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

Canada

NSIRA

2020 // Annual Report

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

October 18, 2021

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 second annual report. Consistent with subsection 38(1) of *the National Security and Intelligence Review Agency Act*, the report includes information about our activities in 2020, as well as our findings and recommendations.

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

Yours sincerely,

The Honourable Marie Deschamps, C.C.

Chair
National Security and Intelligence Review Agency

Table of contents

Message from the members

The National Security and Intelligence Review Agency (NSIRA) began operating in 2019 as a new independent accountability mechanism in Canada. Our broad review and investigations mandate covers the national security and intelligence activities of departments and agencies across the federal government. In our first annual report, released in 2020, we discussed our initial activities from our inception in July 2019 to December 2019.

We are pleased to now present our second annual report, covering our activities in our first full year of operation. In 2020, we completed numerous reviews and investigations, engaged with stakeholders in the national security and intelligence community, including our international counterparts, launched an ambitious review plan for the coming years, initiated a comprehensive reform of our complaints investigation process, developed a uniform approach to information verification in reviews (our "trust but verify" approach), began standardizing our review processes, and made strides in formalizing efforts to coordinate and collaborate with various partner organizations. NSIRA's Secretariat also continued to grow steadily in size, expertise, and administrative, technical, and substantive capacity. We achieved all of this within the considerable constraints presented by the COVID-19 pandemic.

We are committed to transparency and public engagement, striving to keep Canadians informed about national security and intelligence activities, and ensure our plans reflect the priorities of all Canadians. Our annual report is one way among many of achieving this. We also aim to achieve this through regularly engaging with stakeholders, members of diverse communities, and parallel review bodies internationally, including those that comprise the Five Eyes Intelligence Oversight and Review Council (FIORC). We are likewise committed, and have began to, releasing public versions of our reports as they are completed (our "write for release" initiative), and to provide timely updates via our website and social media platforms.

After the release of our inaugural annual report, we sought and received feedback from academic and community stakeholders. As a result of these consultations, we have reorganized how we present some of the material in our 2020 annual report. In particular, we have grouped our review summaries, including any findings and recommendations, according to the institutions to which they pertain. We also discuss the outcomes and themes of interagency reviews. As well, this report sets out a framework for more robust statistical reporting on certain aspects of the activities of the Canadian Security Intelligence Service and the Communications Security Establishment activities, to enable year-to-year comparisons.

The pandemic delayed our plans and progress on reviews, investigations, and corporate initiatives in 2020, as was the case for many industries and sectors around the world. As of writing, our staff has begun to have more regular access to our offices and to the classified material critical to our work. More frequent and sustained access will help us conduct our work in a more timely and efficient manner. We look forward to carrying out an ambitious agenda in the year ahead.

We wish to extend our sincere thanks to our NSIRA staff for their dedication and diligence over the past challenging year, and for their continued efforts to build a strong organization.

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

Executive summary

1. The National Security and Intelligence Review Agency (NSIRA) marked its first full year in operation in 2020. With the agency's broad jurisdiction under the *National Security and Intelligence Review Agency Act* (NSIRA Act), it reviewed and investigated national security and intelligence matters relating to not only the Canadian Security Intelligence Service (CSIS) and the Communications Security Establishment (CSE), but also several federal departments and agencies, including:
    - the Department of National Defence (DND) and the Canadian Armed Forces (CAF);
    - Global Affairs Canada (GAC);
    - the Royal Canadian Mounted Police (RCMP);
    - Immigration, Refugees and Citizenship Canada (IRCC);
    - the Canada Border Services Agency (CBSA);
    - Transport Canada;
    - the Public Health Agency of Canada; and,
    - all departments and agencies engaging in national security and intelligence activities in the context of NSIRA's yearly reviews of the *Security of Canada Information Disclosure Act* and the *Avoiding Complicity in Mistreatment by Foreign Entities Act*.
2. The agency also focused on standardizing and modernizing the processes that govern the two main functions under NSIRA's mandate—reviews and investigations—to ensure that our processes are robust, clear, and transparent.
3. The year 2020 also saw the organization grow in size and capacity, as it continues efforts to enhance its technical and subject-matter expertise.

Review highlights:

Canadian Security Intelligence Service

4. Over the course of 2020, NSIRA completed two reviews that strengthened its knowledge of important areas of CSIS activity:
    - The review of CSIS's threat reduction measures (TRM) found that CSIS met its obligations under ministerial direction. However, in a limited number of cases, CSIS's TRMs were not "reasonable and proportional."

- The review of CSIS and RCMP intelligence-sharing through the lens of an ongoing investigation shed light on an important unresolved issue in Canada's national security framework: the limitations on the use of CSIS intelligence to support RCMP criminal investigations, also known as the "intelligence-to-evidence" dilemma.

Communications Security Establishment

5. NSIRA completed three reviews of CSE activities in 2020, including of:
    - CSE's disclosure of Canadian identifying information (CII) to Government of Canada (GC) departments, which found that 28% of requests for disclosure were insufficiently justified to warrant the release of CII;
    - ministerial authorizations (MAs) and ministerial orders (MOs) under the CSE Act, which allow CSE to engage in activities that would otherwise be unlawful, to support its mandate; and
    - CSE's signals intelligence (SIGINT) data retention policies and procedures, to better understand the SIGINT lifecycle management process and compliance with legal data retention limits and related government and internal policies.

Department of National Defence and the Canadian Armed Forces

6. In 2020, NSIRA completed a review of DND/CAF, which examined how the Canadian Forces National Counter-Intelligence Unit (CFNCIU) conducted its counter-intelligence gathering activities—focusing particularly on how the unit's activities corresponded with legal and governance frameworks.

Global Affairs Canada

7. In 2020, NSIRA completed its first dedicated review of Global Affairs Canada (GAC) focusing on one of its programs.

Other departmental reviews

8. NSIRA also began reviews regarding a specialized RCMP intelligence unit, to better understand the national security role and responsibilities of Immigration, Refugees and Citizenship Canada, and a review of air passenger targeting at the Canada Border Services Agency.

Cross departmental reviews

9. NSIRA conducted two mandated cross-departmental reviews in 2020:
    - a review of directions issued with respect to the Avoiding Complicity in Mistreatment by Foreign Entities Act; and
    - a review of disclosures of information under the *Security of Canada Information Disclosure Act* (SCIDA); and
10. NSIRA also began another cross-departmental review in 2020:
    - a review to map the collection and use of biometrics across the federal government in security and intelligence activities.

Investigation highlights:

11. In 2020, NSIRA reformed and modernized its complaints process to promote efficiency and transparency. Two priorities guided this process of modernization, namely, promoting access to justice for self-represented complainants, and putting in place more streamlined and less formal procedural steps.
12. As part of this reform process, NSIRA created new Rules of Procedures, completing an extensive consultation exercise with stakeholders in the public and private sectors to ensure the most effective and considered final product. The new rules have come into force on July 19, 2021.
13. NSIRA also developed a new policy statement in 2020 that commits to publishing redacted and de-personalized investigation reports to promote and enhance transparency in its investigations.

01 //

Introduction

1.1 Who we are

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

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

1.2 Mandate

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

Reviews

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

security or intelligence matters that a minister of the Crown refers to NSIRA. Annex C describes NSIRA's review framework.

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

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

Investigations

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

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

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

1.3 Annual Reports to Parliament

9. Each calendar year, NSIRA has a statutory obligation to submit to the Prime Minister a report on its activities in the preceding year, along with its findings and recommendations.[4]

2019 Annual Report

10. NSIRA's first annual report (2019 Annual Report) covered the six-month period from July 2019 when NSIRA was established, through to the end of 2019. In that report, the agency discussed the reviews and investigations that it had either completed or launched in 2019, with the accompanying findings and recommendations. It also published the results of reviews that had not yet been made public by its predecessor organizations, the Security Intelligence Review Committee (SIRC) and the Office of the Communications Security Establishment Commissioner (OCSEC).[5]

11. The *2019 Annual Report* also presented NSIRA's review findings through a novel framework called the "information continuum." Given the agency's comprehensive, overarching review mandate, this framework offers a lens for understanding key national security- and intelligence-related themes, trends and challenges that are common to departments and agencies across the federal government. This lens allows for discussing shared concerns in Canada's overall security and intelligence architecture, and informs future review priorities and the recommendations for addressing them. The information continuum is discussed further in section 2.1 below.[6]

2020 Annual Report

12. In response to feedback received from stakeholders, NSIRA's second annual report groups the review summaries according to government department, including for CSIS and CSE. Nevertheless, NSIRA continues to be committed to presenting broader themes and observations on national security and intelligence accountability across Canada.

