SIRC reviewed CSIS's use of datasets.[28] These datasets were not collected under the authority of a warrant. The review examined whether the collection of such datasets met the statutory test for collection by CSIS under section 12 of the CSIS Act, which is that information can be collected only to the extent "strictly necessary." Most of the datasets were not directly related to national security threats. SIRC found that there was no comprehensive governance framework guiding the collection, retention and use of bulk datasets. There was also no requirement to assess the datasets to ensure that they met the requirement of being "strictly necessary" to advise the government on suspected threats. These events pushed CSIS to reconsider the legal underpinnings of its collection of datasets. Amendments to the CSIS Act included in the *National Security Act, 2017,* have since provided CSIS with an explicit authority to collect, retain and use datasets containing personal information that is not directly and immediately related to a threat to the security of Canada. As noted in the final SIRC certificate, pending the coming into force of the *National Security Act, 2017*, CSIS continued its dataset program despite the legal risks that had been identified.

43. These examples illustrate how the adoption of new collection technologies also poses a challenge for review bodies, who must equip themselves with the technical expertise needed to ensure that the implications of the technologies being deployed are fully understood. This is particularly important given that the use of many new technologies is a closely guarded secret and thus shielded from public scrutiny. As such, it is largely up to review and oversight bodies to scrutinize the use of these technologies. NSIRA's plans to address this issue are set out in the section on "Future priorities."

Candour

44. CSIS has struggled to overcome an institutional culture of secrecy that has contributed to failures to fully disclose certain activities and information to the Federal Court, to the Minister of Public Safety and Emergency Preparedness, and to review bodies. A lack of candour can be particularly problematic where it intersects with the use of new technology. The difference between collection that is lawful or unlawful often hinges on very specific details regarding the information that the technology will enable CSIS to collect. A key consideration is whether that information will reveal intimate details of the lifestyle and personal choices of an individual. The breadth of the information collected and other details of its use can also affect a technology's level of intrusiveness. It is thus vital that oversight and review bodies are made fully aware of departmental activities in order to fulfil their mandates. The broader the scrutiny of a new technology's use, the more that its implications will be thoroughly considered.

45. Three times in recent years,[29] the Federal Court has found that CSIS failed in its duty of candour toward the Court during warrant applications. In two of the three instances, CSIS omitted certain information regarding the use of technology to collect information. The omissions compromised the Court's ability to properly exercise its judicial control function. Indeed, it is worth noting that the Court is not required to approve CSIS warrants, even if CSIS meets the basic statutory requirements. The Court must also be satisfied that the warrant powers are reasonable in light of all the circumstances, and must therefore be given all the information it needs to make this key assessment. The Court is also permitted to place any conditions on CSIS warrants that it considers to be in the public interest, and must therefore be able to appreciate the privacy implications of new technologies.

46. The Minister of Public Safety and Emergency Preparedness also plays an important role overseeing the activities of CSIS because of his or her statutory responsibilities related to the CSIS warrant process. Before CSIS can submit a warrant application to the Federal Court, the application must first be approved by the Minister. The Minister — and the officials in Public Safety Canada who advise the Minister — must therefore be provided with all relevant information. It is notable that the Minister has felt it necessary to issue ever-more precise and detailed direction to CSIS specifying that the organization must keep the Minister informed of its activities. The most recent example, the 2019 Ministerial Direction for Accountability, specified that CSIS must inform the Minister of activities "where a novel authority, technique, or technology, is used. This includes novel uses of existing authorities, techniques, or technologies."[30]

Human source activities

47. Most recently, CSIS failed to meet its duty of candour to the Court in relation to its human source activities.[31] CSIS sometimes pays human sources to collect intelligence. Often, the access these sources have to valuable information is directly related to their personal involvement in terrorism or other threat activities. In paying these individuals for their information, CSIS runs the risk of violating the laws that prohibit paying any money or providing any other resources that support terrorism or other criminal activity. For years, CSIS relied on the doctrine of Crown immunity to provide a legal justification for its actions and to remain within the ambit of the rule of law. The law in Canada has evolved in recent decades, however, making the use of Crown immunity increasingly tenuous as a justification.

48. In 2015 and 2016, SIRC raised a number of questions regarding the legality of CSIS's human source activities. Notably, SIRC recommended that CSIS obtain legal clarification regarding the continued viability of its reliance on Crown immunity.[32] In response, CSIS obtained legal advice in early 2017 that concluded that Crown immunity could no longer be used to justify activities that would ordinarily be unlawful. This set off a chain of events inside government that culminated in the creation of a new statutory regime allowing CSIS to take actions that would otherwise be unlawful in the course of its human source operations. This new regime

was introduced as part of Bill C-59, the *National Security Act, 2017,* which came into force in mid-2019. While Bill C-59 was before Parliament, however, CSIS decided to continue several human source operations, given their intelligence value, despite the fact that they seemed to violate the law. CSIS only decided to halt these activities in January 2019.

49. In March 2019, SIRC completed its certification of the 2017–18 annual report submitted by the Director of CSIS to the Minister of Public Safety and Emergency Preparedness. Prior to the *National Security Act, 2017,* SIRC was required to certify the lawfulness of the activities described in each of CSIS's reports to the Minister. The 2017–18 report discussed CSIS's continued reliance on Crown immunity in the context of its human source activities. SIRC reviewed the situation and concluded that CSIS had in fact been advised that Crown immunity could no longer be used as a legal defence. As a result, in its certificate, SIRC found that CSIS had knowingly broken the law. SIRC also made clear that although CSIS's operations could have been important from the standpoint of national security, this in no way excused it from adhering to the rule of law. [33]

50. Starting in early 2018, the Federal Court began to question the legal basis of CSIS's human source activities independently of SIRC. These questions led to a series of proceedings that culminated, as mentioned, in the Court finding CSIS to have breached its duty of candour to the Court.[34] Specifically, CSIS did not inform the Court that CSIS's warrant applications were based on intelligence likely collected by illegal means. The Court also observed certain failings with regard to the Department of Justice's role in the situation. The Court recommended that there be a broader, independent review of the systemic, governance and cultural shortcomings and failures at CSIS and the Department of Justice that resulted in CSIS engaging in illegal activity and in the related breach of its duty of candour to the Court.

51. In response to the identified shortcomings, the government referred the matter to NSIRA for review under paragraph 8(1)(c) of the NSIRA Act. This review, conducted both at the request of the Minister and also under NSIRA's autonomous review authority in section 8 of the Act, is now under way.[35] Two members of NSIRA, the Honourable Marie Deschamps, C.C., a former Justice of the Supreme Court of Canada, and Professor Craig Forcese of the Faculty of Law at the University of Ottawa, are jointly leading the review.

52. These events are troubling. CSIS not only broke the law, but CSIS and its legal counsel also failed to disclose important matters to the Federal Court, which they were required to do. CSIS also failed to provide key legal opinions to SIRC, or else provided them many years too late, even though SIRC had a legal right to this information.

Future priorities

53. NSIRA's review mandate has three principal parts: the review of CSIS, the review of CSE, and the review of the national security or intelligence activities of all other federal entities. The review of CSIS and CSE will always remain central to NSIRA's mission, but over the coming years, NSIRA will systematically map and review other departments' collection activities. In so doing, NSIRA will scrutinize collection activities to ensure that they are lawful, reasonable and necessary. In other words, NSIRA will not only consider whether a department can collect information, but also whether it reasonably should do so in light of the department's mandate and the implications for privacy.

54. In our reviews, NSIRA will emphasize scrutiny of a department's or agency's use of technology, and particularly new or emerging technologies that pose the greatest risks. NSIRA's reviews will make recommendations with an eye to improving departmental processes to manage the legal and privacy risks associated with the use of technology. When relevant, NSIRA will examine departmental candour with ministers and oversight bodies, consistent with Canada's broader system of accountability for national security and intelligence.

55. To achieve these goals, NSIRA will invest in building in-house technological expertise, through a combination of hiring technological experts, training and reaching out to the broader technological community. NSIRA will also collaborate with allied accountability bodies through a forum known as the Five Eyes Intelligence Oversight and Review Council (FIORC).[36] NSIRA will seek to stay current with regard to new and emerging technologies, including artificial intelligence, machine learning and quantum computing, and related concerns such as "big data." Our goal is to be able to review departmental use of these technologies and their effects in a timely and effective manner.

56. NSIRA has also worked — and will continue to work — with the Office of the Privacy Commissioner of Canada (OPC) and the National Security and Intelligence Committee of Parliamentarians (NSICOP) on matters of joint concern to ensure that the broadest range of perspectives are brought to bear.

CSIS

57. Over the next year, much of NSIRA's review scrutiny of CSIS will be dedicated to the review stemming from the Federal Court decision discussed above.

58. In addition, NSIRA will systematically map CSIS's use of technology and its warrant powers. NSIRA will then undertake reviews of the technologies and powers that are deemed to pose the greatest risks. In this way, NSIRA will gain knowledge of CSIS's most intrusive activities over time. NSIRA will also increase scrutiny of the warrant process in order to monitor CSIS's candour to the Federal Court.

59. In addition, the *National Security Act, 2017,* gave CSIS a suite of new powers. NSIRA will review CSIS's use of these powers in the coming years so as to help inform Parliament's statutory review of the *National Security Act, 2017*, which will begin in 2022 or 2023. In particular, NSIRA will review CSIS's use of datasets, including those that are publicly available, as well as the new justification regime for CSIS activities, that are undertaken in support of collection, which would otherwise be unlawful. NSIRA is also required each year to review at least one aspect of CSIS's activities under its threat reduction mandate. This mandate authorizes CSIS to go beyond the collection of information in order to take active measures to "reduce" threats to the security of Canada. Over the coming years, NSIRA will take stock of CSIS's use of these powers since they were acquired in 2015.

CSE

60. CSE uses a range of collection powers and technologies in its everyday operations. Over time, NSIRA intends to comprehensively review the full suite of collection techniques in place at CSE. NSIRA will start by focusing on certain collection techniques that are authorized under a ministerial authorization and comparing them to techniques that are authorized through other channels. As well, NSIRA will examine how CSE addresses incidentally intercepted information, especially the information of Canadians or persons in Canada, and how it decides whether to retain the information.

61. The rapid technological evolution in areas such as quantum computing, 5G and artificial intelligence will affect the work of CSE, perhaps more than any other federal entity. These technologies could also result in the collection of new information or the development of new collection techniques. Using our growing technical expertise in these areas, NSIRA will conduct both general and targeted reviews of the use of these technologies.

62. CSE has also received new powers in the *National Security Act, 2017,* including the ability to carry out defensive and offensive cyber operations. CSE cannot use these powers to collect information, separately from authorizations issued under its foreign intelligence or cybersecurity mandates. As CSE begins to conduct these operations, NSIRA will review them to ensure they are not being used for — or do not result in — the collection of information.

Other government departments

63. For entities other than CSIS and CSE, NSIRA's initial reviews will build foundational knowledge of departments with significant collection programs. Of note, NSICOP has already reviewed the security and intelligence activities of the Canada Border Services Agency (CBSA) and of the Department of National Defence (DND) and Canadian Armed Forces (CAF). These reviews identified certain areas of risk, including the use of what is termed "scenario-based targeting," which is used to screen travellers entering the country, as well as the CBSA's use of covert surveillance in Canada.[37] NSIRA will build on NSICOP's work with in-depth reviews of the collection activities of these departments and agencies.

64. NSIRA also intends to map collection through the rest of the federal national security and intelligence apparatus. In particular, NSIRA will explore the collection programs of the RCMP by looking in detail at the RCMP's national security criminal investigation program, and by examining how the RCMP collects intelligence in support of those investigations. Throughout, NSIRA will be mindful of public concerns with respect to law enforcement, and pay due attention to the RCMP's activities in sensitive sectors and to any appearance of bias.

65. Within the next three years, NSIRA will examine the collection activities of Global Affairs Canada (GAC). NSIRA will also map the collection and use of biometrics across the government in relation to its security and intelligence activities. This review will examine the collection and use of biometrics by Immigration, Refugees and Citizenship Canada, the CBSA and Transport Canada in relation to their national security responsibilities and canvass the use of biometrics by CSIS and the RCMP in security intelligence and national security-related police investigations.

66. Among the novel and complex areas of collection that NSIRA will also review is the collection of financial intelligence. Financial intelligence is a core component of national security collection, especially in relation to terrorism. It is also central to large law enforcement intelligence operations, especially those that involve money laundering and terrorist financing. Canada's financial intelligence centre of expertise and responsibility is the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC). NSIRA will review FINTRAC's activities and examine FINTRAC's relationship with domestic partners.

67. Over the course of the next year, NSIRA will also conduct targeted reviews of DND/CAF. NSIRA has already begun to review the Canadian Forces National Counter-Intelligence Unit to determine how this unit conducts its counter-intelligence gathering activities and, in particular, how the unit's activities correspond to legal and governance frameworks by focusing on cases of right-wing extremism. NSIRA will also review the Defence Intelligence Enterprise, to gain a general overview and to learn how it is positioned within DND/CAF governance frameworks and authorities. In light of recent media coverage, this review will focus on medical and open-source intelligence.

Medical intelligence and public health intelligence

68. Given the current COVID-19 pandemic, NSIRA will explore how the Government of Canada collects intelligence on medical issues or in relation to the health of Canadians. This is known as medical intelligence, or public health intelligence. At present, NSIRA does not have a firm understanding of what the government considers to be medical intelligence or the extent to which medical intelligence is used. To rectify this gap, NSIRA will review the Public Health Agency of Canada, as well as DND/CAF, whose American counterpart operates the National Center for Medical Intelligence. In Canada, medical issues are usually not part of the public discourse as to what should or should not constitute the government's intelligence

priorities. Medical intelligence will be a completely new area for NSIRA, and it is hoped that it will provoke a useful conversation in light of current events.

Section III — Safeguarding

69. Safeguarding refers to the protection of people, information and other government assets within the national security and intelligence portfolio. Information collected, analyzed and used within this community is often sensitive, either due to the sources and methods from which it is derived, or because of attendant legal protections. [38]

70. There are real consequences when safeguarding measures fail. Should hostile actors like terrorists or foreign governments gain access to information on human sources, for example, this could put lives at risk. Likewise, if hostile actors learn details on electronic methods of collection, this could lead them to apply countermeasures, which could limit Canadian knowledge on key security and intelligence priorities. There is also reputational risk to the Canadian security and intelligence community if allies perceive that the sensitive information they share with Canada, in trust, is not being adequately protected. It is therefore incumbent on the government to ensure that such information is secured from exploitation, compromise or other unauthorized disclosure.

71. Several security breaches in recent years illustrate that the Canadian national security system has not been immune from the risks associated with "insider threats."[39] The first contemporary public reminder of this risk was the successful prosecution of Jeffrey Delisle. He was a Canadian Navy Sub-Lieutenant who, in 2007, began releasing classified information to the Russian government.[40] On November 30, 2013, Qing Quentin Huang was arrested and charged with attempting to communicate safeguarded information to the Chinese embassy in Ottawa. Mr. Huang had been employed in a sector providing specialized services to the government.[41] Last year, police laid charges against Cameron Ortis, a civilian executive within the RCMP, who was charged with leaking classified information to foreign entities.[42] Both the *Huang* and *Ortis* cases remain before the courts.

Safeguarding policy and legal thresholds

72. Safeguarding is neither a legal term of art nor a precisely defined policy term. It encompasses several distinct elements clustered together due to their impact on the protection of people, information and assets. For this reason, the rules for safeguarding begin with the two main policy instruments that govern the management of security within the Government of Canada: the Policy on Government Security and the Directive on Security Management.[43] These policy instruments outline the various requirements for organizations and employees to contribute to security in the workplace.

73. The Treasury Board Secretariat (TBS) is the lead government agency responsible for setting the minimum standards, or safeguards, used to support these policy instruments, covering:

- information and identity assurance;
- individual security screening;
- physical security;
- information technology security;[44]
- emergency and business continuity management; and
- government contracting.[45]

74. Department- and agency-specific policies and procedures across the security and intelligence community — derived from the TBS standards — also set out additional security requirements.[46] As important as it is to define what safeguarding is, it is equally important to understand what it is not. In this context, safeguarding does not refer to measures directed at persons who do not have access to sensitive government information or assets.[47]

75. Employees in the security and intelligence community are also subject to liability for any violation of the provisions of the *Security of Information Act* (SOIA),[48] which sets out various offences related to the handling of classified material. For instance, the SOIA defines "special operational information" as information that the Government of Canada is taking measures to safeguard.[49]

76. One of the important objectives of the SOIA is to prohibit the unlawful disclosure of sensitive information. However, a mechanism allows for situations where an individual believes that the disclosure of such information is in the public interest — that is, whistleblowing — for example, in preventing public servants from committing a crime in the course of their duties. Whistleblowing protections guard against violations of public trust that erode the confidence of the public in the government's practices. Whistleblowing protections give an individual a potential legitimate defence against prosecution under some offences in the SOIA.[50]

77. Because the stakes can be high for disclosing safeguarded information, the SOIA outlines a series of preconditions that would enable an accused person to avoid criminal liability for such disclosures.[51] If they are met, the Court will perform a balancing exercise to determine whether the disclosure was in the public interest. These preconditions include weighing factors like the extent or risk of harm created by the disclosure and the seriousness of the alleged offence. However, where the accused is alleging an offence has been committed (and except where disclosure of information is necessary to avoid grievous bodily harm or death), the judge may find the public interest favoured disclosure only where the accused first reported the wrongdoing. NSIRA is the final step in this reporting chain.

Safeguarding themes

78. The concept of safeguarding has an impact on NSIRA's work in three crucial ways. First, as discussed above NSIRA has procedures for receiving reporting of wrongdoing by whistleblowers. Second, NSIRA must ensure that our members, employees and systems safeguard sensitive information, assets and people from compromise. Third, in both our review and complaint investigation activities, NSIRA plays a crucial role in assessing if the governance systems used to deter, detect and mitigate such risks are compliant, reasonable and necessary.

79. NSIRA has prioritized safeguarding as a review theme to be examined yearly. In selecting this as a review priority, we will help determine the extent to which the security and intelligence community is appropriately safeguarding its employees, information and assets, and will report on whether such practices are lawful, reasonable and necessary to reduce the identified risks. To this end, in our first year NSIRA completed one safeguarding review relating to CSIS, and started another within DND. The latter review was ongoing at the time of writing. When these two reviews are considered holistically along with available open-source information, broader observations can be made about safeguarding.

80. A key observation is the importance of maintaining security vigilance. Currently, the security system engages in high-intensity scrutiny at predetermined intervals — e.g., initial screening on hiring, five-year updates to security clearances, yearly employee security awareness week — and then periods between these intervals where security is less prominent. Moreover, if other priorities take precedence, the time between intervals could increase. In the case of Mr. Delisle, for instance, his Top Secret security clearance had lapsed and was not properly updated prior to his arrival at the government facility where he committed his crimes. Had proper clearance renewal standards been followed, his loyalty to Canada would have been assessed and other vulnerabilities scrutinized.[52]

81. Another important observation is the essential role of clear, concise and updated policies in setting standards across the government. As already mentioned, TBS establishes the minimum security standards for government departments and agencies to follow. Gaps in these standards could create a domino effect, with each department and agency creating their own policies and procedures. Such gaps could lead not only to an absence of standardization across government, but also, in certain cases, to the unreasonable and unnecessary application of security practices.

The polygraph

82. A final observation relates to the government's use of the polygraph for screening security and intelligence employees. Commonly referred to as a lie detector test, the polygraph is a technology that measures and records several physiological indicators such as blood pressure, pulse, respiration and skin conductivity while

a person responds to a number of questions. “Deceptive” answers produce physiological responses that can, so it is alleged, be differentiated from those associated with “non-deceptive” answers.

83. The TBS Standard on Security Screening, created in 2014, cites the use of the polygraph as an appropriate tool, among others, for assessing candidates seeking an Enhanced Top Secret (ETS) clearance. CSIS, in conducting security assessments for its staff, uses the results of the polygraph as a determinative element when granting ETS clearances, rather than an instructive element, to be considered as part of a series of relevant factors.[53] If an outside candidate, employee or individual contracting with the Government of Canada is denied a security clearance that is necessary to obtain or keep federal employment or a contract, the individual can make a complaint to NSIRA pursuant to section 18 of the NSIRA Act. If NSIRA’s jurisdiction is established, the complaint would be investigated by an NSIRA member. This could include, for example, a complaint where a CSIS employee was terminated solely because of the revocation of a security clearance, and the Deputy Head of CSIS could have based the decision to revoke the clearance on the results of a polygraph test. Given the highly invasive and controversial nature of this technology, NSIRA decided to examine the use of the polygraph within our latest safeguarding review of CSIS. We sought to determine the justifications for its use, and the extent to which such determinations are reasonable and necessary.

84. Several key observations were derived from this analysis. First, this tool can have profound negative impacts on an employee’s mental health if not used appropriately. Second, CSIS was unable justify the merits of examiners — who are not medical practitioners — to ask medical-related questions of the people they examine. Third, the outcomes or consequences for polygraph exams conducted on external applicants compared with CSIS employees differed. [Text removed - As of November 20, 2020, NSIRA and CSIS could not agree on how all of the facts of this review should be presented in an unclassified, public document]. Essentially, a successful polygraph is a determinative factor for external applicants in obtaining an ETS clearance through CSIS. Fourth, CSIS requires policy clarity for cases where employees fail the polygraph examination. Finally, CSIS did not conduct a privacy impact assessment (PIA) for the use of the polygraph, despite a PIA being required by government policy when a department or agency is dealing with “personal information.”[54]

85. These issues raised in the CSIS context are related to a much broader consideration: namely, the extent to which the government’s overarching policy document, the Standard on Security Screening,[55] provides adequate guidance for departments and agencies when they implement this safeguarding measure. For example, this standard requires the use of the polygraph for all ETS clearances, but it is silent on any guidance on the implementation of this requirement, including the conditions for the reasonable use of the polygraph. Rather, such key considerations are left to the discretion of specific departments and agencies.

86. The OPC has also raised concerns with TBS as to how the polygraph examination is used as an enhanced screening requirement under the 2014 Standard on Security Screening. In July 2017 correspondence, for example, the OPC noted particular concerns surrounding its effectiveness, sensitivity and privacy implications, and the potential adverse consequences associated with polygraph examinations.[56]

87. These contemporary observations are not new. In seven consecutive annual reports, ranging from 1985–86 to 1991–92, SIRC requested that CSIS stop using the polygraph. One of the key concerns raised by successive committees were SIRC's "grave doubts" about the use of the technology, pointing to the fact that test results could be wrong 10% of the time or more.[57] As well, Canadian courts have refused to admit the results of a polygraph as evidence in criminal trials. The Supreme Court of Canada has found that they are unreliable and risky, and would not assist the Court in determining a person's guilt or innocence.[58]

88. After consideration of the foregoing, on December 12, 2019, NSIRA sent a letter to TBS seeking access to the legal advice prepared for Treasury Board on how the polygraph complies with Canadian legal requirements, as well as a summary of the evidentiary basis used to establish the requirement for using the polygraph, and any assessments of how the use of the polygraph achieves its intended goal. The TBS response failed to answer NSIRA's questions. However, the letter did acknowledge that the next round of security policy modifications was under way.

89. When SIRC recommended in 1985 that CSIS should cease using the polygraph, it was meant to allow the government time to reach definitive conclusions about whether this technique should be employed by Canadian agencies and, if so, under what circumstances and under what rules. SIRC requested what sound government policy instruments should always require: namely, that there are consistent approaches across government; that risks are managed; and that policies exhibit public service values such as probity, prudence, equity and transparency. NSIRA has not been provided with evidence that suggests that the use of the polygraph meets all of these policy requirements. To this end, future reviews will examine the polygraph's use outside of CSIS, and based on the information assessed, NSIRA will make a definitive determination about the legality and utility of this instrument.

Future review priorities

90. NSIRA will conduct several reviews of safeguarding practices in the coming years, in an effort to ensure that we are covering as broad a spectrum as possible of security and intelligence community actors. These safeguarding reviews will allow NSIRA to remain involved in relevant key priorities of the field, such as legality, privacy, science-based tools and international best practices.

91. As an independent agency charged with assessing propriety and legality at the core of our mandate, we make our own assessment of the lawfulness of the actions of the security and intelligence community. This forms the basis for NSIRA findings, recommendations and reporting. To this end, NSIRA intends to maintain a strong focus on assessing the process for the input of expert legal advice. Within the context of specific reviews, NSIRA will review the Department of Justice's role in providing legal analysis to security and intelligence stakeholders.

92. Considering the primacy of privacy in much of the information collected and used by the government in this field, another priority is the need to evaluate the government's respect for privacy rights, regardless of the policy merits of the safeguarding measure. One of NSIRA's fellow accountability organizations, the OPC, plays a key role in helping ensure government compliance with Canadian privacy legislation.[59] NSIRA will continue to work collaboratively with the OPC on future safeguarding reviews.

93. In keeping with NSIRA's mandate to assess the reasonableness and necessity of a department's exercise of its powers, NSIRA intends to go beyond assessing whether safeguarding measures are legally sound and privacy compliant. NSIRA's mandate includes reviewing for necessity and reasonableness. For any government to continue to build an adaptive security system, scientific evidence and data-driven analysis must inform which safeguarding tools and processes are necessary. Currently, NSIRA is concerned that there is an absence of transparent and defensible science underpinning policy decisions for selecting security measures. Therefore, our future reviews will include the examination of scientific justifications for specific safeguarding measures.

94. Finally, NSIRA will assess the potential for the government to further advance collaborative practices through additional outreach with foreign partners in allied countries. Although it is known that exchanges of this nature are routine within certain sectors of the security and intelligence community, another feature of these exchanges that should be examined is the extent to which these outreach and coordination efforts relate to safeguarding measures and the extent to which they help revitalize the government's security posture. NSIRA's reviews will also provide insight into this component of international best practices.

95. Five safeguarding reviews are planned over the coming years to ensure coverage of as broad a spectrum as possible of security and intelligence community actors. The first will address an aspect of security screening within GAC. The second safeguarding review will relate to CSE's use of the polygraph for employee security screening; this will be in addition to the yearly reviews of CSE that routinely cover various cybersecurity initiatives used to protect government systems from exploitation. The third review will consider the use of biometrics across the Canadian government. The final two reviews will examine aspects of the RCMP (i.e., the division devoted to Operations Research within this police force, while the other will evaluate the security/safeguarding implications of the *Ortis* case, using the RCMP's own internal reviews as a starting point for our analysis).

96. This series of reviews relating to safeguarding will help to provide Parliament and all Canadians with facts about the adequacy of security practices within the security and intelligence community, and ideally, help improve such safeguarding measures. Most importantly, NSIRA exists to ensure that whatever government security standards are ultimately created, they are tested through expert scrutiny and their application is reported on to encourage sustained public debate.

Section IV — Sharing

97. Departments and agencies complement the information they collect on their own with robust information sharing both domestically and internationally. Counter-terrorism, in particular, requires an integrated response, one that involves multiple departments and agencies, in Canada and internationally. Indeed, this is one of the lessons that has been learned post-9/11, but it comes with its own risks and a concomitant need for caution.

98. Information sharing in the security and intelligence community, however, is a broader issue than sharing information to prevent acts of terrorism. Departments share not only to prevent acts of terrorism, but also to counter espionage, foreign interference and the proliferation of restricted technologies. They also share information to advance Canada's foreign policy and defence priorities. Moreover, they share information broadly — within the security and intelligence community; outside that community with other federal, provincial, municipal and private sector organizations; and with foreign partners.

99. Equally noteworthy is the impact of technology on information sharing. Departments are able not only to collect vast amounts of information, but also to share that information more quickly and easily than ever before. And the burgeoning field of data analytics encourages the sharing of information that can then be analyzed.

100. Against this backdrop, information sharing raises issues of privacy and potential mistreatment abroad, as well as the need to protect sensitive sources and methods when information is shared. These are important issues for Canadians and for policy-makers, and so they will be for NSIRA as well in our review work.

Legal framework for sharing

101. A complex legal framework governs departments' information sharing. The *Privacy Act* is an overarching piece of legislation; it is not limited to issues pertaining to the sharing of personal information for national security purposes. The Act sets out specific rules regarding when and why federal government agencies are permitted to share personal information. More recently, Parliament also enacted the *Security of Canada Information Disclosure Act* (SCIDA),[60] discussed below.

102. In addition, agencies such as CSE, CSIS and the RCMP are subject to specific provisions in their governing statutes for sharing information. Departments can also share information for specific purposes under specific legislation. For example, under the *Customs Act,* CBSA officials can share customs information where that information is reasonably regarded by the official to be information relating to the national security or defence of Canada. Likewise, in certain circumstances, FINTRAC and law enforcement bodies receive and disclose financial information pursuant to the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act.*

103. Departments' information sharing can also be shaped by international agreements and resolutions, as well as guidance from their respective ministers.

Information-sharing challenges

104. On the basis of three commissions of inquiry in the past 15 years[61] — as well as numerous reviews by NSIRA's predecessors OCSEC and SIRC[62] — we can safely say that the key challenges of sharing information for national security purposes domestically and internationally are well documented.

105. Justice Major's Commission of Inquiry into the bombing of Air India Flight 182[63] addressed several questions, including whether there was effective cooperation and sharing of information between CSIS and the RCMP. Ultimately, the inquiry concluded that the failure of domestic agencies to share information effectively contributed in a material way to the tragic downing of the Air India flight.

106. Since then, CSIS and the RCMP have taken steps to strengthen their information sharing and cooperation. The objective of a CSIS national security investigation is to provide security intelligence to the government; the RCMP collects evidence to be used in a judicial process. While collecting for these different purposes, the two agencies have a shared interest in protecting their respective sources and investigative techniques.

107. In national security investigations, intelligence agencies — most notably CSIS — can be reluctant to share information with the police. Police themselves might want to maintain a distance from intelligence information because it could eventually be subject to disclosure; disclosure disputes can delay or disrupt criminal prosecutions. From a public safety perspective, the limited sharing between intelligence and police agencies could be harmful. This was Justice Major's central conclusion. It can complicate coordination and impede or delay the range of public safety actions available to the government. This is known as the "intelligence to evidence" dilemma.

108. To address this issue, CSIS and the RCMP have developed a One Vision framework. The framework seeks to enhance cooperation and streamline information sharing.

109. The intelligence to evidence issue was a key part of the country-wide national security consultations that the government undertook in 2016.[64] Ultimately, the government did not bring forward any legislative amendments to specifically address this issue. During our first year, however, NSIRA heard from an external expert that CSIS and the RCMP continue to wrestle with this challenge. The two organizations are undertaking a thorough review to find ways they can remove unnecessary impediments to information sharing and facilitate successful enforcement. Given the importance of the CSIS-RCMP relationship, NSIRA has launched an in-depth case study, to be completed later in 2020, that examines this relationship.

Clear authority for sharing

110. Historically, departments wanting to share national security information regarding threats to Canadian citizens and interests have been concerned about the lack of an independent authority to do so. The *Privacy Act*'s "consistent use" provision can be used in the national security context where there is a reasonable and direct connection to the original purpose for which the information was obtained. However, this legislation is not specific to the national security context.[65] Overall, it was believed that the complexity of the legal landscape was impeding the sharing of information with national security and intelligence agencies.

111. In response, the government passed the *Security of Canada Information Sharing Act* (SCISA) in 2015. It created a single legislative authority for federal government institutions to disclose information on an activity that "undermines the security of Canada." The intent in doing so was to improve the effectiveness and timeliness of sharing threat-related information, including by departments and agencies that are outside the core security and intelligence community. In separate reviews of disclosures under SCISA, however, both SIRC[66] and the OPC[67] were critical of departments' internal controls and record keeping.