13. In the 2020 *Annual Report*, NSIRA therefore presents:

    - its "trust but verify" approach, developed to ensure it has timely access to all relevant information when conducting department and agency reviews;
    - an update on the agency's plans to continue presenting review analyses through the information continuum lens;
    - summaries of NSIRA's completed and ongoing reviews of CSIS, CSE, and other government departments and agencies in 2020, with background in the next section and summarized in Annex D, as well as detailed findings and recommendations listed in Annex E;[7]
    - data on CSE and its compliance-related activities, to promote greater transparency in these matters;

- NSIRA's plans for upcoming department and agency reviews, including to inform the three-year mandated parliamentary review of the *National Security Act, 2017*, that is expected to begin in 2022;
- summaries of complaints investigations completed and ongoing in 2020;
- an outline of the agency's new, modernized complaints process, the result of an extensive reform initiative; and,
- statistics on NSIRA's complaints investigations in 2020 in Annex F.

1.4 Values and goals

14. NSIRA is committed to:

    - being open and transparent, to keep Canadians informed about the lawfulness and reasonableness of our country's national security and intelligence activities;
    - anticipating the various risks that are part of each of the reviewed entities' mandate;
    - being, as well as being seen to be, objective and independent;
    - maintaining methodological excellence, to ensure the rigour and quality of NSIRA's approach;
    - engaging regularly with partners, stakeholders, and community members; and,
    - fostering forward- and innovative-thinking, to keep abreast and, ideally, stay ahead of new technology and an ever-changing national security environment.

15. As part of a commitment to methodological excellence, NSIRA developed its "trust but verify" approach (highlighted below) to provide an important measure of confidence in the completeness of information received from departments and agencies.

16. In 2020 the NSIRA Secretariat also began work to develop a Code of Conduct for all employees, which was finalized in June 2021. The Code sets out the organizational values that guide the workforce's activities and functions and the expected standards that must be observed during and after a person's employment with the NSIRA Secretariat.[8]

17. Additional details on NSIRA's values and goals related to transparency, anticipation of risk, objectivity and independence, methodological excellence, stakeholder and community engagement, and forward- and innovative-thinking can be found in Annex G.

1.5 Trust but verify

18. The *NSIRA Act* grants the agency extensive access rights to information: with the exception of Cabinet confidences, NSIRA is entitled to have access in a timely manner to any information in the possession or under the control of any department. In conducting reviews and investigations, it requires timely access to a wide range of information, people, and assets. This, in turn, requires regular support from expert liaison units that can provide documentation, arrange briefings, answer questions, and generally guide and implement NSIRA's access requirements. NSIRA's ability to fulfil its mandate can be challenged when it faces delays in receiving information.

19. As a review agency, NSIRA must be able to assure Parliament — and through it, Canadians — that it has a high level of confidence in the completeness of the information received from departments and agencies, and hence, in the robustness of its findings. The "trust but verify" approach is a critical tool for reaching this objective.

20. NSIRA recognizes, on the one hand, that the principle of trust requires each party to understand and appreciate the mandate, and feel confident in the integrity, of the other. Of course, in a review relationship there will necessarily be healthy tensions stemming from differences in perspective.

21. On the other hand, verification is a fundamental prerequisite of any credible review. NSIRA must be able to independently test the completeness of the information it receives.

22. Moving forward, NSIRA will implement a "tailored access" process for conducting verification. Tailored access involves identifying its information access needs in response to the specific review or investigation and collaborating with departments and agencies in determining the various types of access that will constitute the best manner in which to obtain that information. The tailored access process may include targeted access of computer networks and information, proxy access, dedicated office space, and access to training materials.

    - Targeted access constitutes direct access to a department's or agency's computer networks and/or sensitive information. Targeted access is the gold standard for ensuring a robust verification of information received as part of the trust but verify approach.
    - Proxy access involves a departmental or agency intermediary who accesses information repositories in the presence of NSIRA staff, and who can review relevant information as it appears on the system.

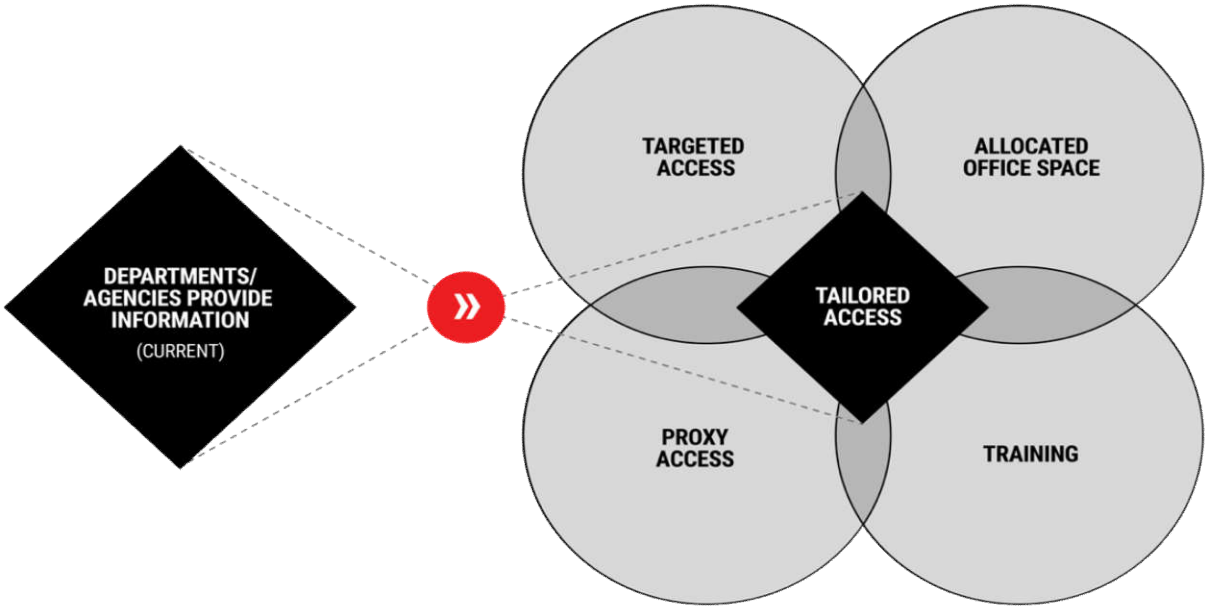
- Allocated office space at departments or agencies, either temporary or permanent, enables more expedient and secure exchanges of information.
- Access to training requires access to departmental or agency training modules relating to relevant corporate policies and other matters, to allow NSIRA to build specific knowledge.

23. The tailored access processes can place logistical and resource strains on departments and agencies having to implement them, and may require a shift in culture. Overall, however, tailored access provides mutual benefits. Tailored access processes can increase transparency and accountability on all sides, allow information to be accessed in a more secure and timely manner, foster positive professional interactions, improve overall expertise, and strengthen evidence-based findings and recommendations. Moreover, NSIRA believes that tailored access will, over time, result in a reduced workload for liaison staff at departments and agencies under review.

24. The trust but verify approach is not new. Both NSIRA and its predecessor, SIRC, have already had long-standing tailored access arrangements with CSIS that include targeted (direct) access to CSIS's computer networks and sensitive information.

25. The trust but verify principle is a key aspect of maintaining the integrity and credibility of NSIRA's reviews. In keeping with the commitment to transparency and methodological rigour, its reviews will contain a "confidence statement" to report NSIRA's confidence level in the completeness of the information on which the findings rely, given agency's ability to verify. The confidence statement is an important tool for apprising ministers, Parliament, and members of the public on the extent to which NSIRA has been able to access all relevant information.