112. The legislation was amended and renamed SCIDA as part of the *National Security Act, 2017.* Further, NSIRA now has a statutory requirement, pursuant to subsection 39(1) of the NSIRA Act, to conduct a review of disclosures made under SCIDA. To ensure robust review of these disclosures, and in keeping with the statutory authority to coordinate to avoid unnecessary duplication of work, NSIRA and the OPC have agreed to work together on these review efforts.

113. NSIRA is also looking beyond SCIDA to other aspects of the challenge of having clear authority to share information for national security purposes. In our first year, NSIRA has elected to conduct three reviews that feature CSE's incidental collection and use of Canadian identity information, including disclosure of such information to departments. When sharing intelligence reports with

other departments and agencies, CSE typically suppresses Canadian identity information, which is collected incidentally in the course of its foreign intelligence activities and its cybersecurity and information assurance activities. However, departments and agencies that can demonstrate they have the legal authority and operational justification to receive the Canadian identity information can submit to CSE a request for disclosure of the information. NSIRA expects to complete a review later in 2020 that focuses on the lawfulness and appropriateness of Canadian identity information disclosures, and a review that focuses on CSE's ministerial authorizations and ministerial orders.

SCIDA INFORMATION SHARING SCHEME

BEFORE DISCLOSURE

GC institution requests information from another GC institution. The recipient institution must be listed in schedule 3 of the Act.

GC institution, on its own initiative, decides to disclose to a GC institution listed in schedule 3 of the Act.

The information that the GC institution is expected to share is in respect of activities that undermine the security of Canada as defined in s.2 of the Act.

DISCLOSURE TEST

The disclosing institution must be satisfied that:

a) the disclosure will contribute to the exercise of the recipient institution's jurisdiction, or the carrying out of its responsibilities, under an Act of Parliament or another lawful authority; and

b) the disclosure will not affect any person's privacy interest more than it is reasonably necessary in the circumstances.

(paragraphs 5(1)(a) and 5(1)(b)).

OTHER REQUIREMENTS

Copy to NSIRA
In relation to the record keeping requirement, a copy of every record of disclosure shared or received must be provided every year to NSIRA. (subsec. 9(3))

Destroy or return
The receiver must, as soon as feasible after receiving disclosure, destroy or return any personal information that is not necessary for the institution to exercise its jurisdiction, or to carry out its responsibilities, under an Act or Parliament or another lawful authority, in respect of activities that undermine the security of Canada. (subsec. 5.1 (1))

(continued)

Accuracy and reliability
GC institution that discloses information under subsection (1) must, at the time of the disclosure, also provide information regarding its accuracy and the reliability of the manner in which it was obtained. (subsec. 5(2))

Recordkeeping
GC institution must, as soon as feasible after receiving it under section 5, destroy or return any personal information, as defined in section 3 of the *Privacy Act*, that is not necessary for the institution to exercise its jurisdiction, or to carry out its responsibilities, under an Act of Parliament or another lawful authority, in respect of activities that undermine the security of Canada (subsec. 5.1(1)) unless otherwise required by law. (subsec. 5.1(2))

CSIS - Exception
Recordkeeping requirement does not apply to CSIS in respect of any information that relates to the performance of its duties and functions under s. 12 of the CSIS Act. (subsec. 5.1(3))

Review of CSE's Privacy Incidents File

114. One review featuring Canadian identity information was NSIRA's first completed review relating to CSE. The review examines CSE's Privacy Incidents File, which records privacy incidents discovered by CSE. 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. The review of the Privacy Incidents File was an annual review conducted by OCSEC, CSE's former independent review body. For this review, based on an examination of a selected sample of incidents reported in the Privacy Incidents File for the period of July 1, 2018, to July 31, 2019, NSIRA commended CSE's timely response to reporting and mitigating privacy incidents. However, NSIRA made five additional findings and corresponding recommendations for CSE to improve its documentation, mitigation and privacy protection practices.

Sharing with international partners and the risk of mistreatment

115. Justice O'Connor's inquiry into the actions of Canadian officials in relation to Maher Arar examined the circumstances under which a Canadian citizen, Maher Arar, was rendered to Syria and tortured. A key outcome of the inquiry was its conclusion that sharing inaccurate or non-caveated[68] information with foreign partners can result in the mistreatment and torture of individuals, as it did with Mr. Arar.

116. The government responded by issuing a series of ministerial directions on information sharing with foreign partners, culminating in the *Avoiding Complicity in Mistreatment by Foreign Entities Act* (Complicity Avoidance Act), which came into force in 2019 and required written direction be issued by the Governor in Council (GIC) to the deputy head of multiple departments and agencies. The GIC directions have codified the expectations of departments and agencies. In particular, there is now a clear prohibition for any sharing of information that would result in a substantial risk of mistreatment of an individual. Additionally, they limit the use of any information that was likely obtained through the mistreatment of an individual.

117. Throughout its history, SIRC paid careful attention to CSIS's information-sharing practices with foreign partners. It also specifically addressed the operationalization of the relevant ministerial direction. Its attention to these issues continued through 2018–19, through two separate reviews of CSIS foreign stations. The first of these reviews focused on the need for CSIS to institute and follow a rigorous decision-making process with respect to sharing information with foreign partners, supported by foreign arrangements anchored in thorough assessments of the human rights records of Canada's foreign partners.

118. The second foreign station review also examined CSIS's relationships with foreign partners within the geographic region encompassed by the station. In this case, all of the foreign partners are deemed high risk from a human rights perspective and, thus, restrictions have been placed on all foreign arrangements in the station's area of responsibility.

119. One of NSIRA's first reviews examined changes to CSIS's procedures and policies on information sharing by means of a detailed examination of three cases,

identified as high risk, that had been reviewed by CSIS's Information Sharing Evaluation Committee.[69] The review yielded two recommendations meant to ensure that decisions are made at a level commensurate with the assessment of risk, and that legal opinions are sought, as appropriate, to ensure compliance with the law and ministerial directions when sharing information with a foreign entity.

120. As part of our governing statute, NSIRA is now required to review departments' implementation of GIC directions on information sharing with foreign partners under the Complicity Avoidance Act. To date, the GIC has issued these directions to 12 departments, including several that have never before received formal direction specific to information sharing with foreign partners.[70]

121. To prepare for this new responsibility, NSIRA launched our first interagency review, an assessment of how six departments and agencies— the CBSA, CSE, CSIS, DND, GAC and the RCMP — were implementing the 2017 Ministerial Direction on Avoiding Complicity in Mistreatment by Foreign Entities, which was the basis of the direction under the Complicity Avoidance Act. The purpose of the review was also to provide a future roadmap for departments that, pursuant to the Complicity Avoidance Act, received this direction for the first time in 2019.

122. NSIRA found significant variation among the six departments and agencies in terms of their success in implementing the 2017 ministerial direction. Some, like CSE, have developed and rolled out comprehensive policy suites to guide their information sharing with foreign partners. Some departments face challenges in operationalizing this direction. Some also face challenges in establishing decision-making mechanisms that are independent from the operational front line in cases where there is a risk of mistreatment. One of the key issues that NSIRA's review identified was the inconsistent application of the "substantial risk" threshold across departments and agencies. This will be an area of inquiry in the future.

Future priorities

123. NSIRA has a specific statutory requirement to review the implementation of GIC direction under the Complicity Avoidance Act, and to review disclosures under SCIDA. These reviews are annual requirements, reflecting the potential risks to Canadians when departments and agencies share under these respective statutory mandates. NSIRA will be attentive to those risks, including the potential risks to privacy posed by information sharing. At the same time, however, NSIRA intends to map and review the full range of information sharing in which departments engage — under different statutes and legal sources, as well as internationally and with one another, provincial and territorial agencies, and the private sector.

124. Over our first three years, NSIRA will begin to explore information sharing across the security and intelligence community. We will focus on key partnerships, and how departments and agencies collaborate in keeping Canadians safe

and achieving Canada's foreign policy and defence objectives. The scope of information sharing is broad, and NSIRA hopes to build our understanding of this issue over time.

125. NSIRA has begun a building block review of CSIS-RCMP collaboration and information sharing in relation to a particular investigation. One of the objectives of this review is to document the challenges that the two agencies face in relation to the intelligence to evidence dilemma.

126. NSIRA will examine other key partnerships within the security and intelligence community, including information sharing between CSIS and CBSA to prevent people or goods posing a threat to national security from crossing the border. We will also examine how CSE and CSIS collaborate to collect foreign intelligence that is useful for Canadian policy-makers.

127. NSIRA will also look at horizontal arrangements, and information sharing across different levels of government. For example, we will assess institutionalized measures to promote sharing and cooperation, such as in relation to Integrated National Security Enforcement Team investigations. These teams are led by the RCMP and include representatives from other federal agencies, as well as representatives from municipal police services and provincial police in the case of Ontario and Quebec. NSIRA will also look at information sharing outside of the counter-terrorism context, including how departments and agencies protect Canada's economic security, beginning with actions under the *Investment Canada Act* and extending to include the full spectrum of tools at the government's disposal.

128. NSIRA will examine information sharing with private sector organizations, such as information that the Canadian Centre for Cyber Security collects from organizations to prevent or mitigate cyber attacks by hostile state actors,[71] or that chartered banks report to FINTRAC for investigating suspicious financial transactions.

129. Finally, NSIRA recognizes that in examining information sharing with foreign partners, we can see and understand only Canadian actions. NSIRA therefore participates in international fora such as FIORC, which brings together review bodies from Canada, Australia, New Zealand, the United Kingdom and the United States to stay up to date with (unclassified) trends internationally and to share best practices. Given the close relationship that exists among the Five Eyes intelligence agencies, information sharing has been a topic of discussion at FIORC. These discussions are one way for NSIRA to address the potential gap in accountability that exists with respect to international cooperation.

130. In sum, cooperation and information sharing among members of Canada's security and intelligence community have always been essential features of Canada's national security efforts. In practice, this means that there will be very little of NSIRA's review work that will not include attention to information sharing in some form or another. NSIRA will be attentive to the risks of sharing, as well as the need for effective and timely sharing.

Section V
— Action

131. "Actions" refer to any activities undertaken by a federal government department or agency to influence an outcome relating to national security or intelligence. Actions can also come as a result of intelligence collection and/or intelligence sharing. Intelligence is one aspect of the information and analysis that shape how actions are construed and implemented. The action itself, and the influence of intelligence, can be visible (overt) or invisible (covert) to Canadians. A visible action would eventually be known to the recipient, while the occurrence of an invisible action might never be known.

132. The former review bodies, SIRC and OCSEC, could conduct only agency-specific reviews of the key "collectors": CSIS and CSE. Their reviews of national security activities tended to focus on collection, safeguarding and information sharing. This briefly changed when Parliament enacted the *Anti-terrorism Act, 2015*, and SIRC began to undertake reviews of CSIS's new mandate to reduce threats to the security of Canada. SIRC provided the only after-the-fact review of these extraordinary new powers. However, SIRC's reviews remained confined to CSIS's actions — a narrow subset of the broad array of national security-related actions taken every day across Canada's security and intelligence community.

133. NSIRA's mandate goes beyond intelligence and its collectors, extending to any national security-related activity of any department or agency. Our statutory authorities equip us with the power to review the full range of "action" activities. Such activities have rarely been subject to any form of independent review, and NSIRA is able to ensure that they now are.

134. The *National Security Act, 2017*, established clear mandates for the main intelligence collectors subject to review, CSIS and CSE, to act in certain circumstances against perceived national security threats. For CSIS, this new legislation updated its threat reduction mandate. For CSE, the Act established active cyber operations (ACO) and defensive cyber operations (DCO) as aspects of its mandate. These new authorities merely supplement the many existing authorities that enable over a dozen other federal security and intelligence departments and agencies to take actions relating to national security, making the "action" cluster of activities vast. For instance, actions within the security and intelligence community include the interception of people and goods at the border by the CBSA and criminal arrest (including, potentially, preventive detention) by the RCMP.

135. The range of actions within NSIRA's mandate to review "any activity carried out by a department that relates to national security or intelligence" is broad, and includes such actions as denying a person entry into Canada, revoking a Canadian's passport, placing a person on the *Secure Air Travel Act* list (Canada's "No Fly List"), disrupting a person's affairs through a threat reduction measure, detaining an alleged terrorist or carrying out military actions in an armed conflict. Sometimes, a high-level strategic decision can also be an action activity, such as a policy choice on a national priority like securing the Arctic.

136. NSIRA's reviews in this area overlap with other priority subject areas. We can review national security action activities that stem from intelligence collection, national security actions unrelated to intelligence collection, and national security actions that lead to intelligence collection. As an example of this last category, a CAF tactical raid during an overseas mission could yield new sources of intelligence that might then seed an NSIRA review in that area.

137. Due to the largely secretive nature of national security and intelligence actions, the effects and impacts are often unseen by the larger public. NSIRA is acutely conscious of concerns expressed during our outreach to civil society with how actions of the security and intelligence agencies might affect the lives of Canadians. This amplifies earlier concerns, primarily centred on privacy issues stemming from information collection and sharing. As a result, one of our key tenets is, to the extent possible, to bring transparency and accountability to our reviews of the actions of the security and intelligence community.

Past review observations

138. As mentioned, before the *National Security Act, 2017,* reviews did not typically extend to the realm of action activities. For this reason, NSIRA has only a modest archive of domestic review materials from which to extrapolate themes in action reviews. NSIRA's current focus is to build on foundational reviews to derive key themes. This report discusses NSIRA's approach to future review in the next section. Nevertheless, some themes have emerged from past reviews of CSIS's threat reduction measures (TRMs) — which were the only action activities reviewed in the past.[72]

139. From the introduction of its TRM mandate in 2015 to August 2020, CSIS has not sought a warrant from the Federal Court for TRM activities. When introduced, TRM powers raised legal questions and potential issues related to the Charter. The *National Security Act, 2017*, addressed many of these ambiguities, and enacted new provisions that strengthened Charter protections. NSIRA will closely monitor CSIS's use of TRMs and review its assessments of when warrants are required for TRMs. NSIRA will also be attentive to how CSIS executes any TRM conducted under the authority of a warrant — and pay close attention to the extent of CSIS's compliance with all court directions and conditions.

Action activities by the numbers

2018 and 2019 CSIS TRM warrants under section 12.1/21.1 of the CSIS Act	
TRM warrant applications granted:	**0**
TRM warrant applications denied:	**0**

2019 CSE ACO/DCO ministerial authorizations issued under the following subsections of the CSE Act	
subsection 29(1), defensive cyber operations:	**x**
subsection 30(1), active cyber operations:	**x**

CSE has confirmed that, in 2019, ministerial authorizations were signed under each subsection listed in this table. However, CSE is of the view that releasing the specific numbers would be injurious to national security. NSIRA disagrees with this view. As of November 20, 2020, this issue could not be resolved. NSIRA will continue to work with CSE with a view to finding a compromise.

CSE

140. Other themes arising in our review of action activities stem from the widespread commentary within civil society relating to CSE's new powers to conduct ACOs and DCOs. Prior to the *National Security Act, 2017,* CSE's mandates limited the organization (primarily) to observation and collection. Now, under its ACO/DCO mandates, CSE can direct actions through the global information infrastructure at the activities of foreign individuals or foreign entities outside Canada. CSE can conduct ACO activities on or through the global information infrastructure to degrade, disrupt, influence, respond to or interfere with the capabilities or activities of entities as they relate to international affairs, defence or security. CSE can conduct DCO activities on or through the global information infrastructure to help protect the electronic information and information infrastructures of federal institutions or those designated as being important to the Government of Canada. These powers have equivalents among those available to Five Eyes partners. They also empower CSE to play a significant, but unprecedented, role in national security action activities.

141. Civil liberties groups have identified ACO/DCO activities as a principal concern with the *National Security Act, 2017,* and point specifically to the absence of independent oversight (that is, pre-authorization) of these activities. Under the current statutory regime, in order for CSE to lawfully conduct ACO/DCO, the Minister of National Defence must authorize all such activities. This authorization requires the Minister to conclude that there are reasonable grounds to believe that the activity is reasonable and proportionate, having regard to the nature of the objective to be achieved and the nature of the activities. Additionally, the Minister of Foreign Affairs must approve ACO activities and must be consulted on DCO activities.[73]

142. Ministerial authorizations for ACO/DCO activities do not require the approval of the Intelligence Commissioner, which is not the case for foreign intelligence and cybersecurity activities.[74] There is, therefore, no scrutiny by an arm's-length, independent body of ACO/DCO authorizations prior to their approval. This is why NSIRA considers our reviews of ACO/DCO actions to be particularly important. Unlike in the case of CSIS TRMs, CSE has no statutory obligation to notify NSIRA when it undertakes ACO/DCO activities. NSIRA intends, however, to focus proactively on these activities.

143. Although legislation limits powers such as TRMs and ACO/DCO, these activities occur in secret. This is in contrast with other types of national security actions, such as arrests made by police, which are overt and can be challenged in open court. NSIRA considers the opacity of certain types of actions to warrant future reviews. The more secret the national security action, the more essential it is for NSIRA to conduct rigorous review.

Law enforcement

144. Prior to the enactment of the *National Security Act, 2017*, the RCMP's national security-related activities were reviewed by the Civilian Review and Complaints Commission for the RCMP.[75] Those national security-related actions are now reviewed by NSIRA. The enactment of new offences — especially terrorism offences — and a focus on terrorism have drawn police into a greater national security role. Police investigate crime, and have a role in preventing its occurrence. In doing so, police might investigate, among other things, terrorism offences, while at the same time being involved in community-based programs directed at countering radicalization to violence. They can also engage in crime prevention or risk mitigation actions that do not lead to full prosecutions. The traditional tool for holding police accountable is the criminal justice system. For example, police conduct will be scrutinized during a criminal trial. However, accountability mechanisms are less robust where police pursue national security threat disruption strategies that are not challenged in the courts. Therefore, we believe that NSIRA's review functions will become particularly important in these circumstances.[76]

145. The CBSA's scrutiny of people and goods crossing the border can be triggered by intelligence shared from domestic and foreign partners or derived from its own collection and assessment efforts. CBSA actions include searches at the border and the seizure or interdiction of goods, currency and people. These searches and the CBSA's determination that a non-Canadian might be inadmissible can have implications for people's liberty, privacy, freedom of movement and commercial interests. NSIRA's task is to review the CBSA's national security and intelligence activities in an effort, among other things, to ensure that it fully complies with its legal requirements. This is especially true as, at present, no independent body currently can hear public complaints against the CBSA.

Future priorities

146. In our reviews of action activities, NSIRA makes findings and recommendations on an organization's compliance with the law and any applicable ministerial direction and the reasonableness and necessity of its exercise of its powers. NSIRA is in a unique position to assess the Government of Canada's visible or invisible actions and to provide assurance to Canadians that their national security and intelligence agencies are accountable in order to protect Canada's national security interests and defend the rights and freedoms of Canadians and people residing in Canada.

147. NSIRA's strategic plan focuses on reviewing three types of action activities: operational actions, law enforcement actions and administrative actions, defined below.[77] In each of the following categories, NSIRA has identified certain action activities of interest that we will scrutinize in future reviews. The items listed are not necessarily part of NSIRA's review plan but serve to highlight the breadth of situations that fall within reviews of the "action" activities undertaken by the security and intelligence community.

- *Operational:* covert action activities in direct support of a national security objective. Operational actions of interest to NSIRA include: CSE's use of ACO/DCO, to be reviewed annually; CSIS TRMs, to be reviewed annually; and CAF's operations in theatre and on the battlefield.

- *Law enforcement:* covert or overt action activities to enforce laws, investigate crimes and make arrests. Law enforcement action activities on which NSIRA might concentrate, while being sensitive to the administration of justice and the concept of police independence in investigative decisions, include the CBSA's targeting that leads to the identification and/or interception of high-risk people, goods and conveyances that pose a threat to the security of Canadians, and RCMP investigations that could lead to detention, arrest or prosecution.

- *Administrative:* visible action activities taken in the act or process of administering a statutory power entrusted by Parliament to the federal government. Administrative action activities on which NSIRA might focus include: GAC's implementation of foreign policy and trade sanctions; the *Investment Canada Act* reviews of investments that could be injurious to national security; the decision to add a person to the *Secure Air Travel Act* list under the Passenger Protect Program; and national security-related admissibility issues.

148. As NSIRA's capacity to conduct reviews expands, we will compile a complete picture of the actions that national security and intelligence agencies take in exercising their mandates, and assess these actions for legal compliance, reasonableness and necessity.

Complaints

Section I
— NSIRA's complaints investigation mandate



03

Under the NSIRA Act, one of NSIRA's core functions is to investigate complaints in the following instances:

- complaints with respect to an activity carried out by the Canadian Security Intelligence Service (CSIS) or the Communications Security Establishment (CSE);
- complaints referred by the Civilian Review and Complaints Commission for the RCMP (CRCC) with respect to an activity by the Royal Canadian Mounted Police (RCMP) that is closely related to national security; and
- complaints regarding the denial or revocation of security clearances to federal government employees and contractors.[78]



150. Through the *National Security Act, 2017*, NSIRA inherited the complaints functions of the Security Intelligence Review Committee (SIRC) and the Office of the CSE Commissioner, which investigated complaints related to CSIS and CSE, respectively. In addition, NSIRA absorbed responsibility for investigating national security-related complaints against the RCMP. NSIRA also inherited SIRC's complaints investigation infrastructure, but it was evident early in our mandate that the SIRC model needed to be enhanced to provide more timely and efficient investigations. NSIRA has therefore begun to rework the Rules of Procedure and enhance the overall process. NSIRA has also worked collaboratively with the RCMP and the CRCC to effectively manage national security-related complaints against the RCMP.[79]

Section II — Synopsis of trends and key themes

151. NSIRA has experienced an increase in the volume of complaints we receive, specifically complaints against CSIS, as well as complaints relating to security clearances. In comparison to the complaints statistics in the SIRC annual report for 2017–18 and statistics for 2018–19, NSIRA has seen an increase of 40% for newly opened complaint files. In particular, complaints against CSIS have doubled and security clearance complaints have increased by 30%.[80] NSIRA did not investigate most of the recent complaints against CSIS because we concluded that they were not in NSIRA's jurisdiction — they did not concern an activity carried out by CSIS, or NSIRA was satisfied that the complaints were trivial, frivolous or made in bad faith.[81]

152. The majority of the complaints received relating to the alleged denial or revocation of a security clearance did not fall within NSIRA's mandate. Rather, it turned out they were related to a complainant's reliability status or enhanced reliability status. NSIRA may only investigate complaints relating to security clearances, not reliability status matters. Complaints relating to reliability status generally must be challenged on judicial review in the Federal Court. As a result, NSIRA investigated very few security clearance complaints. A lesson drawn from the past year is that departments and agencies should ensure that they provide clear and accurate information regarding an individual's rights of review and redress, and correctly identify both the nature of the security status at issue and the body to whom the person may complain as a result of being denied that status. By the same token, NSIRA is taking steps to increase the public's awareness of our mandate, while also ensuring that complainants are informed of their redress mechanisms early on so that their rights to seek a remedy are preserved.

153. With respect to security clearance complaints investigated both by NSIRA and SIRC, some of the key issues revolved around out-of-country background checks and cases in which there was insufficient information to grant an individual a security clearance. One of the lessons derived from these types of complaints is that departments must ensure that individuals receive a written notice informing them of the reasons for the decision, if that is possible in the circumstances (i.e., such disclosure is not prohibited under federal legislation). Going forward, NSIRA will continue to encourage the parties to make efforts to informally resolve complaints at the earliest opportunity.

Section III — Whistleblower protection

154. The *Public Servants Disclosure Protection Act (PSDPA)* is whistleblowing legislation that offers federal public sector employees an external mechanism to report ethical breaches and to complain about reprisals that they believe they have suffered.[82] The PSDPA, however, specifically excludes members of CSIS, CSE and the Canadian Armed Forces (CAF), as well as all people who wish to make a disclosure pertaining to special operational information.[83] CSIS, CSE and the CAF have implemented internal mechanisms for disclosure of wrongdoing, pursuant to their requirements under the PSDPA. However, the current structure offers no external reporting mechanisms for disclosures that pertain to special operational information and/or for employees from CSIS, CSE or the CAF.

155. As discussed above, a "public interest defence" is available, in certain circumstances, to Canadian whistleblowers who are permanently bound to secrecy and who have been charged with certain offences under the *Security of Information Act* (SOIA).[84] This defence is available only if the accused has followed the steps outlined in the SOIA before making the disclosure to the public.[85] The SOIA identifies NSIRA as a forum in which, under certain conditions, this kind of disclosure of wrongdoing can be made.[86] However, the SOIA does not describe how this process is meant to function procedurally nor does it articulate the role, if any, that NSIRA should play in accepting disclosures of wrongdoing from CSIS, CSE or CAF employees.

156. In previous correspondence to the Attorney General,[87] NSIRA identified these legislative gaps and the negative implications for national security that can occur when democratic countries have deficient protocols for whistleblowing within their national security and intelligence communities. In the interim, NSIRA will be implementing internal procedures to address concerns brought forward by members of the security and intelligence community. If the concern brought to NSIRA is not within the scope of the public interest defence under section 15 of the SOIA, NSIRA can examine the matter if it relates to NSIRA's review mandate, pursuant to subsection 8(1) of the NSIRA Act.

157. Canada's threat environment and national security landscape require effective and robust protections for Canada's national secrets and for the public servants who keep these secrets. Potential legislative amendments to enhance current whistleblowing protections for members of the security and intelligence community could include amendments to the SOIA, to the PSDPA or to the NSIRA Act. A key component of any legislative amendment would be external accountability and protections akin to those of the Office of the Integrity Commissioner under the PSDPA.

Section IV
— Priorities for the year ahead

158. In 2020, NSIRA is modernizing the complaints process. NSIRA's goal remains the just, efficient investigation and resolution of complaints. Modernization is needed to adapt to the changing complaints landscape. Two priorities will guide the modernization: access to justice for self-represented complainants and a broader spectrum of tools to streamline the resolution of complaints.

159. To this end, NSIRA is updating our website and revising our forms to provide clearer directions for potential complainants. We intend to place greater emphasis on explaining NSIRA's jurisdiction, and how to file complaints, which should assist in a complaint starting in a timely fashion and in the correct forum. Further, the website will contain a guide for self-represented complainants, so they can better navigate each step of the process and have their complaint resolved in an appropriate way.

160. One size never fits all. Each complaint that NSIRA receives calls for a unique approach. As noted, we are currently updating our Rules of Procedure. The new rules will allow for greater flexibility, efficiency and transparency. Some of the changes under consideration are the following: a discussion of expectations with a complainant at the outset; a new process for quickly deciding jurisdiction; an interview with the complainant; more options for informal resolution; quick and standardized disclosure of information between the parties; and, a requirement for declassified file summaries and chronologies. NSIRA believes these changes will allow complaints investigations to proceed more quickly and in a more efficient manner.

Engagement and transparency



04

As expressed in the *National Security Act, 2017* preamble, "enhanced accountability and transparency are vital to ensuring public trust and confidence in Government of Canada institutions that carry out national security or intelligence activities."[88] Along with public engagement, these are core values for NSIRA and we consider each to be vital to ensuring that we fulfil our mandate. The benefits of public engagement have been underscored in recent years, including through the national security consultations undertaken by the government in 2016. Engagement with stakeholders during our first year of operation helped establish connections and relationships that we will build on in the years ahead. As outlined in this section, NSIRA has taken strong steps in our first year of operation to promote increased transparency of national security and intelligence activities. In addition to our own initiatives, NSIRA will continue to encourage departments and agencies to promote transparency of their activities, including in fulfilment of the National Security Transparency Commitment.[89]



Section I
— Engagement

162. In 2019, NSIRA launched a series of public engagements to increase awareness about the organization, to expand our network, and to deepen our understanding of Canadians' concerns with respect to national security and intelligence activities. In 2019 and into 2020, we undertook engagement sessions throughout the country with various stakeholders, including academics, civil society, law enforcement and government organizations.

163. These sessions provided a valuable opportunity for NSIRA to hear from stakeholders about programs and issues that they recommended for NSIRA review, as well as the privacy and civil liberties risks they felt these programs presented. The uniformly positive feedback that NSIRA received from stakeholders demonstrated the value of these engagements.

164. Internationally, NSIRA continues to be actively involved with the Five Eyes Intelligence Oversight and Review Council, which allows NSIRA to: advance our knowledge of cross-cutting international themes in the area of national security and intelligence accountability; share priorities and compare best practices; collaborate on key issues of mutual interest; and promote coordinated review of issues of international importance.

165. Over the coming year NSIRA intends to continue our program of outreach and engagement. We will take advantage of opportunities to connect with stakeholders nationally and internationally via videoconference and, where possible, in person. In the year ahead, engagement will focus on four key areas:

- expanding our network with respect to issues related to new and emerging technologies (including artificial intelligence), to better understand their use as well as the risks and opportunities they present from a national security accountability perspective;
- broadening our dialogue with stakeholders to inform future review priorities;
- building new relationships with community groups to demystify the complaints investigation process; and
- scaling up recruitment efforts to ensure we continue to build an elite workforce with a diverse set of skills and backgrounds.

Section II
— Transparency

166. NSIRA has taken a number of steps to increase openness and transparency related to our work and the work of the national security and intelligence community. We established a Twitter account[90] early in our mandate, which we are using to share content, provide updates on our work and provide a platform for dialogue on security-related issues.

Redaction and writing for release

167. Over recent months, NSIRA has begun publishing reports from our predecessor organization, the Security Intelligence Review Committee (SIRC), that had been redacted for release to individuals who had applied to see the reports through the *Access to Information Act.* Under the *Access to Information Act,* the reports only had to be made available to the applicant. To support transparency, NSIRA plans to gradually publish online redacted versions of all SIRC reviews, from 1985 to 2019, which involves more than 270 reports.[91]

168. To complement this initiative, NSIRA also wishes to proactively redact and release future NSIRA reports as they are approved and translated throughout the year, rather than waiting for the release of our annual report to publicize our findings and recommendations. This aims to enhance the timeliness and relevance of NSIRA's work to public discourse on national security and intelligence issues. It also means that we can devote more time and space in future annual reports to discussing and analyzing horizontal or thematic trends, rather than individual (or vertical) reviews or issues.

169. NSIRA is working with departments and agencies to ensure that this new approach takes place in such a way that vital national security and intelligence information is protected, while at the same time providing the public with as much insight as possible into the results of our reviews. On a case-by-case basis, relevant ministers will be offered an opportunity to raise concerns with respect to the release of specific reports.

170. To facilitate redaction efforts and release reports in an efficient and timely manner, NSIRA has committed to making efforts to "write for release." This method includes writing as much as possible at an unclassified level, including unclassified executive summaries; clearly identifying within a report what portions contain classified information; and leaving classified information out of the body of the report where possible and, instead, including it in footnotes or annexes.

Conclusion

171. We are very proud of NSIRA's achievements during our first five months of operation. We have an ambitious agenda for the year ahead, despite the constraints imposed by the pandemic. We have set in motion a review plan that covers multiple issues over the coming year and will involve numerous departments and agencies. We are in the midst of significantly overhauling our complaints investigation process, with the aim of making it more accessible for all. We will also expand our corporate infrastructure to facilitate our growth over the years ahead, including through the acquisition of additional office space and the hiring of talented new staff.