Fig. 1 Tailored access



02 //

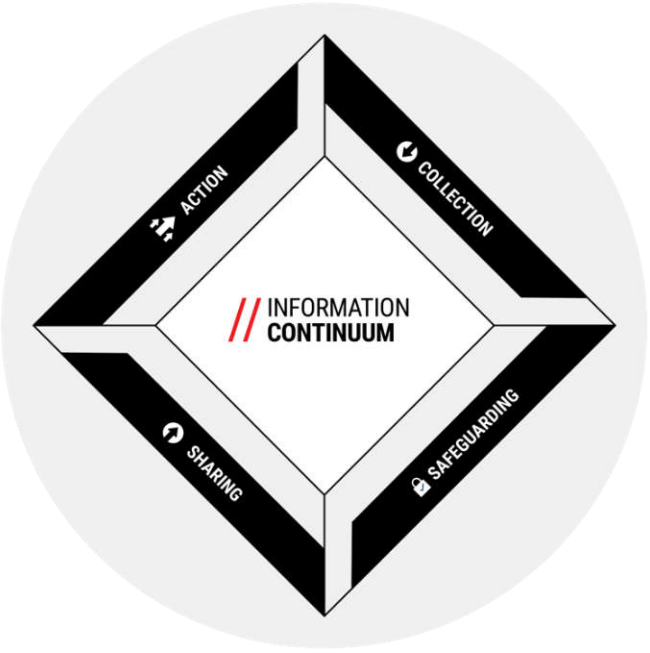
Review

2.1 The information continuum

1. As previously mentioned, NSIRA's review mandate extends throughout the federal government. NSIRA's broader jurisdiction allows it not only to examine the national security and intelligence activities of a specific organization, but also to identify common themes that emerge across government.

2. In the *2019 Annual Report*, NSIRA introduced a framework to assist in discussing and analyzing such trends. The "information continuum" identifies four main stages in the lifecycle of national security and intelligence information where problems can arise, including in information collection, safeguarding, sharing, and use in real-world actions.[9]

Fig. 2 Information continuum



3. In an environment that is constantly changing, including the rapid development of new technologies, each stage presents potential challenges for departments and agencies engaging in national security and intelligence activities. Despite the challenges, all national security and intelligence activities must comply with the law and applicable ministerial directions, and meet the tests of reasonableness and necessity.

4. The *2019 Annual Report* also identified a number of future priorities that would benefit from analysis through the lens of the information continuum. To achieve these goals, NSIRA promised to invest in building in-house technological expertise, collaborate with allied accountability bodies through the Five Eyes Intelligence Oversight and Review Council, and seek to stay current with new and emerging technologies such as artificial intelligence, machine learning, quantum computing, and "big data."

5. NSIRA also pledged to continue to work with the Office of the Privacy Commissioner (OPC) and the National Security and Intelligence Committee of Parliamentarians (NSICOP) on matters of joint concern to ensure the broadest range of perspectives are addressed.

6. NSIRA continues to examine national security and intelligence activities through the lens of the information continuum, and plans on presenting work on its website using the continuum approach to help situate horizontal themes for national security review. For 2020, however, this report builds on some feedback NSIRA received on last year's annual report and uses a more institutional approach as a narrative device.[10]

2.2 Reality of review during a pandemic

7. As noted in the *2019 Annual Report*, NSIRA staff continued to work remotely in 2020, which meant limited office access and, therefore, minimal access to the classified physical and electronic documents that must be protected in a secure environment, and that are critical to NSIRA's work. Just as all organizations have had to adapt to the realities of the pandemic, so has NSIRA. It revised its review plans, and implemented strict rotating schedules to enable limited office access for classified work to safely continue to fulfill its statutory obligations and uphold its commitments to Canadians.

2.3 Parliamentary review of the *National Security Act, 2017*

8. The omnibus *National Security Act, 2017*, which established NSIRA and made major changes to Canada's national security framework, contains provisions mandating a review by Parliament during NSIRA's fourth year of operation, which will be in 2022.

This comprehensive review will require Parliament to assess the effects of the *National Security Act, 2017*, on the operations of the Canadian Security Intelligence Service (CSIS), the Royal Canadian Mounted Police (RCMP) and the Communications Security Establishment (CSE) that relate to national security, information sharing, and the interaction of those organizations with NSIRA, the Office of the Intelligence Commissioner and NSICOP.[11]

9. NSIRA has structured and sequenced its review plan in order to inform Parliament's examination of new powers granted to security agencies through the *National Security Act, 2017*. Reviews of these new powers will take place over the course of 2021 and into early 2022, to determine whether they were exercised in compliance with the law and ministerial direction, and whether they were reasonable and necessary.

2.4 CSIS reviews

Overview

10. Under the *NSIRA Act*, NSIRA has a mandate to review any CSIS activity. The Act requires NSIRA to submit an annual report to the Minister of Public Safety and Emergency Preparedness on CSIS activities each year, including information related to CSIS's compliance with the law and applicable ministerial directions, and the reasonableness and necessity of the exercise of CSIS's powers.[12]

11. In 2020, NSIRA completed two CSIS reviews, summarized below. NSIRA also began two more reviews: a review of CSIS's technology programs and intelligence collection techniques, and a review of the duty of candour owed by both CSIS and the Department of Justice in warrant proceedings before the Federal Court. Other NSIRA ongoing reviews, including multiple agency reviews, have a CSIS component.

Threat reduction measures

12. Under the *Anti-terrorism Act, 2015,* CSIS was granted the authority to undertake threat reduction measures (TRMs). NSIRA is required to review, annually, at least one aspect of CSIS's performance in using its threat reduction powers.[13]

13. This was NSIRA's first review of CSIS's threat reduction mandate. It included a detailed compliance review of a sample of TRMs from 2019. The review also included a high-level analysis of CSIS's use of TRMs over the past five years to identify trends and to inform NSIRA's choice of future review topics.

14. The sample reviewed by NSIRA consisted of TRMs that were employed to disrupt threats to Canadian democratic institutions in relation to the 2019 federal election. NSIRA assessed the measures against legislative and policy requirements, as well as ministerial direction.

15. For all the measures reviewed, NSIRA found that CSIS met its obligations under ministerial direction, namely that CSIS consulted with its government partners and completed an assessment of the operational, political, foreign relations and legal risks of each TRM.

16. For most of the measures taken by CSIS, NSIRA noted that the measures satisfied the requirements of the *Canadian Security Intelligence Service Act (CSIS Act)*. NSIRA also noted, however, that in a limited number of cases, CSIS selected individuals for inclusion in the TRM without a rational link between the selection of the individual and the threat. As a result, these measures were not "reasonable and proportional" as required under the *CSIS Act*.[14]

17. For one type of TRM reviewed by NSIRA, CSIS deemed that a warrant was not required. NSIRA identified concerns about factors which would require CSIS to consider fully the implications of the Canadian Charter of Rights and Freedoms for its measures, and could require CSIS to obtain warrants before taking certain measures.

18. Finally, NSIRA noted some inconsistencies in the type of information provided to CSIS decision-makers in its internal requests for approval. NSIRA also found gaps and inconsistencies in CSIS's documentation, which had the effect of hindering NSIRA's compliance review. As a result, NSIRA recommended that formalized and documented processes be developed for the management of all TRM-related information. In addition, NSIRA recommended that all pertinent facts relating to the TRM be formally provided to the National Security Litigation and Advisory Group (NSLAG), which is part of the Department of Justice, to ensure that the NSLAG has the information necessary to provide considered legal advice.

19. The legal issues and questions raised in this review, as well as the analysis of trends across the last five years, point the way to further reviews by NSIRA. In particular, NSIRA was struck by the potential for a class of TRMs to affect rights and freedoms protected under the Charter. In future, NSIRA will pay particular attention to this class of TRMs and the associated legal risks. NSIRA also notes that CSIS has yet to undertake a TRM under the authority of a court warrant. If and when CSIS obtains a TRM warrant, NSIRA will prioritize it for review.

Response to NSIRA's recommendations

20. NSIRA's recommendations, CSIS' management responses, and other details about this review, are found in Annex E of this report.

CSIS-RCMP relationship in a region of Canada through the lens of an ongoing investigation

21. CSIS and the RCMP must work together and share intelligence to effectively counter national security threats.[15] NSIRA examined the state of the relationship between CSIS and the RCMP through the lens of an ongoing investigation in a specific region of Canada. NSIRA undertook an in-depth study of both agencies' operations, with particular attention to how the two agencies collaborated on this investigation in recent years, both in this region and at headquarters. Although the findings of this review are specific to the given investigation, NSIRA has no reason to believe that the investigation in question is atypical, and thus this review provides insight into the more general state of the two agencies' relationship.

22. With respect to CSIS's investigation specifically, NSIRA found that CSIS was reliant on a narrow set of information and was thus vulnerable; NSIRA observed how external factors arose that sharply limited CSIS's ability to collect intelligence on the threat in question, resulting in collection gaps.

23. NSIRA found that in the specific region in question, CSIS and the RCMP had developed a strong relationship that has fostered effective tactical de-confliction of operational activities. Nonetheless, technological constraints made CSIS-RCMP de-confliction in the region excessively burdensome and time-consuming.

24. The RCMP's use of CSIS information in support of criminal prosecutions has long been limited by perceived risks of involving CSIS or CSIS information in a prosecution. As an element of this, NSIRA observed a general reluctance on the parts of both CSIS and the RCMP to connect CSIS information to an RCMP investigation. In the case of the regional investigation in question, CSIS intelligence had not been shared or used in a way that significantly advanced the RCMP's investigations.

25. On the whole, NSIRA found that CSIS and the RCMP had made little progress in addressing the threat under investigation. Moreover, CSIS and the RCMP did not have a complementary strategy to address the threat.

26. NSIRA has the legal authority to assess CSIS-RCMP activities from the perspective of both parties, and is not limited to the standpoint of CSIS, as was the case for the

Security Intelligence Review Committee (SIRC). This regional review exposed an important, yet unresolved, issue in Canada's national security framework: the limitations on the use of CSIS intelligence to support RCMP criminal investigations, often termed the "intelligence-to-evidence" dilemma. Given the centrality of the CSIS-RCMP relationship to Canada's national security architecture, NSIRA will return to this topic in future years.

Response to NSIRA's recommendations

27. NSIRA's recommendations, CSIS' management responses, and other details about this review, are found in Annex E of this report.

Statistics and data

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

    The number of section 21 warrant applications (a) approved, and (b) denied; each further broken down as either new or replacement/supplemental.

    - Number of section 21 warrant applications approved: 15
    - New: 2
    - Replacement: 8
    - Supplemental: 5
    - Number of section 21 warrant applications denied: 0

    The number of section 21.1 warrant applications (a) approved, and (b) denied; each further broken down as either new or replacement/supplemental.

    - There were no warrant applications under section 21.1.

    The number of CSIS targets

    - 360 targets

    The number of publicly available datasets (a) evaluated, and (b) retained.

    - Six section 11 PADs were evaluated and retained.

    **Note that one had been collected in late 2019 but was evaluated in 2020.*

The number of Canadian datasets (a) evaluated, and (b) retained after authorization by the Court, and the number of such requests denied.

- There were zero Canadian datasets evaluated, subject to a request, or retained in calendar year 2020.

The number of foreign datasets (a) evaluated, and (b) retained after approval by the Minister and Intelligence Commissioner, and the number of such requests denied (by either the Minister or Intelligence Commissioner).

- There were zero foreign datasets evaluated in calendar year 2020. (All pending submissions were evaluated in 2019.)
- There was one foreign dataset retained after authorization by the Minister (Director as designate, November 18, 2020) and approval by the Intelligence Commissioner (December, 16, 2020) in calendar year 2020. (It was evaluated in 2019.)
- There were no requests for foreign datasets denied by the Minister or Intelligence Commissioner in calendar year 2020.

The number of TRMs (a) approved, and (b) executed.

- Approved: 11
- Executed: 8

The number of Justification Framework (a) approvals, and (b) invocations.

- Emergency designations made under section 20.1(8): 0
- Authorizations given under section 20.1(12): 147
- Written reports submitted under section 20.1(23): 123 (this includes 39 commissions by employees and 84 directions)

The number of internal CSIS compliance incidents.
In 2020, External Review and Compliance processed 50 compliance incidents. Of these, 29 were considered to be administrative, 14 related to warrant terms and conditions, and 7 related to internal policies, procedures or directives.

General compliance challenges: Outdated operational policies

29. As legal and operational environments have evolved over the years, the suite of internal policies and procedures governing CSIS operations has drifted out of date. These operational policies and procedures translate the limits imposed by law and ministerial directions into everyday practice for CSIS activities.

30. NSIRA, and previously SIRC, noted concerns with out-of-date policies and procedures in reports and reviews over the years. CSIS also recognizes these concerns, but has struggled to adequately resource and prioritize the renewal of its operational policy suite. The result is a confusing collection of old and new policies, and *ad hoc* directives that have not yet been incorporated into policy. Over the past two years, CSIS has reported that more than 150 of its operational policy related documents need to be developed, updated, or significantly revised.

31. Written policies and procedures that do not reflect current operational realities and legal requirements—or are simply not internally consistent—elevate the risk that CSIS will not comply with the law and ministerial directions. CSIS employees should always have a clear, consistent and up-to-date suite of policies and procedures that makes compliance easy.

32. NSIRA is aware of CSIS' ongoing efforts to overhaul and organize its full range of operational policies and procedures. Since the backlog has persisted for years, it remains unclear whether the latest efforts at renewal are sufficiently well-resourced to truly remedy the situation in a timely manner.

Internal compliance and proactive disclosure to NSIRA

In 2020, CSIS proactively disclosed to NSIRA a compliance issue related to certain operational activities. After CSIS employees raised concerns about an operational program, CSIS conducted an internal compliance review. The initial review focused on compliance with CSIS policies and procedures, but as the issue was explored CSIS opted to conduct a legal assessment as well. CSIS has since taken a number of steps to address the shortcomings it identified, including improved operational governance and management accountability. NSIRA received a comprehensive briefing on the matter in early 2021; CSIS is also providing, and has committed to continue to provide, NSIRA with the full range of relevant internal documents. NSIRA is examining this material with interest and will follow up with CSIS as appropriate.

This incident illustrates how departmental compliance mechanisms and NSIRA's external review mandate can complement each other. NSIRA encourage CSIS to continue to engage the agency when internal compliance issues of note are uncovered.

2021 CSIS review plan

33. In 2021, NSIRA is commencing or conducting three reviews exclusively focused on CSIS, one review focused on CSIS and the Department of Justice and a number of interagency reviews with a CSIS component. The reviews are summarized below.

34. In addition to NSIRA's two legally mandated reviews of the *Security of Canada Information Disclosure Act* and the *Avoiding Complicity in Mistreatment by Foreign Entities Act*, NSIRA has initiated or is planning the following CSIS reviews, for completion in 2021:

Survey of new technology programs and intelligence collection techniques

This review, initiated in 2020, involves a broad survey of CSIS's technology programs and intelligence collection techniques, with a particular focus on those that require authorization by court warrant. The review will help to identify specific technologies or investigative techniques that merit future review due to their novelty, potential intrusiveness, or potential for posing risks to compliance. Once identified, these technologies or techniques will be reviewed over subsequent years to ensure legal compliance.

Review arising from the Federal Court's judgment in 2020 FC 616

This review arises from the Federal Court's judgement in *2020 FC 616*.[16] To fully identify systemic, governance and cultural shortcomings and failures that may have led to the breach noted by the Court, NSIRA has undertaken an extensive program of document review and briefings involving both CSIS and the Department of Justice. NSIRA is also conducting confidential interviews with CSIS and Department of Justice employees, at various levels, to better understand the dynamics shaping decision-making in both departments and the interactions between the departments. In addition, NSIRA has consulted with external experts where possible. This review is distinct from other reviews NSIRA has conducted, as it is led by two NSIRA members: Marie Deschamps and Craig Forcese. The final report is expected to be completed in late 2021 or early 2022.

35. Beyond 2021, NSIRA intends to explore CSIS reviews of topics including, but not limited to:

- ministerial direction issued to CSIS;
- CSIS intelligence collection relating to foreign interference;
- CSIS datasets; and
- CSIS's justification regime for intelligence collection activities.