172. We look forward to deepening our relations with other review and oversight bodies in Canada and internationally, as well as with diverse stakeholder groups to ensure that our work is as effective and as meaningful as possible. On that note, we hope that this report is useful. We encourage all readers to tell us their thoughts on the format, the content, and any aspects that we can improve in the next iteration.[92]

173. We are very grateful to our staff for continuing to achieve strong results despite the challenges that the ongoing pandemic has presented. We look forward to tackling the many challenges and opportunities that await us in the year ahead.

Annex A:
Summaries of NSIRA reviews finalized during the reporting period

REVIEW OF CSIS' USE OF GEOLOCATION INFORMATION

1. The background for this review was recent decisions by the Federal Court, most particularly the IMSI decision in September 2017, that impact CSIS's collection, use and retention of data, including geolocation data. The decision found that, though CSIS's authority under section 12 does authorize it to obtain geolocation information for which there is a low expectation of privacy, anything beyond that, such as geolocating an individual, would require a warrant.

2. CSIS's data collection and exploitation activities are of ongoing interest to NSIRA. This was the first dedicated look by NSIRA at CSIS's collection of geolocation data, a particular type of digital information that can be used to geolocate an individual.

3. The primary objective of this review was to assess whether CSIS's collection of geolocation information was compliant with the *Canadian Charter of Rights and Freedoms* (Charter) and the CSIS Act, as well as Ministerial Direction and operational policy. In this case, at issue was whether the use of the data to collect information about an individual's location information constituted a search for the purposes of section 8 of the Charter, such that a warrant would be required. To conduct this assessment, an in-depth case study of a specific form of geolocation information was conducted.

4. The review was also an opportunity to note more broadly that, in this environment, ongoing legal support to CSIS's data exploitation activities is essential to allow CSIS to operate at an acceptable level of risk and, further, that CSIS and the Department of Justice are expected to demonstrate institutional leadership in this regard.

Findings and Recommendations

There was a risk that CSIS breached section 8 of the Charter

5. The review found that there was a risk that CSIS breached section 8 of the Charter during the trial period in which it used the data without a warrant. NSIRA concluded that, in most cases, CSIS will need a warrant to collect a person's location information; otherwise, there will be a risk of breaching section 8 of the Charter, which protects against unreasonable searches and seizures.

Recommendation: That CSIS review its use of the geolocation data it collected and make a determination as to which of the operational reports generated through the use of this data are in breach of section 8 of the Charter. These operational reports and/or any documents related to those results should be purged from its systems.

CSIS overlooked multiple indicators that using this data might raise legal issues

6. The review found that CSIS overlooked multiple indicators that using this data might raise legal issues, including internal discussions early on, when concerns about legal risk were raised. In this case, moreover, it was noted that there were indications of a need for caution with respect to the data in the period before the trial was even begun, including the IMSI decision of the Federal Court, which found that geolocating an individual would require a warrant.

7. It was suggested that it would not have been possible to conduct a thorough assessment of the data before the trial period based on the reasoning that a risk assessment is only possible with full use of the data. NSIRA accepts in principle that there are situations when it would be difficult to appreciate the legal risks until such time as the data is accessible to CSIS and fully evaluated. Notwithstanding the difficulties, it is the responsibility of CSIS to mitigate all risks, including legal risks, to the extent possible.

Recommendation: That policy be developed or amended as appropriate that would require a documented risk assessment, including legal risks, in situations like this, when information collected through new and emerging technologies may contain information in respect of which there may be a reasonable expectation of privacy. A policy centre for this type of collection should be clearly identified.

There was no policy centre clearly responsible for the use of the data

8. The review sought to determine whether CSIS had sufficient safeguards in the form of formal procedures and policies to ensure that it is able to comply with its legal obligations amid a period of rapid change in technology and a correspondingly fluid legal environment.

9. The review found that there was no policy centre clearly responsible for the use of the data. This was supported by an examination of CSIS's policies and procedures in place at the time and that guided the decision to authorize the initial use of the data for a trial period. The review pointed to three discrete units involved in the acquisition, assessment and approval of the data for the trial period. Ultimately, however, the review was unable to identify which of the three units should have had responsibility for the assessment of this type of data.

There were no developed policies or procedures around the assessment and handling of new and emerging collection technologies

10. The review sought to determine whether CSIS's existing policies or procedures accommodated for this type of collection. The review found that there were no developed policies or procedures around the assessment and handling of new and

emerging collection technologies, such that a formal evaluation of the legal risks would have been required. NSIRA was also told that there is no formal process for the evaluation of risk, including legal risk, in cases like this, given that the data was assessed as "open source". The review identified this as a possible gap in CSIS's process and noted the requirement in Ministerial Direction that the risk of operational activities be assessed across four pillars (operational, political, foreign policy and legal).

The record of approval was not properly retained

11. Finally, the review found that the record of approval to pilot the data consisted of an email and that this email did not form part of the official record, as it should have been.

REVIEW OF CSE'S PRIVACY INCIDENTS FILE

1. NSIRA completed its first ever review of CSE since the coming into force of the NSIRA Act.

2. NSIRA's review examined CSE's Privacy Incidents File (PIF), which collates privacy incidents discovered by CSE. 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.

3. The objectives of the review were to assess and evaluate CSE's policies and practices in response to privacy incidents. NSIRA researchers examined a selected sample of 72 incidents out of a total of 123 incidents reported in the PIF for the period of July 1, 2018 to July 31, 2019.

Findings and Recommendations

4. For the privacy incidents examined, NSIRA believes that CSE employed compliance measures in a timely manner and according to policy. However, NSIRA made five additional findings and corresponding recommendations to improve CSE's documentation, assessment, and mitigation of privacy incidents.

PIF as a tool to prevent systemic incidents and identify areas of weakness

5. While CSE has adopted a layered approach to increasing privacy protection measures, CSE is not using the PIF, or any similar collated record of privacy incidents, to prevent systemic incidents from re-occurring, or to identify any areas of weakness in existing policy and/or practice that may reduce the occurrence of privacy incidents.

Recommendation: CSE should examine the totality of all privacy incidents with the view to identifying systemic trends or areas of weakness in existing policy and/or practice that may reduce privacy incidents.

Inconsistent mitigation, reporting and documentation of privacy incidents

6. Upon examination of the PIF and all supporting documentation, NSIRA found that the mitigation, documentation and reporting of privacy incidents was inconsistent and did not always meet the objectives set out in CSE internal policy.

Recommendation: CSE should adopt a consistent approach to assessing and documenting all privacy incidents.

Ability to further mitigate potential harm from privacy incidents

7. The mitigation actions for many privacy incidents are focused on stopping the continued potential harm after an incident was discovered. However, for some types of incidents, NSIRA believes that CSE is able to do more to mitigate potential harm arising from privacy incidents.

Recommendation: CSE should further examine potential harm arising from privacy incidents to determine if additional mitigation measures are warranted.

Limited assessment of incidents as material privacy breaches

8. As per the Treasury Board of Canada Secretariat's Directive on Privacy Practices, CSE must report the occurrences of material privacy breaches. However, CSE's assessment of whether an incident was a material privacy breach was limited.

Recommendation: CSE should standardize its policy on assessing whether incidents constitute a material privacy breach.

One inappropriate mitigation method

9. NSIRA found that a CSE policy in response to some incidents is an inappropriate mitigation method. This method did not appear to meet legal and Ministerial Authorization criteria and has the potential to engage section 8 of the Charter.

10. CSE re-examined the use of the mitigation method in question as a result of concerns expressed by NSIRA during the review, and this led to a decision by CSE to rescind the practice in November 2019.

Recommendation: CSE should rescind this policy, or obtain a legal opinion on the lawfulness of this practice.

REVIEW OF CSIS INFORMATION SHARING

1. To meet the requirements of its mandate to investigate threats to the security of Canada, CSIS must exchange information with foreign entities. However, there are risks involved in exchanging information with these entities which means that CSIS has had to develop various measures to mitigate the risks. For example, the exchange of information is subject to written or verbal caveats and assurances, which restrict how CSIS' information can be used or shared.

2. The purpose of NSIRA's review was to determine whether, in the three cases in question, CSIS had secured sufficient assurances to ensure that when information is exchanged, it can comply with its legal obligations and ministerial directions; and, insofar as possible, it can mitigate the risks of exchanging information with foreign entities.

3. Three case studies were reviewed based on decisions made by the Information Sharing Evaluation Committee (ISEC or Committee) in 2018-2019. In the three cases, the review examined the information exchange cycle, meaning, from the creation of the memorandum of understanding to the potential risk of exchanging information with a foreign partner.

Findings and Recommendations

Involvement of the Director in decision making

4. When the Committee made a decision, CSIS was not required to solely take the opinion of Legal Services into account in its decision-making process. A decision was adopted if it received the majority of votes, regardless of the opinion of Legal Services.

5. The assessment of the mitigating measures and their impact is not just a legal issue, it is also based on the facts presented. CSIS remains responsible for the Committee's decisions. Nevertheless, Legal Services has a unique perspective with respect to advising the Committee of the legal principles, thresholds and standards, and providing opinions on whether CSIS acted in keeping with the permitted legal rules and instruments.

6. In the opinion of NSIRA, the Director must be advised when the Legal Services representative does not believe the planned action is permitted by law. The review showed that a few cases studied should have been referred to the Director to enable the latter, not the Committee, to be responsible for the final decision in compliance with the MD: Avoiding Complicity in Mistreatment by Foreign Entities.

Recommendation: When, in the opinion of Legal Services, the substantial risk of mistreatment cannot be mitigated, the case should be automatically referred to the Director of CSIS for a decision.

Obtaining a legal opinion in writing for the use of new measures

7. During the review, CSIS examined new measures for mitigating risk with a view to permitting the exchange of information when there are human rights concerns associated with a foreign entity. In a few of the cases studied, these measures were proposed to mitigate the substantial risk of mistreatment. In these cases, CSIS obtained only verbal legal advice.

8. NSIRA recognizes that the time allotted to prepare a legal opinion before a meeting does not always lend itself to obtaining formal advice in writing. Nevertheless, the Committee members should understand how innovative measures work before they are satisfied that the measures selected constitute a sufficient mitigating measure. Formal advice would enable CSIS to determine the possible validity of these new measures as mitigating measures.

Recommendation: CSIS should request a formal legal opinion to determine whether these new measures could be considered mitigating measures in the future when information is exchanged with a foreign entity.

REVIEW OF DEPARTMENTAL FRAMEWORKS FOR AVOIDING COMPLICITY IN MISTREATMENT BY FOREIGN ENTITIES

As part of our governing statute, NSIRA is now required to review departments' implementation of GIC directions on information sharing with foreign partners under the Complicity Avoidance Act. To date, the GIC has issued these directions to 12 departments, including several that have never before received formal direction specific to information sharing with foreign partners.

To prepare for this new responsibility, NSIRA launched our first interagency review, an assessment of how six departments — the CBSA, CSE, CSIS, DND, GAC and the RCMP — were implementing the 2017 Ministerial Direction on Avoiding Complicity in Mistreatment by Foreign Entities, which was the basis of the direction under the Complicity Avoidance Act. The purpose of the review was also to provide a future roadmap for departments that, pursuant to the Complicity Avoidance Act, received this direction for the first time in 2019.

NSIRA found significant variation among the six departments in terms of their success in implementing the 2017 Ministerial Direction. Some, like CSE, have developed and rolled out comprehensive policy suites to guide their information sharing with foreign partners. Some departments face challenges in operationalizing this direction. Some also face challenges in establishing decision-making mechanisms that are independent from the operational front line in cases where there is a risk of mistreatment. One of the key issues that NSIRA's review identified was the consistent application of the "substantial risk" threshold across departments and agencies. This will be an area of inquiry in the future.

REVIEW OF CSIS's INTERNAL SECURITY BRANCH

1. Ensuring the protection of people, information and other assets is the responsibility of CSIS's Internal Security (IS) Branch, which conducts personnel security screening, inquiries, and investigations into employees or security incidents. This NSIRA review was a follow-up to a 2013 SIRC study of CSIS's IS Branch that found a number of serious shortcomings related to CSIS's handling of sensitive case files, access lists and the practices and management of internal investigations.

2. The objectives of NSIRA's review were to assess the progress made by CSIS in implementing the 2013 recommendations, as well as assess the adequacy, adherence and effectiveness of IS processes used to examine actual or potential security incidents, violations and breaches.

3. NSIRA concluded that while significant improvements have been made with respect to internal security at CSIS since the 2013 review, further improvements to internal security policies could strengthen the consistency of decision-making on personnel security files and investigations, and improve the procedural fairness of these processes writ large.

Findings and Recommendations

Internal inquiries/investigations at CSIS are professionally managed and seek to minimize bias and subjectivity to the extent possible.

4. SIRC's previous review of CSIS's IS Branch in 2013 was controversial, not because of the nature of the review, but due to the totality of the implications derived from the findings: namely, internal security at CSIS had a number of serious shortcomings. The evidence assessed from the current review has led NSIRA to arrive at an updated conclusion. In particular, CSIS's training and mentoring programs have been augmented: policy has generally been improved; decision-making pertaining to inquiries was documented in the appropriate files; and finally, CSIS has taken constructive steps towards reducing bias and subjectivity through the creation of innovative tools and by consulting with pertinent stakeholders outside of IS to help develop practical risk-mitigation strategies.

CSIS conducted the activities reviewed in accordance with its legal obligations set out in the CSIS Act. However, CSIS has not developed sufficiently detailed governance on when and how to report suspected criminal activity uncovered during an internal inquiry/investigation or security assessment.

5. When IS Branch uncovers suspected criminal activity, law enforcement often needs to be promptly informed; however, there may also be a risk in reporting to law enforcement in haste. There are several important issues to consider when deciding whether or not (and how) to report information to the police. Once law enforcement is involved, the relationship between the employee and the Service is irrevocably impacted. Furthermore, the issues may include:

privacy protections; labour relations obligations; the authority under which the disclosure is taking place; the method of disclosure; the appropriate authority to receive the disclosure; whether or not to notify the individual about the disclosure: as well as any potential harm to the employee, to the Service, to other employees, to the government, and to the public interest.

Recommendation: CSIS develop an internal policy, in consultation with Treasury Board Secretariat (TBS), outlining parameters on reporting information obtained during the course of IS screening, inquiries, and investigations to law enforcement in a timely manner.

The Unit responsible for the methodology and application of the polygraph has a number of interrelated governance issues, including:

- *Informal policies and procedures*
- *Lack of clear boundaries between polygraph and medical analysis;*
- *Limited oversight of polygraph program;*
- *No privacy impact assessment on polygraph process; and*
- *No employee feedback mechanism specific to the polygraph*

6. The review observed that IS Branch's current policy suite is insufficiently detailed to answer questions related to standardization of polygraph assessments, examiner training, quality-control measures and definitional thresholds. CSIS could not justify the merits of examiners – who are not medical practitioners – to ask medical-related questions of the people they examine. There are also limited oversight controls of the polygraph program.

7. Given that the polygraph is an invasive tool, employees are required to consent to having it administered if they want to have their Enhanced Top Secret (ETS) clearance granted or renewed. NSIRA therefore enquired about Privacy Impact Assessments (PIAs) conducted on the polygraph process at CSIS. According to TBS, a PIA is to be initiated for a program or activity whenever personal information is used for, or is intended to be used as, part of a decision-making process that directly affects the individual. Despite this policy requirement, no PIA has been conducted on CSIS's polygraph process; following the review, CSIS signalled an intent to undertake a PIA for the program.

8. In the absence of a PIA, NSIRA enquired about other mechanisms or processes by which to gauge employee experiences with the polygraph. CSIS employees both understand the need to take the polygraph and expect that their examination will be conducted professionally. Despite this reasonable expectation, there is no employee survey question exclusive to polygraph-related activities, although test subjects can raise issues with managers responsible for the polygraph. The CSIS Director has publicly acknowledged that harassment, bullying, and reprisals are issues which need to be addressed across the Service. NSIRA observed no evidence of similar systematic issues associated with the administration of the polygraph.

Recommendation: CSIS strengthen internal governance over polygraph activities, including modifying the methodology for conducting polygraph assessments, as appropriate.

Based on the information reviewed and interviews conducted on CSIS's use of the polygraph, NSIRA observed:

- *The polygraph is central to CSIS' inquiry and five-year update processes;*
- *The outcomes or consequences for polygraph exams conducted on external applicants compared with CSIS employees differed; and*
- *CSIS requires policy clarity for cases where employees fail the polygraph examination.*

9. Historically, CSIS has underscored that security clearances or employment are not denied solely based on a polygraph examination; supporting evidence from other sources has always been required. SIRC was critical of the use of the polygraph by CSIS and has questioned the polygraph's accuracy and the extent to which it was voluntary. For this review, there were noted differences in outcomes between external applicants and CSIS employees, even with similar test results.

10. Essentially, a successful polygraph is a determinative factor for external applicants in obtaining an ETS clearance through CSIS.[Text removed - As of November 20, 2020, NSIRA and CSIS could not agree on how all of the facts of this review should be presented in an unclassified, public document]. CSIS has no clarity in its policy on how to address this issue.

11. In addition to the above challenges, the review identified that polygraph examinations can have profound negative impacts on an employee's mental health if not used appropriately. Employees who spoke to NSIRA on condition of anonymity described the negative impact that their unfavorable polygraph results had on their lives, and was particularly evident during documentation review of post-exam correspondence between employees and the unit responsible for administering the polygraph.

Recommendation: CSIS update applicable policy and procedures on the use of the polygraph to address security and procedural fairness implications stemming from failed polygraph results.

Based on the information reviewed and interviews conducted, NSIRA found that IS complies with the Standard on Security Screening and its own policies in its management of complex cases arising from the security assessment process, but notes that the associated decision-making could be strengthened with improved governance and policy clarity.

12. NSIRA believes that fair and consistent standards for interpreting criminality, including admissions to minor criminality, would ensure that CSIS applies its judgements equally given the primacy of its role in security assessment for the Government of Canada. NSIRA notes that IS Branch is undertaking macro-level tracking of decisions rendered and their associated rationale, which will improve the ability of IS interviewers to locate relevant previous decisions rendered as well as the considerations and circumstances involved. NSIRA supports IS's decision to solidify this responsibility within a new position to be created, and believes this will be a strong step toward improved documentation and definition of the practical threshold.

Recommendation: IS further align its overarching policy suite with the assessment criteria for adverse information outlined in the Standard on Security Screening, as well as update the its Questionnaire Guidebook with clear definitions and risk indicators.

Several pertinent legal opinions and legal documents were received only once the review was substantially written and complete, preventing their timely incorporation and consideration in the final report.

As a result of delayed disclosure, a total of five pertinent legal opinions, and two other pertinent legal documents, were received after the report was drafted and sent through for internal review. NSIRA was able to make some amendments to the draft on certain specific issues in order to properly reflect the recently obtained information. However, these legal opinions were relevant to the issues covered in the report and the review would have benefited from their full consideration. NSIRA notes, however, that access to all of the other information pertaining to this review was provided efficiently and effectively both electronically and on paper files.

Annex B:

Summaries of unreleased SIRC and OCSEC reviews up to July 2019

SIRC Reviews, April 2018-July 2019

SIRC Certificate 2018-07

In March 2019, SIRC completed its certification of the Director of CSIS's 2017-18 Annual Report to the Minister of Public Safety and Emergency Preparedness.

To support certification, SIRC reviewed a number of topics discussed in the report, including CSIS targets under the age of 18, information sharing cases involving a significant risk of mistreatment, a survey of CSIS's internal compliance reporting, and an aspect of CSIS's operations involving "Canadian Fundamental Institutions" or CFIs. CSIS defines CFIs as political, government, religious, post-secondary, and media establishments. Overall, SIRC found these activities to have been compliant with the CSIS Act, Ministerial Direction, and internal policies and procedures.

There was an important exception, however. Until January 2019, the Director of CSIS approved certain CSIS human source activities despite CSIS having been advised that they were "high legal risk", which is to say that the activities were very likely unlawful. As a result, SIRC concluded that "CSIS undertook human source activities despite knowing that these activities did not comply with the CSIS Act and Ministerial Direction, which stipulates that the rule of law must be observed." SIRC further observed that although the operations may have been important or valuable, this did not mitigate their unlawfulness.

NSIRA has since published a redacted version of the certificate, available at: https://nsira-ossnr.ca/wp-content/uploads/2020/09/2018-07-eng.pdf

Review of CSIS Threat Reduction Measures

This review was conducted pursuant to the CSIS Act, which stipulates that SIRC review each year, "at least one aspect of the Service's performance in taking measures to reduce threats to the security of Canada." SIRC found that all Threat Reduction Measures (TRMs) reviewed were in compliance with the CSIS Act, ministerial direction and applicable policies and procedures. SIRC also reviewed the evaluation of the threat reduction activity – i.e., the performance measurement. The difficulty in measuring performance is a challenge for all Five Eyes partners when engaging in disruption activities. SIRC found that CSIS is making efforts to improve performance measurement, there is work that remains to be done, however. Particular attention will have to be paid to assessing intermediate and strategic outcomes, leaving as little room as possible for subjectivity.

Review of CSIS's Execution of a Warranted Technical Collection

This baseline review examined CSIS's practices for acquiring information from third parties in support of its technical collection. SIRC found that changes to CSIS's compliance governance system have enhanced the overall management of compliance risks in the context of warranted operations. SIRC is satisfied with the action taken by CSIS in the cases reviewed to manage the risks identified through this process. SIRC also found that CSIS took action to manage the risks, and reported incidents of non-compliance that involved powers executed under the authority of a warrant, to the Federal Court, and in certain cases, to the Minister of Public Safety and to SIRC.

Review of CSIS Activities Involving Basic Identity information

CSIS defines Basic Identifying Information (BII) as the names and addresses – and occasionally other electronic identifiers – found in the customer records associated with phone or other accounts sold by communications service providers. Access to BII permits CSIS to identify otherwise unknown persons of interest. For instance, CSIS may come into possession of a phone number associated with suspected threat activities. CSIS can then seek to obtain a warrant authorizing the collection of the name and address associated with the account that owned the phone number.

Recent changes to the BII collection process, in response to Federal Court rulings, have made the timely collection of BII challenging for CSIS. SIRC recommended that, should significant difficulties persist, CSIS and partners explore options to address these challenges. Options should bear in mind the privacy and Charter dimensions of BII.

Normally, CSIS does not know the identity of the person whose BII it seeks. It is thus unavoidable that some of those unmasked will ultimately be found to have no involvement in threat-related activities. Despite this, CSIS retains the information nearly indefinitely. The CSIS Act, however, obliges CSIS to collect and retain information only to the extent "strictly necessary". BII can reveal details of a person's activities for which they have a reasonable expectation of privacy, details CSIS might not have been authorized to collect had the identity of the individual been known in advance. CSIS should thus be particularly prudent in retaining such information.

CSIS currently has no comprehensive written policy regarding the collection, handling, retention, and disposal of BII, or the management of warrant compliance risks unique to BII. This increases the risk that CSIS personnel will inadvertently fail to comply with CSIS policy, or even the terms and conditions of BII warrants. SIRC recommended that CSIS prioritize the drafting of a comprehensive policy and process document for the collection, handling, retention, and disposal of BII. This should include procedures for the assessment of BII collected, and its destruction, segregation or other special handling when it is unlikely to be of significant value or relevance.

Review of CSIS Investigation of Foreign Influenced Activities

This review looked at the investigation of the foreign influenced activities of a foreign state. SIRC found that CSIS demonstrated its awareness of the political sensitivities associated with certain sources in this investigation, and found that CSIS complied with its internal policies. SIRC recommended that CSIS consult with the Department of Public Safety in order to clarify expectations with respect to being made aware of these certain sources. SIRC also found that advice from CSIS on the threats to the security of Canada posed by this foreign state was sufficient. However, SIRC also recommended that CSIS's advice on counterintelligence investigations be detailed enough that the government is fully aware of the operational challenges surrounding the investigation and its impact on the advice provided.

Review of CSIS's Engagement with Foreign Intelligence Services Operating within Canada

This study examined CSIS's foreign intelligence relationships and how CSIS strategically manages foreign agency activities within Canada or with Canadians as well as associated legislation and ministerial direction. SIRC found that incremental changes to MD and CSIS policies have collectively reduced the requirement to inform the Minister about foreign activities within Canada. SIRC found that the policy suite used to guide CSIS's interactions with foreign agencies operating in Canada or with Canadians abroad has not been applied consistently and is at times contradictory. In addition, SIRC found that there is no systematic verification of this policy suite to ensure that conditions are followed. SIRC recommended that CSIS create a systematic verification process to assist in managing this process. SIRC also found that CSIS did not meet the requirements of ss.7(1) of the CSIS Act. SIRC recommended that CSIS consult with the Department of Justice on the proper interpretation of ss.7(1) of the CSIS Act, and based on this, restart the legislatively required consultations with Public Safety Canada.

Review of a Foreign Station (#1)

SIRC reviewed the activities of a CSIS foreign station. SIRC found that the station's intelligence collection was well aligned with ministerial direction, and that CSIS's presence has improved Canada's understanding of threats to national security in the region. Two procedural gaps were identified and raised concerns for SIRC. The first relates to CSIS's foreign arrangements, for which the station had not sought new or renewed assurances from foreign entities since 2010. SIRC expects that CSIS will prioritize the seeking of assurances and the renewal of past assurances to ensure human rights are respected when sharing information. Secondly, a disjointed risk assessment process resulted in decision makers lacking awareness of the full extent of the risks of a certain operation. SIRC expects a single approval point for operation will more clearly document the full assessment of risk.

Review of a Foreign Station (#2)

SIRC reviewed the activities of a CSIS foreign station. SIRC found no issues with the nature and extent of information shared with foreign agencies during the review period. However, SIRC recommends that CSIS strengthen the guidance it provides to foreign stations following events that have the potential to affect foreign partnerships. In addition, SIRC found that there is neither a policy, nor a policy centre, detailing the proper guidelines on a specific protective device used for employee safety in dangerous areas. SIRC recommends that CSIS develop a policy or a policy centre on the governance of such protective devices, which could be incorporated into a larger Personal Protective Equipment framework.

Review of the Section 16 Foreign Intelligence Collection Program

This review explored how CSIS managed the increased demand for a specific type of section 16 operation. SIRC identified multiple bureaucratic issues that can transpire during section 16 investigations, such as delays caused by domestic partners and a lack of CSIS resources. Despite these issues, when executed efficiently, SIRC found this type of collection is a useful and important tool to the Minister of Foreign Affairs and the Government of Canada. SIRC also found that CSIS does not have a policy suite governing the section 16 program and relies on a Deputy Director of Operations Directive from 2014. SIRC recommended that CSIS adopt and publish a specific policy suite that details the requirements and expectations of the section 16 program.

OCSEC Reviews, March-July 2019

Review of a Foreign Signals Intelligence Collection Program Conducted by CSE under a Ministerial Authorization and a Ministerial Directive

This review examined CSE's activities under a particular foreign intelligence collection program from 2008-2015. For a number of reasons, including the eight-year review period, employee turnover and competing priorities of the CSE Commissioner's office, this review could not be completed until July 2019. In total there were six recommendations, three of which are no longer applicable following the coming into force of the CSE Act. OCSEC concluded that while CSE complied with the law, it did not abide by two expectations in a Ministerial Directive (MD) relating to the collection program. The MD also no longer applies following the coming into force of the CSE Act.

Review of a Privacy Incident Concerning a Metadata Analysis Activity by CSE

This review covered a particular privacy incident concerning a metadata analysis activity from the 2016-2017 Privacy Incidents File (PIF). It was completed on June 21, 2019, and stated that CSE complied with the law. OCSEC recommended that CSE ensure that privacy incident reports contain all relevant known information in order to describe and document each incident in a comprehensive manner. The rest of the 2016-2017 Privacy Incidents File Report was included in OCSEC's 2017-2018 Annual Report to the Minister.

Annex C:
Summaries of complaint investigations

Allegations related to a security assessment pertaining to an application for permanent residence: Complaint pursuant to section 41 of the CSIS Act

SIRC investigated a complaint pursuant to section 41 of the CSIS Act in which the Complainant alleged that CSIS made false allegations to a government department pertaining to the security assessment on an application for permanent residence. The Complainant further alleged that there was undue delay in dealing with the process on the application for permanent residence. As part of the security screening process for a permanent residence application, a security screening interview may be conducted by CSIS. The issue on Immigration security screening and CSIS' mandate was raised with regards to advising the federal government on immigration matters specifically when it comes to providing advice to those government departments, namely the Citizenship and Immigration Canada (CIC) and to the Canada Border Services Agency (CBSA).

Pursuant to sections 14 and 15 of the CSIS Act, CSIS conducts immigration and citizenship security screening. CSIS then conducts screening verifications. Should there be no adverse information, CSIS provides their response to the department that made the request. If the screening process reveals outstanding concerns in relation to adverse information, CSIS writes a brief and sends it to the appropriate department. The role of CSIS is to provide advice to the government departments involved and information in its possession which may be of interest in making a determination of the admissibility of the person. SIRC investigated and reviewed the advice provided by CSIS.

SIRC findings

SIRC found that CSIS did not make false allegations to both CBSA and CIC on the advice provided related to the application for permanent residence. Proper internal policies and procedures as well as the relevant provisions of the CSIS Act were followed.

On the issue of disclosure, the Complainant alleged that CSIS failed to meet its disclosure obligations to SIRC. SIRC concluded that it is for it to comment on the appropriateness of CSIS disclosure of classified information. SIRC was satisfied that the relevant evidence was properly placed before it.

With respect to the Complainant's submissions on the allegation of undue delay, SIRC determined that the screening process was conducted in a timely manner.

For these reasons, the complaint was dismissed.

Denial of a Security Clearance: Complaint pursuant to section 42 of the CSIS Act

SIRC investigated a complaint pursuant to section 42 of the CSIS Act concerning the denial of the Complainant's security clearance at any level by a Department. The Department also revoked the Complainant's reliability status. SIRC found that there were reasonable grounds to deny the Complainant's security clearance based on the totality of the information and evidence provided as a result of the security screening process.

Upon the evidence before it, SIRC investigated the security screening process conducted by CSIS and the Department. SIRC heard evidence on the security clearance process, and the policies and authorities in place for the decision-making on the security clearance assessment.

During its testimony, the Complainant alleged that he was subject to intimidation and harassment in his work environment as a result of the impact of the security screening investigation and that he was under surveillance by the American and Canadian security services and police services. The Complainant denied the allegations made following the results of the security assessment.

SIRC was satisfied that the Complainant was afforded procedural fairness during both the CSIS screening investigation and the Department's security screening review process. SIRC found that the Complainant was properly informed regarding the considerations provided and was given an opportunity to respond to them.

SIRC investigated the findings regarding the CSIS Security Assessment. SIRC was satisfied that the information relied upon by CSIS was accurate, credible, represented fairly and cast in its proper light.

SIRC findings and recommendation

SIRC found that there were reasonable grounds under the Policy on Government Security and Personnel Screening Standard for the Deputy Head of the Department to deny the Complainant's security clearance.

SIRC was satisfied with the accuracy of the information upon which the Department relied to make the decision.

For these reasons, SIRC recommended that the decision to deny the security clearance be upheld.

Allegations related to CSIS's actions that led to the denial of a site access clearance and revocation of a security clearance resulting in loss of employment: Complaint pursuant to section 41 of the CSIS Act

SIRC investigated a complaint pursuant to section 41 of the CSIS Act in which the Complainant alleged that CSIS's actions led to the revocation of the Complainant's site access clearance that caused loss of employment. The Complainant further alleged that such actions constituted discrimination and violated the Complainant's constitutional rights, and that CSIS provided a security assessment that is unfair and unreasonable. Lastly, the Complainant alleged that CSIS denied the Complainant's site access clearance as a form of retaliation against the Complainant.