Access

36. The range of information that CSIS must proactively inform NSIRA about has expanded under amendments to the *CSIS Act*. NSIRA must be informed about matters that include CSIS's use of datasets, threat reduction measures, disclosures of information, and the new justification framework for otherwise unlawful activities. Since these requirements are embedded in the *CSIS Act*,[17] it is NSIRA's understanding that Parliament intended that NSIRA keep itself continuously apprised of these activities. To this end, NSIRA will systematically monitor the information received from CSIS for its compliance with the law, and the reasonableness and necessity of those activities.

37. However, NSIRA considers it vital that CSIS also keep NSIRA informed of those activities beyond those that CSIS is explicitly required to bring to NSIRA's attention. NSIRA is working with CSIS to establish a process that builds on NSIRA's existing direct access to CSIS's main databases. This process will enable NSIRA to obtain additional information that complements the information that CSIS is required to report to NSIRA.

38. This endeavour will not only strengthen the content of NSIRA's public annual reporting, but will also better inform the annual classified report on CSIS that NSIRA must provide to the Minister of Public Safety and Emergency Preparedness.[18]

39. CSIS has been subject to independent review since its creation in 1984. To manage its relationship with external review bodies, CSIS has long maintained a dedicated review secretariat, which is currently housed within its External Review and Compliance branch. CSIS's review secretariat has enhanced its ability to meet its statutory obligations to provide NSIRA with timely access to the information NSIRA deems relevant. In 2020, NSIRA was generally satisfied with its access to CSIS.

40. During this reporting period, CSIS personnel have remained supportive and available to the extent possible, and in several instances in 2020, went to exceptional lengths to assist NSIRA is completing reviews whose timelines had themselves been disrupted by COVID-19. Although CSIS and NSIRA may disagree on specific issues — as is to be expected with regard to an external accountability body — NSIRA is of the view that the continued cooperation of CSIS personnel under difficult circumstances reflects an underlying understanding of and respect for the role of independent review at CSIS.

2.5 CSE reviews

Overview

41. As set out in the *NSIRA Act*, NSIRA has a mandate to review any CSE activity. Under the NSIRA Act, NSIRA must also submit an annual report to the Minister of National Defence on CSE activities each year, including information related to CSE's compliance with the law and applicable ministerial directions, and the reasonableness and necessity of the exercise of CSE's powers.[19]

42. In 2020, NSIRA completed three CSE reviews. This annual report also presents results from a 2019 review that NSIRA was unable to share in the *2019 Annual Report*. NSIRA also initiated three reviews, as discussed below.

43. In meetings with representatives from Canadian civil society and academia, some stakeholders expressed an interest in receiving follow-up information pertaining to reviews conducted under the former Office of the CSE Commissioner (OCSEC).[20] NSIRA remain committed to redacting, translating, and publishing OCSEC historical reviews as resources permit. However, many of OCSEC's reviews are no longer relevant in light of the legislative amendments introduced in 2019 by the *National Security Act, 2017*. Many of OCSEC's recommendations have also been implemented, since they called for changes to the law that were subsequently captured in the *National Security Act, 2017*. As well, any ministerial directions and other instruments issued under the previous legal framework for CSE (*National Defence Act*) are now obsolete, having been reissued under the new authorities.

Disclosure of Canadian identifying information to Canadian partners

44. On June 18, 2021, NSIRA released a public summary of its review of CSE's disclosures of Canadian Identifying information (CII).[21] When CSE conducts foreign signals intelligence (SIGINT) collection, it suppresses any incidentally collected CII in its intelligence reporting to protect the privacy of Canadians and persons in Canada.[22] Nevertheless, the Government of Canada and foreign recipients of these intelligence reports can request the details of this information—including names, email addresses, and IP addresses—if they have the legal authority and operational justification to receive it.

45. In 2020, NSIRA reviewed the lawfulness and appropriateness of CSE's disclosure of CII, focusing on CSE's disclosure of CII to other Government of Canada departments.[23]

This review examined a sample of CSE's CII disclosures from July 1, 2015 to July 31, 2019 containing 2,351 Canadian identifiers, including in the context of assisting CSIS's foreign intelligence collection under section 16 of the *CSIS Act*.[24]

46. NSIRA found that although CSE approved 99% of requests for CII disclosure from its domestic partners, 28% of all requests were not sufficiently justified to warrant the release of CII. As a result, NSIRA concluded that CSE's implementation of the CII disclosure regime lacked rigour, and may not have complied with its responsibilities under the *Privacy Act*. This report therefore constituted a compliance report pursuant to section 35 of the *NSIRA Act*, and was presented to the Minister of National Defence on November 25, 2020.[25]

47. NSIRA also found that CSE's releases of CII collected under section 16 of the *CSIS Act* were conducted in a manner that was unlikely to have been communicated to the Federal Court by CSIS. CSIS had provided the Federal Court with testimony about its treatment of information about Canadians collected through section 16 of the CSIS Act. Yet, when NSIRA compared this testimony with how CSE handled information about Canadians collected when assisting CSIS in relation to section 16, NSIRA found notable discrepancies in the standards communicated to the Federal Court. CSIS was not involved in assessing or releasing the disclosures about which NSIRA had concerns; these disclosures were handled solely by CSE.

Response to NSIRA's recommendations:

48. As detailed in Annex E of this report, CSE accepted all 11 of NSIRA's recommendations. CSE initiated a privacy impact assessment of its CII disclosure regime, and has informed NSIRA that it is in the final stages of implementing an updated version of its CII request software, which is intended to ensure that all necessary information related to operational justification, and legal authority is captured prior to a disclosure taking place. CSE has also ceased releasing CII collected under section 16 of the *CSIS Act* until the Federal Court is fully informed about CSE's sharing of information derived from collection under section 16 warrants.

Ministerial authorizations and ministerial orders under the *CSE Act*

49. After the CSE Act came into force in 2019, CSE received a new set of ministerial authorizations (MAs). These documents, issued by the Minister of National Defence, authorize CSE to engage in activity that risks contravening an "Act of Parliament or interfering with a reasonable expectation of privacy of a Canadian or person in

Canada." [26] For example, such activities might include the incidental interception of private communications during CSE's foreign SIGINT collection activities.

50. The *CSE Act* also created the legislative authority for the Minister to "designate electronic information or information infrastructures or classes of electronic information or information infrastructures as being of importance to the Government of Canada"[27] through a ministerial order (MO). Designating infrastructures as being of importance to the Government of Canada enables CSE to share certain kinds of information, and provide direct assistance.

51. In 2019, the Minister of National Defence issued seven MAs and three MOs under the *CSE Act*. NSIRA received comprehensive briefings on the activities authorized by each MA and MO. Based on the records that CSE provided, NSIRA believes that CSE employed considerable rigour in the MA application process. NSIRA found that CSE's MA application requests contained sufficient information, and provided more information than previous applications under CSE's pre-*CSE Act* governing legislation, *National Defence Act*, thereby allowing for greater transparency of CSE's activities.

52. NSIRA found, however, that CSE has not fully assessed the legal implications of certain activities enabled since the *CSE Act*, which have not yet occurred, but which are permissible under a specific type of MA. NSIRA also found that CSE was unable to provide an assessment of its obligations under international law regarding the conduct of active cyber operations.

53. CSE's briefings on these matters have informed NSIRA's three-year review plan. In particular, this review highlighted the immediate need for NSIRA to focus on CSE's active cyber operations (ACOs) and defensive cyber operations (DCOs), given that the Intelligence Commissioner does not provide approval for these activities and that CSE has no statutory obligation to notify NSIRA when it undertakes these activities. Active and defensive cyber operations represent a new aspect of CSE's mandate, and NSIRA will closely examine both the governance policies and procedures for these activities, as well as the operations themselves.

Response to NSIRA's recommendations

54. As detailed in Annex E, CSE generally accepted NSIRA's recommendations in relation to this review. CSE agrees that its operations should be assessed with respect to compliance with international law, but continues to dispute NSIRA's assertion that it was unable to provide an assessment of its obligations under international law.[28]

Signals Intelligence data retention policies and procedures

55. Inspired by a similar review by the U.S. Inspector General for the National Security Agency, NSIRA completed a review of CSE's SIGINT data retention policies and procedures in December 2020. The purpose of the review was to understand the SIGINT data lifecycle management process and learn about compliance with legal data retention limits, and with government and internal policy. Non-compliance with these limits could potentially adversely affect civil liberties and privacy protections. NSIRA completed its review and will use the information learned as a foundation for a future review.

Privacy Incidents File (2019)

56. On March 4, 2021, NSIRA publicly released its first review of CSE, which was a 2019 review of CSE's Privacy Incidents File (PIF).[29] 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. NSIRA's 2019 PIF review, including findings and recommendations, was discussed in Annex A of the *2019 Annual Report*. NSIRA was unable to publish CSE's responses to NSIRA's recommendations in time for that report, and so these responses are now included in Annex E to the present annual report.

Response to NSIRA's recommendations

57. CSE accepted all five of NSIRA's recommendations regarding the 2019 PIF review. CSE is pursuing a standardized mechanism for identifying and reporting on incidents with privacy interests, and is investigating ways to reach more streamlined and uniform reporting between operational compliance teams. CSE committed to standardizing its policy on how to assess whether a privacy incident constitutes a material privacy breach, and re-examining its assessment methods to ensure they are effective and reasonable. In November 2019, CSE also abolished a specific practice that NSIRA had raised concerns about.

Statistics and data

58. To achieve greater public accountability, NSIRA is requesting that CSE publish more statistics and data about public interest and compliance-related aspects of its activities. This section presents some of this CSE data.[30]

59. NSIRA intends to provide data on an annual basis to provide benchmarks and enable comparison. It cautions, however, that some CSE data are difficult to interpret without significant analysis and full context, and may not necessarily indicate particular practices or developments.

60. In 2020, CSE provided foreign intelligence reports to more than 2100 clients in over 25 departments and agencies within the Government of Canada in response to a range of priorities related to international affairs, defence, and security. As examples, CSE believes that its own intelligence reporting helped thwart or respond to foreign cyber threats, supported Canada's military operations, protected deployed forces, identified hostile state activities, and provided insight into global events and crises to help inform Government of Canada policies and decision making. [31]

61. In calendar year 2020, CSE received 24 requests for assistance from CSIS, the RCMP, and the Department of National Defence, and actioned 23 of these requests.

62. Also in 2020, CSE recorded a total of 81 incidents in its PIF, second party privacy incidents file (SPIF), and minor procedural errors file.

63. In calendar year 2020, CSE was issued six MAs. The table below provides a breakdown of these MAs, as well as of MAs from calendar year 2019, which NSIRA was unable to publish in its 2019 annual report. NSIRA will continue to benchmark and compare these, and other statistics, each year.

CSE ministerial authorizations, 2020

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

CSE ministerial authorizations, 2019

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

* Note that the above tables refer to ministerial authorizations (MAs) that were *issued* in the given calendar years, and may not necessarily reflect MAs that were *in effect*. For example, if an MA was issued in late 2019 and remained in effect in parts of 2020, it is counted above solely as a 2019 MA.

64. In June 2021, in CSE's 2020-2021 public annual report, CSE confirmed that it has conducted foreign cyber operations.[32] CSE informed NSIRA that it is not prepared to release specific information related to foreign cyber operations, as it would constitute special operational information that, if disclosed, could be injurious to Canada's international relations, national defence or national security.

Internal compliance programs

65. In addition to NSIRA's independent expert review, CSE's functions are also subject to its own internal compliance programs. For this annual report, NSIRA asked CSE to provide information on some of its internal compliance programs. CSE's Internal Program for Operation Compliance is responsible for activities of the Canadian Centre for Cyber Security (Cyber Centre),[33] while compliance of SIGINT activities is overseen by the SIGINT Compliance section.

66. Unlike some of its international counterparts,[34] NSIRA does not currently assess the effectiveness of department and agency internal compliance programs. However, NSIRA recognizes that assessing such programs would be an important component of its review mandate, and it intends to build capacity in this area. In the interim, there is nevertheless value in publishing the information available on internal compliance, to provide a greater understanding of CSE's policies in this regard. The information provided in this section should not be considered an independent assessment or evaluation.

Internal program for operation compliance

67. The Internal Program for Operation Compliance (IPOC) is responsible for providing mission management support and operationalizing the Cyber Centre's Internal Compliance Program, which encompasses three fundamental accountability pillars:
    - Enabling Compliance (education, prevention, and collaboration);
    - Compliance Verification and Assurance (monitoring, review, and audit); and
    - Compliance Incident Management (analysis, mitigation, and reporting).

68. According to CSE, the Cyber Centre's ability to demonstrate compliance with legal, ministerial, and policy obligations while conducting cybersecurity activities is "a key component of its 'licence to operate'." CSE considers these accountability and transparency values to be at the core of Cyber Centre operations; they are seen as constituting the foundation for maintaining Canadians' trust and confidence in the Cyber Centre's activities.

69. CSE also stated that, in addition to conducting annual compliance monitoring of cybersecurity and information assurance activities, IPOC works with Cyber Centre operational areas to promote "compliance by design," whereby control mechanisms and privacy protection measures are intended to be proactively built into systems, tools, and operational business processes.

SIGINT compliance

70. Ensuring compliance of activities is, according to CSE, "of utmost importance to SIGINT, as it is critical to CSE's continued lawfulness." The SIGINT Compliance section works with employees to clarify their roles in compliance, for example through employee engagement, incident handling, annual compliance accreditation training, and compliance advice on new and established SIGINT initiatives. The section works to build and maintain a compliance review framework based on the CSE Act and other appropriate legislation, as well as CSE's internal policy instruments.

71. According to CSE, this compliance review framework dictates internal compliance reviews that the group must complete annually over a three-year cycle. Moreover, the SIGINT Compliance group is meant to review SIGINT activities across the entire lifecycle of intelligence production, from data acquisition to processing, analysis and end-product dissemination. When necessary, these reviews contain required actions that employees in certain activity areas must complete to maintain or improve compliance. These required actions must be tracked and updated regularly by both the compliance group, as well as senior management.

72. NSIRA understands that transparency related to compliance is not achieved overnight, and that CSE's transparency efforts are, as CSE told NSIRA, "still a work in progress." NSIRA can assist CSE in such efforts, for example by providing information to the Canadian public about CSE's lawfulness, compliance, and its functions more broadly.

Internal compliance errors reported to NSIRA

CSE states that it promotes a culture of compliance and encourages the self-reporting of potential compliance incidents. In 2019-20, CSE had concerns that it may have received information outside of a valid MA period, in relation to cybersecurity activities on a certain type of infrastructure.

CSE ultimately notified the infrastructure owner, purged the inadvertently received information from its systems in accordance with standard privacy safeguards, and launched a review of the incident for the purpose of identifying and implementing additional privacy protection measures. CSE also proactively engaged the Minister of National Defence and NSIRA for transparency and accountability purposes.

NSIRA appreciates that CSE brought this incident to its attention. NSIRA did not consider the incident to be of major concern, but view CSE's proactive and voluntary notification of the incident as a key success in the NSIRA-CSE relationship. NSIRA feels that CSE's response to this incident bodes well for effective and honest communication and collaboration moving forward.

2021 CSE review plan

73. In general, NSIRA prioritizes its reviews of CSE based on legislative requirements, as well as risk. In the case of risk, NSIRA seeks to identify those activities that may potentially pose higher risks of legal non-compliance, often because these activities are new and untested, or operate under the updated authorities of the CSE Act. NSIRA also engages with various stakeholders, both internal and external to the Government of Canada, to consider CSE-related concerns that should be reviewed.[35]

74. Over the coming years, NSIRA will focus on newer aspects of CSE's mandate, as well as on CSE's use of certain emerging technologies, including artificial intelligence. In particular, NSIRA has heard various concerns from Canadian stakeholders about CSE's

novel foreign cyber operations mandate. NSIRA is closely examining CSE's foreign cyber operations, including in two ongoing reviews, and NSIRA will continue to review these kinds of operations in future. NSIRA will also continue to review discrete CSE activities in cybersecurity and SIGINT based on their associated risks.