The Complainant requested three remedies from SIRC which are as follows:

- CSIS be sanctioned in a manner to ensure its misconduct does not recur in the future;
- The Minister provide appropriate redress to the Complainant, including injuries the Complainant has suffered as a result of CSIS's actions and remedies under section 24 of the *Canadian Charter of Rights and Freedoms* (the Charter); and
- The Minister clear the Complainant of any allegations regarding the security of Canada.

SIRC considered evidence from the Complainant and CSIS as well as other relevant material made available during the course of the investigation of the complaint.

SIRC findings

SIRC found that CSIS acted lawfully and appropriately by denying the Complainant's security clearance and unsupported the Complainant's allegation regarding CSIS retaliating against the Complainant.

SIRC found that the Complainant's allegation that CSIS acted unlawfully and inappropriately by demanding the Complainant to engage in espionage on its behalf was unsupported.

SIRC also found that CSIS breached the Complainant's constitutional rights under section 8 of the Charter.

SIRC further found that CSIS did not afford the Complainant the level of procedural fairness he was owed in the course of certain investigations.

SIRC further found that CSIS's security assessment led to the denial of the Complainant's site access clearance, which caused loss of employment.

With respect to the Complainant's allegation that the Committee refer the matter to the Canadian Human Rights Commission, SIRC found that it would not be appropriate to make such a finding as there is sufficient evidence before it to make findings on the Complainant's allegations.

Finally, SIRC found that there was no evidence before it that would lead it to conclude that CSIS acted in bad faith in storing unsolicited material from an organization.

SIRC recommendation

SIRC recommended that CSIS follow through on obtaining legal advice in order to thoroughly consider and apply appropriate legal authorities in arriving at its decisions on the actions to take.

With respect to the Complainant's request for the recommendations indicated above, SIRC indicated that its mandate is to investigate alleged acts or things done by CSIS.

SIRC further indicated that it would exceed its mandate by making recommendations to the Minister for action he could consider. Upon considering the Report will be given to the Minister, SIRC was satisfied that the Minister will take any action he deems appropriate in the circumstances and pursuant to his own authorities.

Conclusion

SIRC concluded that there is no evidence that would lead to the conclusion that CSIS's actions constitute discrimination and it would not be appropriate for SIRC to ask the Canadian Human Rights Commission for its opinion and comments about this complaint. For the reasons above, the complaint was supported in part.

Allegations of disclosure and the sending of false information and identities to a third country: complaint under section 41 of the CSIS Act

The complainant went to SIRC in relation to a traumatic event he and his family experienced. The complainant's son, a minor at the time, had contact on social media with an individual whom the complainant identifies as a "cybercriminal." According to the complainant, the cybercriminal attempted to manipulate his son and convince him that living in a Western community was a sin. The complainant agreed to meet with two CSIS officers and later had them over to his home to discuss with his son his interactions with that individual. In this interview, the complainant alleges that the CSIS officers encouraged the complainant and his family to report the situation by telephoning the Royal Canadian Mounted Police (RCMP), which the complainant did that evening. The next day, his son was arrested at his home by the RCMP in front of a media circus set up close to the complainant's home. His son was ultimately released shortly thereafter and was not charged with any offence. However, the complainant argues that the consequences of these incidents still affect his family.

In part, the complainant blames CSIS and its officers for what happened to his family, if only for their inaction and their information sharing. The complainant objects to the treatment that he and his son received after doing their duty as citizens, which was to cooperate with the authorities and report a threat. He has accused CSIS and the RCMP of taking acting against the victim, his son, rather than the cybercriminal.

The complainant summarizes his allegations against CSIS as follows:

- CSIS sent false information to the RCMP Integrated National Security Enforcement Team;
- Faced silence from two RCMP members regarding the arbitrariness of RCMP members;
- CSIS sent the complainant's identity and that of his son to a third country;
- CSIS violated the findings and recommendations in Justice O'Connor's commission regarding the transfer of information;
- CSIS violated their privacy, integrity and security.

Conclusions

SIRC concluded that all allegations forming the basis of this complaint were to be rejected because they are rebutted by the evidence filed. The investigation into this complaint examined all the relevant facets stemming from the allegations.

SIRC concluded that CSIS acted in compliance with its mandate and priorities. No evidence was submitted demonstrating that CSIS strayed from the Act or its applicable targeting policies. SIRC finds that the thorough procedures regarding investigations involving minors were followed. SIRC concluded that CSIS had reasonable grounds to suspect the activities in question constituted a threat to the security of Canada and therefore took investigation steps under section 12 of the *Canadian Service Intelligence Service Act*. SIRC does not see the need to issue any recommendations to CSIS.

Annex D:
Statistical Tables on Complaints

April 1, 2018 – March 31, 2019

Intake inquiries	**91**	
New complaint files opened **Deemed received as per Rule 5**	**25** s. 41 (CSIS Complaints): 14 s. 42 (Security Clearances): 11 s. 45 (CHRC Act): 0	
Complaint files over which determination on jurisdiction was made	**19** Jurisdiction Accepted s. 41: 3 s. 42: 2 s. 45: 0	 Jurisdiction Declined s. 41: 7 s. 42: 7 s. 45: 0
Complaint files withdrawn prior to determination on jurisdiction	**2**	
Active complaint investigations during this time period (Once jurisdiction has been accepted)	**14**	
Complaint investigations carried over from the last fiscal year	**9** s. 41: 7 s. 42: 2	
Complaint investigations for which jurisdiction was accepted during this time period	**5**	
Total complaint investigations closed	**2**	
Complaint investigations closed	**0 Withdrawn** **0 Resolved** **2 Reports** s. 41: 2 s. 42: 0	
Complaint investigations to be carried forward to the next calendar year	**12** s. 41: 9 s. 42: 3	

April 1, 2019 – December 31, 2019

Intake inquiries	**67**
New complaint files opened **Deemed received as per Rule 5**	**32** s. 16 (CSIS Complaints): 17 s. 17 (CSE Complaints) : 0 s. 18 (Security Clearances): 10 s. 19 (RCMP Complaints): 5 s. 19 (Citizenship Act): 0 s. 45 (CHRC Act): 0
Complaint files over which determination on jurisdiction was made	**18** Jurisdiction Accepted s. 16: 3 s. 18: 0 s. 19: 1 Jurisdiction Declined s. 16: 6 s. 18: 8 s. 19: 0
Complaint files withdrawn prior to determination on jurisdiction	**3**
Active complaint investigations during this time period (Once jurisdiction has been accepted)	**16**
Complaint investigations carried over from the last fiscal year	**12** s. 16: 9 s. 18: 3
Complaint investigations for which jurisdiction was accepted during this time period	**4**
Total complaint investigations closed	**4**
Complaint investigations closed	**1 Withdrawn** **1 Resolved** **2 Reports** s. 16: 3 s. 18: 1
Complaint investigations to be carried forward to the next calendar year	**12** s. 16: 9 s. 18: 2 s. 19: 1

Annex E:

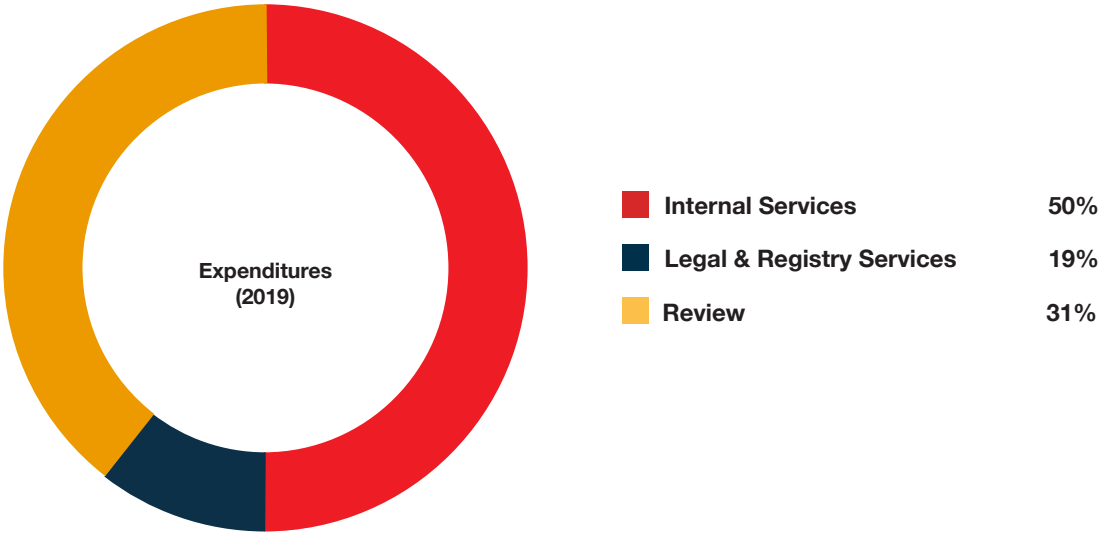
NSIRA corporate organization, achievements and priorities

NSIRA Secretariat staff is organized according to three main business lines: review; complaints investigations; and corporate services. To reflect the expansive mandate of NSIRA and to support review of a broad range of new activities and organizations, the Secretariat will be growing over the coming years, with plans for an ultimate staff complement of 100.

Below is a budgetary snapshot of the organization, followed by detailed information regarding the corporate transition from the Security Intelligence Review Committee (SIRC) to NSIRA, our key accomplishments, and our priorities for the year ahead.[93]

Expenditure reporting

	SIRC Expenditures from January to Year-End	SIRC & NSIRA Expenditures from April to December	Expenditures (2019)
Legal & Registry Services	378,670	663,446	1,042,117
Review	588,535	1,137,683	1,726,218
Internal Services	1,278,813	1,541,302	2,820,115
Total	$2,246,018	$3,342,431	$5,588,450



Transition from SIRC to NSIRA

Throughout 2019, the NSIRA Secretariat focused on ensuring a successful and effective transition to a much larger organization with a much broader mandate. This transition emphasized the following: securing new accommodations; hiring and training staff effectively; establishing strong working relations with departments and agencies, as well as other Canadian review bodies; and delivering on mandatory reporting requirements.

Key challenges from a corporate services perspective throughout the reporting period and continuing into 2020 include:

- hiring and accommodating the talented people needed to deliver on NSIRA's expanded mandate with the staff complement projected to grow from 33 to 100;
- scaling up physical, personnel and information security practices;
- implementing policies, procedures and systems to guide the new organization;
- implementing improvements to our technological and communication infrastructure;
- managing increased annual spending authorities — from $5.3 million to $24.1 million
- increasing the effectiveness of information management policies, systems and practices; and
- establishing effective privacy protection practices.

These challenges have been exacerbated since March 2020 and the continuing pandemic. Dealing with the impacts of COVID-19 has been particularly difficult in the context of accessing classified information, which, of course, can be done only within a secure environment. Nevertheless, NSIRA's corporate services group has achieved a great deal in the first year of operation. These achievements are outlined in greater detail below.

Human resources

Achievements in 2019

- Recruitment of a dedicated human resources team
- Completion and implementation of the core components of a Human Resources Management Policy and of Terms and Conditions of Employment
- Full roll-out of pay-related systems (PeopleSoft and Phoenix) and resolution of most of the long-standing pay issues of staff
- Finalization of NSIRA's organizational structure and completion of the majority of job classifications
- Strengthened staffing practices and implementation of an employee assistance program
- Conclusion of service delivery agreements with other government departments to support human resources operational activities such as processing pay actions, job classification and staffing activities

Security and accommodations

Achievements in 2019

- Creation of a dedicated team of employees responsible for security and accommodation activities
- Development of a multi-faceted security plan
- Completion of projects to maximize the number of offices at NSIRA headquarters and identification of interim, permanent and satellite space options to accommodate NSIRA's growing staff complement

Information technology and information management

Achievements in 2019

- Successful roll out of the Canadian Top Secret Network (CTSN) for all staff who require access to it, which permits secure electronic exchange of information with other departments and agencies
- Successful roll out of Virtual Private Network (VPN) access and encryption functionality, allowing access and exchange of information from existing NSIRA networks to remote desktops/laptops
- Digitization of several paper-based reviews and complaints

Finance, procurement, planning, and access to information and privacy

Achievements in 2019

- Implementation of NSIRA's financial and procurement systems and associated financial coding infrastructure
- Completion of the final financial year-end activities for SIRC and the first financial year-end activities for NSIRA
- Enhanced financial reporting to better support senior management decision-making
- Completion of a privacy impact assessment and an enhanced process for the redaction and release of information

Annex F:
List of abbreviations

Abbreviation	Full Name
ACO	active cyber operations
CAF	Canadian Armed Forces
CBSA	Canada Border Services Agency
CRCC	Civilian Review and Complaints Commission for the RCMP
CSE	Communications Security Establishment
CSIS	Canadian Security Intelligence Service
DCO	defensive cyber operations
DND	Department of National Defence
ETS	Enhanced Top Secret (security clearance)
FINTRAC	Financial Transactions and Reports Analysis Centre of Canada
FIORC	Five Eyes Intelligence Oversight and Review Council
GAC	Global Affairs Canada
GIC	Governor in Council
NSICOP	National Security and Intelligence Committee of Parliamentarians
NSIRA	National Security and Intelligence Review Agency
OCSEC	Office of the Communications Security Establishment Commissioner
OIC	Order in Council
OPC	Office of the Privacy Commissioner
PSDPA	*Public Servants Disclosure Protection Act*
RCMP	Royal Canadian Mounted Police
SCIDA	*Security of Canada Information Disclosure Act*
SCISA	*Security of Canada Information Sharing Act*
SIRC	Security Intelligence Review Committee
SOIA	*Security of Information Act*
TBS	Treasury Board Secretariat
TRM	threat reduction measure

Endnotes

1 Office of the Auditor General of Canada website, https://www.oag-bvg.gc.ca/internet/English/admin_e_41.html

2 Canadian Human Rights Commission website, https://www.chrc-ccdp.gc.ca/eng

3 More information on these elements of the organization are available on the National Security and Intelligence Review Agency (NSIRA) website, http://www.nsira-ossnr.gc.ca/

4 NSIRA Letter to Minister of Public Safety and Emergency Preparedness, March 16, 2020.

5 *Sections 12 and 21 of the Canadian Security Intelligence Service Act, RSC 1985, c C-23 (Re)*, 2020 FC 616, dated May 15, 2020. The decision is available at: https://decisions.fct-cf.gc.ca/fc-cf/decisions/en/item/482466/index.do

6 NSIRA Letter to the Attorney General of Canada, February 25, 2020.

7 NSIRA website, http://www.nsira-ossnr.gc.ca/

8 Consistent with transitional provisions 12(1) and 12(2) of the *National Security Act, 2017* this report also includes summaries of reviews that our predecessor organizations, the Security Intelligence Review Committee (SIRC) and the Office of the Communications Security Establishment Commissioner (OCSEC), had not yet reported on publicly. These are found in Annex B.

9 SIRC website, http://www.sirc-csars.gc.ca/index-eng.html

10 OCSEC website, https://www.ocsec-bccst.gc.ca/en

11 Additional information on corporate resourcing and results is available at: http://www.nsira-ossnr.gc.ca/pubpub/dppm/index-eng.html

12 Royal Canadian Mounted Police (RCMP) website, https://www.rcmp-grc.gc.ca/

13 Prior to this approach, the only way for the public to obtain copies of reviews was through requests under the *Access to Information Act*.