75. In addition to NSIRA's two legally mandated reviews of the *Security of Canada Information Disclosure Act (SCIDA)* and the *Avoiding Complicity in Mistreatment by Foreign Entities Act*, NSIRA has initiated or is planning the following CSE reviews, for completion in 2021:

Review of information use and sharing between aspects of CSE's mandates

This review examines how CSE ensures compliance with its lawful authorities and restrictions when exchanging information between aspects of its mandates. An exchange of information between aspects occurs, for example, if CSE collects information under the foreign intelligence aspect and then shares this information with those operating under the cybersecurity aspect. The review examines how CSE uses such cross-aspect information, in order to ensure compliance with the *CSE Act*. This review was initiated in January 2020, but has been delayed.

Review of CSE's active cyber operations and defensive cyber operations, Part 1: Governance

This review examines CSE's new active cyber operation / defensive cyber operation powers under the CSE Act to ensure legal compliance. It looks at the policy and legal framework for conducting these activities for the 2019-20 MAs. This review was initiated in August 2020, but has been delayed.

Review of an activity conducted under CSE's foreign intelligence Ministerial Authorizations

This review studies an activity conducted under CSE's Foreign Intelligence Ministerial Authorizations to examine CSE's policies and procedures. This activity has not been subject to any external or internal assessment, audit, or compliance review, and as such presents an opportunity for NSIRA to conduct the first-ever review of this CSE activity. CSE provided a preliminary briefing to NSIRA on this topic in early 2021, but this review has been delayed.

Departmental study under section 31 of the NSIRA Act

Under section 31 of the NSIRA Act, NSIRA can direct CSE to conduct a study of its activities that relate to national security and intelligence, to ensure that these activities are carried out in compliance with the law and any applicable ministerial directions, and that they are reasonable and necessary. On completion of the study, CSE must provide a copy of the report to the Minister of National Defence and to NSIRA. Following NSIRA's review of CSE's CII disclosures, NSIRA concluded that CSE's implementation of its disclosure regime under the *National Defence Act* may not have complied with requirements under the *Privacy Act.* Given the change in CSE's governing

legislation in 2019, NSIRA has directed CSE to review its disclosures to Government of Canada partners as well as foreign partners to ensure that these disclosures comply with section 43 of the *CSE Act*.[36]

76. Beyond 2021, NSIRA intends to explore CSE reviews of topics including, but not limited to:

    - *Active Cyber Operations and Defensive Cyber Operations, Part 2: Operations;*
    - *Safeguarding of sensitive information, including use of the polygraph;*
    - *Assistance to CSIS;*
    - *A specific cybersecurity activity as outlined within an MA;*
    - *The Vulnerabilities Equities Management Framework (VEMF);*
    - *The use of emerging technologies, including Artificial Intelligence;*
    - *A foreign SIGINT collection program conducted* under an MA; and
    - *SIGINT retention practices.*

77. NSIRA's mandate allows it to conduct inter-departmental reviews (also known as 'follow-the-thread' reviews), and it intends to do so for several ongoing and planned CSE reviews. In engaging with a range of federal departments and agencies, NSIRA's CII review was its first follow-the-thread review.

Access

78. In 2020, NSIRA's CSE Review Team established office space in CSE's headquarters. This office space, which began partial operations in 2020, includes nine workstations and provides NSIRA with greater access to its CSE counterparts. Access to NSIRA's CSE office is restricted, and appropriate safeguards are in place to ensure NSIRA's independence.

79. A significant challenge to NSIRA's CSE review is the lack of comprehensive and independently verifiable access to CSE's information repository.[37] As one component of addressing challenges, NSIRA is exploring options to have CSE proactively disclose specific categories of information on a regular basis, which would be used to both ensure compliance of activities and inform the conclusions NSIRA provides in the annual classified report to the Minister.[38]

80. As another component of addressing access challenges, NSIRA is also exploring some options with CSE to implement the "tailored access" approach described under section 1.5 of this Report. Implementing tailored access will result in trust being maintained between the two organizations, while ensuring that NSIRA has the ability to

independently verify the information received in the context of its review. It should also be noted that the speed at which NSIRA receives information before the verifications stage remains important, as any delays in receiving information has the potential to impede NSIRA's ability to fulfill its mandate.

81. To encourage greater accountability in the year ahead, NSIRA intends to establish more formal guidelines for the provision of information by departments and agencies, including targets for the timeliness of responses to requests for information, and a framework for reporting publicly on the above.

Conclusion

82. As a new organization, NSIRA continued to staff its CSE Review Team in 2020,[39] in addition to improving its overall understanding of CSE's remit. NSIRA acknowledges the need to continue consolidating its familiarity and expertise with CSE and various aspects related to CSE's functions. Similarly, CSE—which built a close relationship with OCSEC over some 23 years of review — is in the process of building its own familiarity with NSIRA and its mandate. NSIRA also acknowledges that reviews of CSE's functions can be particularly sensitive, for example, because of the high volume of highly classified special information content.

83. NSIRA thanks CSE for timely assistance in providing publicly-releasable information for this annual report, much of which has not previously been made public. NSIRA feels that this reflects steps by CSE toward increased transparency to Canadians. Further, NSIRA is grateful for regular support from CSE's Information Technology services in helping with secure communications.

2.6 Other government departments

Overview

84. One key reason for creating NSIRA was to ensure scrutiny of Canadian national security and intelligence departments and agencies that did not already have dedicated review bodies. To this end, the NSIRA Act provides the legal foundation to "review any activity carried out by a department that relates to national security or intelligence."[40] As would be expected, selecting which departments and agencies outside of CSIS and CSE that require examination is complex and must be continuously updated in tandem with the ever-changing national security landscape.

85. In addition to selecting specific departments for review, NSIRA is developing an integrated review framework that addresses broad-based national security and intelligence issues both horizontally and vertically across departments and agencies. This is in addition to the yearly reviews of the *Security of Canada Information Disclosure Act* and the *Avoiding Complicity in Mistreatment by Foreign Entities Act*, which when considered cumulatively, provide the opportunity to cover the entire community.

86. As previously mentioned in section 1 of this report, NSIRA is working with departments and agencies across government to design a process where the information provided for a review is corroborated and verified for completeness. NSIRA calls this the trust but verify principle: NSIRA trusts departments to provide access to information, people and assets in a timely manner, while having mechanisms in place to allow the agency to independently verify the completeness of the access.

87. It is also important to note that NSIRA works closely with the NSICOP and the OPC to share review plans and de-conflict when reviews touch on similar subjects.

88. Beyond CSIS and CSE, NSIRA initiated reviews with the following departments and agencies in 2020:

    - Department of National Defence / Canadian Armed Forces (DND/CAF);
    - Global Affairs Canada;
    - the RCMP;
    - Immigration, Refugee and Citizenship Canada;
    - the Canada Border Services Agency;
    - Transport Canada; and
    - the Public Health Agency of Canada.
    - the following sections outline reviews completed or initiated in 2020, by department/agency, as well as some planned future reviews.

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

90. The following sections outline reviews completed or initiated in 2020, by department or agency, as well as some planned future reviews.

Department of National Defence and the Canadian Armed Forces

The Canadian Forces National Counter-Intelligence Unit

91. The Canadian Forces National Counter-Intelligence Unit (CFNCIU) falls under the Canadian Forces Intelligence Group within Canadian Forces Intelligence Command and is organized along Regional Detachments. CFNCIU's activities involve investigating and reporting counter-intelligence threats that pose a security risk to DND/CAF, supporting CAF operations to enhance force posture and operational security, coordinating exchanges of threat information with security partners, and providing early warning. CFNCIU's primary responsibility is the collection of security intelligence for integration into national or local threat assessments.

92. The investigative framework for CFNCIU is unique insofar as it covers a broad range of security intelligence concerns similar to those of CSIS, yet is limited in investigative scope to DND/CAF information, people and assets (i.e. nexus to DND/CAF). Unlike CSIS, CFNCIU does not collect expansively on threats given the need for a nexus; and unlike a Departmental Security Officer, CFNCIU does not conduct investigations on issues regarding policy compliance, or security issues involving inappropriate behavior by employees that do not point to an obvious threat. Furthermore, CFNCIU does not have responsibility for security screening or criminal investigations. The investigative scope of CFNCIU is therefore best understood as occupying a very narrow space above those related to discipline and security screening, yet falling below criminal thresholds.