14 National Security and Intelligence Committee of Parliamentarians (NSICOP) website, https://www.nsicop-cpsnr.ca/index-en.html

15 Office of the Privacy Commissioner of Canada (OPC) website, https://www.priv.gc.ca/en/

16 NSICOP included an overview of the various classes of intelligence collection in chapter four of its 2018 annual public report, available at: https://www.nsicop-cpsnr.ca/reports/rp-2019-04-09/intro-en.html

17 Canadian Security Intelligence Service (CSIS) website, https://www.canada.ca/en/security-intelligence-service.html

18 CSIS warrants for the collection of information are issued under section 21 of the CSIS Act. These warrants can either support CSIS investigations into threats to the security of Canada under section 12 of the Act, or they can support CSIS foreign intelligence investigations under section 16 of the Act. See section 21 of the CSIS Act, available at: https://laws-lois.justice.gc.ca/eng/acts/c-46/page-41.html#h-118715

19 Communications Security Establishment (CSE) website, https://www.cse-cst.gc.ca/en

20 See the part of the CSE Act on "Authorizations," available at: https://laws-lois.justice.gc.ca/eng/acts/C-35.3/page-3.html#h-1170483

21 See the *Intelligence Commissioner Act* on the Intelligence Commissioner's "Duties and Functions," available at: https://laws-lois.justice.gc.ca/eng/acts/I-14.85/page-1.html#h-1170243. More information on the role of the Intelligence Commissioner is available on the Office of the Intelligence Commissioner's website, https://www.canada.ca/en/intelligence-commissioner.html

22 A number of overarching statutes govern how government departments can collect, retain and disseminate personal information. The most important of these is the *Privacy Act*.

23 A recent example in this regard is the Ministerial Direction to the Canadian Security Intelligence Service: Accountability, issued September 10, 2019, and available at: https://www.publicsafety.gc.ca/cnt/trnsprnc/ns-trnsprnc/mnstrl-drctn-csisacc-en.aspx

[24] For more information, see especially: OPC (2014), "Metadata and Privacy — A Technical and Legal Overview," https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2014/md_201410/; and SIRC's review of CSIS's use of metadata, http://www.sirc.gc.ca/anrran/2014-2015/index-eng.html#sc2-7

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

[26] SIRC (2015), Broader Horizons: Preparing the Groundwork for Change in Security Intelligence Review — Annual Report 2014–2015, "Baseline review: CSIS's Use of Metadata." http://www.sirc.gc.ca/anrran/2014-2015/index-eng.html#sc2-7

[27] Discussed in the OCSEC 2014–15 annual report, https://www.ocsec-bccst.gc.ca/s21/s46/s20/d274/eng/highlights-reviews-reports-submitted#toc-tm-7-1

[28] SIRC (2016), Annual Report 2015–2016 — Maintaining Momentum, "Review of CSIS's Data Management and Exploitation Activities." http://www.sirc.gc.ca/anrran/2015-2016/index-eng.html#section_2_4

[29] *X (Re)*, 2013 FC 1275, affirmed on appeal in 2014 FCA 249; 2016 FC 1105; and 2020 FC 616, dated May 15, 2020.

[30] Minister of Public Safety and Emergency Preparedness (September 10, 2019), Ministerial Direction to the Canadian Security Intelligence Service: Accountability. https://www.publicsafety.gc.ca/cnt/trnsprnc/ns-trnsprnc/mnstrl-drctn-csisacc-en.aspx

[31] *Sections 12 and 21 of the Canadian Security Intelligence Service Act, RSC 1985, c C-23 (Re)*, 2020 FC 616, dated May 15, 2020. The decision is available at: https://decisions.fct-cf.gc.ca/fc-cf/decisions/en/item/482466/index.do

[32] In the May 12, 2015, review of CSIS's relationship and exchanges with the Department of Foreign Affairs, Trade and Development, SIRC drew attention to the legal constraints facing CSIS with regard to its human source operations when it noted that certain CSIS operations abroad could have been in contravention of the Regulations Implementing the United Nations Resolutions on Taliban, ISIL (Da'esh) and Al-Qaida and other similar laws. SIRC then directed CSIS to undertake a wide-ranging review of its own activities for compliance. Later, in the May 27, 2016, review of CSIS's investigation of Canadian foreign fighters, SIRC noted legal risks associated with certain CSIS operations, and recommended that "CSIS seek legal clarification on whether CSIS employees and CSIS human sources are afforded protection under the Common Law rule of Crown Immunity in regards to the terrorism-related offences of the Criminal Code of Canada."

[33] A redacted version of this certificate is available at: http://www.nsira-ossnr.gc.ca/pubpub/cercer/2018-07-eng.html.

[34] *X (Re)*, 2020 FC 616, dated May 15, 2020. h ttps://decisions.fct-cf.gc.ca/fc-cf/decisions/en/item/482466/index.do

[35] See the NSIRA news release dated July 16, 2020, available at: http://www.nsira-ossnr.gc.ca/nwsspr/rlscmq/20200716-eng.html

[36] United States, National Counterintelligence and Security Center (n.d.), "Five Eyes Intelligence Oversight and Review Council (FIORC). https://www.dni.gov/index.php/ncsc-how-we-work/217-about/organization/icig-pages/2660-icig-fiorc

[37] For NSICOP's review of the Canada Border Services Agency, see chapter three of NSICOP's 2019 annual public report, available at https://www.nsicop-cpsnr.ca/reports/rp-2020-03-12-ar/intro-en.html. For DND, refer to chapter four of NSICOP's 2018 annual report, available at https://www.nsicop-cpsnr.ca/reports/rp-2019-04-09/intro-en.html, as well as the special report available at https://www.nsicop-cpsnr.ca/reports/rp-2020-03-12-sr/intro-en.html.

[38] As NSIRA's knowledge on safeguarding themes expands over the coming years, it is expected that reviews in this field will likewise evolve to include applicable government linkages to the private sector, including examination of federally regulated private sector activities impacting people, information and other assets within the national security and intelligence portfolio.

[39] An insider threat is one that comes from people within an organization, such as employees or contractors, who use their access to internal information, assets or systems to carry out unauthorized disclosures.

[40] CBC News (March 8, 2019), "Convicted spy Jeffrey Delisle released on full parole," https://www.cbc.ca/news/canada/nova-scotia/convicted-spy-russians-canadian-armed-forces-parole-1.5049166

[41] CBC News (June 28, 2019), "Case of Hamilton man allegedly spying for China, tangled in secrecy," https://www.cbc.ca/news/canada/hamilton/case-of-hamilton-man-allegedly-spying-for-china-tangled-in-secrecy-1.5193658

[42] Globe and Mail (October 16, 2019), "RCMP senior officers explored appointing Cameron Ortis as a police officer," https://www.theglobeandmail.com/politics/article-rcmp-senior-officers-explored-appointing-cameron-ortis-as-a-police/

[43] The Policy on Government Security took effect on July 1, 2019. It replaced the Policy on Government Security that was in effect from July 1, 2009 to June 30, 2019. Refer to: https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=16578 The Directive on Security Management and its Mandatory Procedures took effect on July 1, 2019 and replaced a number of security related standards/directives. Refer to: https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=32611

[44] This safeguarding standard can also be described as concerned with cyber-security, an issue that NSIRA will cover within multiple reviews of CSE.

[45] Canadian government departments and agencies have a choice for contracts that are within their delegated contracting responsibilities and that involve access to sensitive information and assets. The department can itself ensure that the contractor meets the appropriate security requirements, or request that Public Services and Procurement Canada (PSPC) perform this task through the Industrial Security Program. This program is designed to safeguard Protected and Secret classified information and assets. In cases where contracts fall outside of a department's delegated contracting responsibilities, PSPC has the default responsibility. https://www.tpsgc-pwgsc.gc.ca/aiprp-atip/efvp-pia/prgsecind-indsecprg-eng.html

[46] For example, employees in the security and intelligence community are more likely to undergo robust training and persistent security reminders and are routinely subjected to security audits of their electronic and physical systems and spaces.

[47] Security screening concepts such as immigration screening, airport and border security measures, or traveller watchlists are completely distinct from safeguarding.

[48] See especially section 8 of the *Security of Information Act* (SOIA) on special operational information. https://laws-lois.justice.gc.ca/eng/acts/O-5/index.html#docCont

[49] Section 4 of the SOIA summarizes miscellaneous offences. https://laws-lois.justice.gc.ca/eng/acts/o-5/page-2.html#h-384913

[50] A more in-depth discussion of whistleblower protections can be found in paragraphs 154–157of this report.

[51] Unless there are exigent circumstances, the accused person must exhaust internal avenues before making the disclosure and NSIRA has a role to play in responding to these concerns of wrongdoing.

[52] CBC News (November 29, 2012), "Early clues to navy spy Delisle's guilt overlooked." https://www.cbc.ca/news/canada/early-clues-to-navy-spy-delisle-s-guilt-overlooked-1.1235506

[53] Treasury Board of Canada Secretariat (October 20, 2014), "Standard on Security Screening." https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=28115

[54] NSIRA (August 2019), Review of CSIS's Internal Security Branch.

[55] Treasury Board of Canada Secretariat (October 20, 2014), "Standard on Security Screening." https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=28115

[56] NSIRA letter to TBS, December 12, 2019.

[57] Refer to SIRC annual reports: 1985–86 to 1991–92, http://www.sirc.gc.ca/anrran/index-eng.html

[58] R. v. Béland [1987] 2 SCR 398

[59] OPC, "For federal institutions." https://www.priv.gc.ca/en/for-federal-institutions/

[60] *Security of Canada Information Disclosure Act* (S.C. 2015, c. 20, s. 2). https://laws-lois.justice.gc.ca/eng/acts/S-6.9/index.html

61 These are: Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar (https://www.canada.ca/en/privy-council/services/commissions-inquiry/arar.html), the internal inquiry into the actions of Canadian officials in relation to Abdullah Almalki https://www.publicsafety.gc.ca/cnt/cntrng-crm/plcng/cnmcs-plcng/rsrch-prtl/dtls-en.aspx?d=PS&i=73612699), Ahmad Abou-Elmaati and Muayyed Nureddin, and the Commission of Inquiry into the Investigation of the Bombing of Air India Flight 182 https://www.securitepublique.gc.ca/cnt/rsrcs/lbrr/ctlg/dtls-en.aspx?d=PS&i=85557953). See also the deliberations of the Special Committee on the Canadian Mission in Afghanistan.

62 See, for example, "Case Studies Regarding CSIS Information Sharing with Foreign Entities" in SIRC's 2017–18 annual report, Building For Tomorrow: The Future Of Security Intelligence Accountability In Canada (http://www.sirc-csars.gc.ca/anrran/2017-2018/index-eng.html#section_2_2) and OCSEC's "Annual Review of CSE Disclosures of Canadian Identity Information" in its 2018–19 annual report (https://www.ocsec-bccst.gc.ca/s21/s85/d445/eng/highlights-reports-submitted-minister#toc-tm-3).

63 Commission of Inquiry into the Investigation of the Bombing of Air India Flight 182 (June 16, 2010). https://www.canada.ca/en/privy-council/services/commissions-inquiry/arar.html

64 Consultation on National Security, available at https://www.canada.ca/en/services/defence/nationalsecurity/consultation-national-security.html; and its supporting background document Our Security, Our Rights: National Security Green Paper, 2016, available at: https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-scrt-grn-ppr-2016/index-en.aspx

65 The *Privacy Act* sets out a series of circumstances where personal information collected by federal departments and agencies can be shared without the consent of the individual concerned. Many of these pertain to information sharing in the national security context. The "consistent use" provision allows personal information to be disclosed "for the purpose for which the information was obtained or compiled by the institution or for a use consistent with that purpose." It provides government institutions with flexibility to operate effectively within their mandates.

66 Security Intelligence Review Committee (2017), SIRC Annual Report 2016-2017: Accelerating Accountability, "Section 2: Reviews," The *Security of Canada Information Sharing Act*. http://www.sirc-csars.gc.ca/anrran/2016-2017/index-eng.html#section_2_8

67 OPC (2017), Review of the Operationalization of the *Security of Canada Information Sharing Act.* https://www.priv.gc.ca/en/opc-actions-and-decisions/audits/ar-vr_scisa_2017.

68 Caveats are limitations on use attached to intelligence products that are shared with partners. For example, one caveat stipulates that the information being shared is for intelligence purposes only and should not be used in a prosecution or shared with other agencies without the consent of the originator; this is known as the Third Party Rule. Non-caveated information thus attaches no limits.

69 See CSIS's 2018 Public Annual Report for more information on the Information Sharing and Evaluation Committee, under "Human Rights Considerations." https://www.canada.ca/en/security-intelligence-service/corporate/publications/2018-public-report/the-confidence-of-canadians.html#tocc5

70 On September 4, 2019, the Governor in Council, on the recommendation of the Minister of Finance, issued Directions for Avoiding Complicity in Mistreatment by Foreign Entities (Directions) to 12 departments and agencies via an Order in Council (OIC). The OIC prohibits any sharing of information that would result in a substantial risk of mistreatment of an individual, as well as certain uses of information that likely was obtained through the mistreatment of an individual.

71 On September 17, 2020, NSICOP launched a review of the government's cyber defence activities. https://www.nsicop-cpsnr.ca/press-releases/pr-cp-2020-09-17/pr-cp-2020-09-17-en.html

72 In July 2019, the coming into force of the *National Security Act, 2017*, modified CSIS's threat reduction powers. Changes to the threat reduction power included new restrictions on the types of threat reduction measures (TRM) that can be pursued; the requirement to consult other federal departments and agencies in respect of their ability to reduce the threat; clarifying when a proposed TRM requires a warrant; and, as part of the reasonable and proportional standard, that CSIS consider the foreseeable effects a TRM could have on the rights of third parties. Furthermore, CSIS must now notify NSIRA of any TRMs that it undertakes.

73 The CSE Act prohibits CSE from using ACO/DCO to intentionally, or by criminal negligence, cause death or bodily harm, or wilfully attempt to obstruct, pervert or defeat the course of justice or democracy. Moreover, CSE is also prohibited from using ACO/DCO to collect information. Under the governing statutory framework, it also seems likely that ACO/DCO activities undertaken by CSE must accord with relevant international law.

[74] More information on the Intelligence Commissioner's role with regard to ministerial authorizations is available at: https://www.canada.ca/en/intelligence-commissioner.html.

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

[76] Section 18 of the RCMP Act establishes that the duties of RCMP officers include the enforcement of laws and the execution of warrants, as well as the "preservation of the peace" and "the prevention of crime."

[77] Action in this context does not include: actions taken throughout the intelligence process; intelligence products such as briefings, reports and recommendations; and safeguarding actions taken to protect classified information.

[78] NSIRA also has the obligation to review complaints that have been referred by the Canadian Human Rights Commission (CHRC), as well as following minister's reports pursuant to the *Citizenship Act*. These instances are very rare, however.

[79] For more information about NSIRA's complaints investigation process, including how to make a complaint, please see NSIRA (2020), "Complaints." http://www.nsira-ossnr.gc.ca/cmpplt/index-eng.html.

[80] For a statistical breakdown, please see Annex D.

[81] Investigations of complaints against CSIS which NSIRA determined it had jurisdiction

to investigate are summarized in Annex C.

[82] *Public Servants Disclosure Protection Act* (SC 2005, c. 46). https://laws-lois.justice.gc.ca/eng/acts/P-31.9.

[83] *Public Servants Disclosure Protection Act* at 2(1).

[84] See section 15(1) of SOIA.

[85] See section 15(1) of SOIA.

[86] See section 15(5) of SOIA.

[87] [Insert date of letter to Attorney General. It is also be worth noting whether we received a reply.]

[88] Parliament of Canada (2019), "Bill C-59."
https://www.parl.ca/DocumentViewer/en/42-1/bill/C-59/royal-assent

[89] Canada (2020), "National Security Transparency Commitment."
https://www.canada.ca/en/services/defence/nationalsecurity/national-security-transparency-commitment.html

[90] NSIRA [@NSIRACanada] https://twitter.com/nsiracanada?lang=en

[91] This process is currently under way, and redacted reports will become available on the NSIRA website at: http://www.nsira-ossnr.gc.ca/

[92] Feedback can be sent to NSIRA's corporate inbox available at: NSIRA (2020), "Contact Us."
http://www.nsira-ossnr.gc.ca/cttctz-eng.html

[93] All of NSIRA's corporate reporting is available at: NSIRA (2020), "Corporate Services."
http://www.nsira-ossnr.gc.ca/abtprp/cormin-eng.html