93. This review examined CFNCIU's domestic efforts at investigating counter-intelligence threats posed to DND/CAF, the rationale used by CFNCIU for justifying investigations, and the associated investigative activities that follow. In this context, the review specifically sought to provide an initial understanding of the DND/CAF governance framework, as well as how CFNCIU views threats, collects intelligence, engages in cooperation and applies analysis. Particular attention was paid to CFNCIU's legal foundations, processes and procedures, and how they contribute to safeguarding against insider-threat scenarios.[41] NSIRA also reviewed how intelligence derived from investigations was conveyed to DND/CAF decision-makers. The full review is currently being redacted and should be released on NSIRA's website soon.

94. NSIRA found that CFNCIU and other DND/CAF security components have been organized into narrowly focused vertical silos that do not work in an integrated manner. While CFNCIU adhered to internal policies used to initiate investigations, it did

not have a formalized process to help guide investigation prioritization based on relevant criteria. It was also evident that CFNCIU required clarity on its legal authorities, to ensure the proper sharing of information in support of administrative and criminal processes.

95. NSIRA further identified the need for DND/CAF to empower CFNCIU to make full use of its investigative capabilities to reduce investigative durations, an issue that NSIRA found runs contrary to the sound safeguarding practices of DND/CAF information, people, and assets.

96. Moreover, NSIRA's review found that CFNCIU did not adequately consider the cumulative effect of its counter-intelligence activities in relation to an investigation subject's privacy, raising questions about the adequacy of CFNCIU's efforts to ensure procedural fairness and prompting NSIRA to recommend that CFNCIU seek advice from the OPC. NSIRA also observed that CFNCIU's information sharing regime was not compliant with Government of Canada policies for safeguarding information, people, and assets.

97. The presence of white supremacy within the Canadian military has been well documented. White supremacist groups actively seek individuals with prior military training and experience, or conversely, encourage individuals to enlist in order to gain access to specialized training, tactics and equipment. Although NSIRA acknowledges that the responsibility for addressing this threat cannot fall uniquely on the shoulders of CFNCIU, the review's multiple findings lead to concern that CFNCIU may not be fully utilized to proactively identify white supremacists across DND/CAF. After examination of case studies and interviews with CFNCIU investigators, the review found that white supremacy poses an active counter-intelligence threat to DND/CAF, and that the CFNCIU's mandate to proactively identify this threat is limited.

98. Finally, following some concerns identified in the later stages of this review, NSIRA will carry out a case study of CFNCIU computer searches and interview processes in 2021 to assess whether these activities were *Charter*-compliant.

DND/CAF response to NSIRA's recommendations

99. DND/CAF agreed with NSIRA's recommendations, and stated that they welcome the review report. DND/CAF agreed that action will be taken at the appropriate levels in conjunction with required expertise and offices, noting that work in this regard has commenced, and that some of NSIRA's recommendations are already being addressed. For example, DND/CAF are working to complete a Privacy Impact

Assessment of Defence Intelligence activities, and will engage the OPC for further input once this assessment is completed.

Reviews in progress

100. NSIRA launched a review of the Defence Intelligence Enterprise to map intelligence collection, and obtain information on the governance frameworks, authorities and structures of defence intelligence with a view towards assisting future review planning. This information was further supplemented by a corollary review of Intelligence Oversight, Review and Compliance within DND/CAF's defence intelligence system. Although there are no findings or recommendations stemming from these inquiries, NSIRA members will receive a briefing note and presentation from NSIRA staff on key observations gained through this process. The expected completion is fall of 2021.

101. NSIRA has also begun to follow-up on issues identified during last year's CFNCIU review. NSIRA's Counter-Intelligence Operational Collection and Privacy Review will further examine CFNCIU's practices concerning subject interview and database access to information management/information technology systems; this latter assessment will require access by NSIRA staff to DND/CAF computer networks to validate how these systems are used when conducting counter-intelligence inquiries.

102. NSIRA has also initiated an examination of DND/CAF's human intelligence (HUMINT) capabilities, primarily through review of the governance of this specialized collection activity. The review will cover the evolution of HUMINT within DND/CAF, including consideration of recent internal initiatives aimed at improving governance and guidance for HUMINT. In the fall of 2021 NSIRA staff will travel to DND/CAF's HUMINT training centre, and will conduct wide-ranging interviews of HUMINT senior leadership, trainers, and practitioners. The review will lay the foundation for a full operational review of HUMINT sources in various theatres of operation.

103. As a result of recent disclosures from DND/CAF through the Scoping Review of the Defence Intelligence Enterprise, NSIRA will also examine DND/CAF's Open Source Intelligence and Medical Intelligence collection activities beginning at the end of 2021. This review will assess the governance and compliance of these activities.

104. COVID-19 has affected timelines and scheduling significantly, resulting in delays of up to six months. While COVID presented challenges affecting timelines and impacting review work, both DND/CAF and the National Security and Intelligence Review and Oversight Coordination Secretariat were attentive to NSIRA requests, providing access to information, people and assets when required.

Global Affairs Canada

105. NSIRA completed its first dedicated review of a Global Affairs Canada program. The review period was January 1, 2017 to December 31, 2019, although information from outside this period was used to conduct a full assessment of specific aspects of this program. Challenges related to COVID-19 resulted in methodological adjustments such as the use of secure video-teleconferencing in place of in-person interviews for some of the employees.

106. While clients of the program find it both unique and valuable to the Government of Canada, the review identified several areas of improvement. NSIRA made a number of recommendations aimed at improving this program. Global Affairs Canada has agreed to "positively address all of the recommendations" and has committed to responding to NSIRA in the near future. Due to the highly sensitive nature of this review, NSIRA will not be publishing anything further at this time.

Royal Canadian Mounted Police

107. In 2021, NSIRA will finish a review of a specialized RCMP intelligence unit, and it will launch a review of the RCMP's National Security Program's human source activities. Going forward, NSIRA plans to increase the number of reviews involving the RCMP. For example, the agency will review how the RCMP and CSIS have responded to the threat posed by ideologically motivated violent extremism.

Immigration, Refugees and Citizenship Canada

108. NSIRA is currently conducting a scoping review of Immigration, Refugees and Citizenship Canada in order to delineate its national security role and responsibilities. While the department has no intelligence collection programs, Immigration, Refugees and Citizenship Canada has an intricate mandate with shared legal authorities and operational responsibilities for ensuring the integrity of the immigration system and mitigating threats to national security from abroad.

Canada Border Services Agency

109. NSIRA has initiated its plan to conduct in-depth reviews of the most sensitive security and intelligence activities of the Canada Border Services Agency (CBSA), as identified by NSICOP: scenario-based targeting, surveillance, confidential human sources,

lookouts and joint force operations. A review of air passenger targeting is currently underway, focusing on how the CBSA uses predictive analyses, including what is termed "scenario-based targeting," to identify inbound air travellers for further scrutiny in relation to national security threats. Reviews of the CBSA's use of confidential human sources and surveillance activities are slated for completion in 2022.

Cross departmental reviews

Avoiding complicity in mistreatment by *Foreign Entities Act*

110. On September 4, 2019, the Governor in Council issued written directions to the Deputy Heads of 12 departments and agencies under the new *Avoiding Complicity in Mistreatment by Foreign Entities Act* (Avoiding Complicity Act). The Avoiding Complicity Act and its associated directions seek to prevent the mistreatment of any individual as a result of information exchanged between a Government of Canada department and a foreign entity. At the heart of the directions is the consideration of substantial risk, and whether that risk, if present, can be mitigated or not. To do this, the Avoiding Complicity Act and the directions lay out a series of requirements that need to be met or implemented by departments when handling information. Under subsection 8(2.2) of the NSIRA Act, NSIRA is required to annually review implementation of all directions sent to departments and agencies.

111. While this was the inaugural annual review under the NSIRA Act, it builds on previous work in this area undertaken by NSIRA and its predecessor SIRC. NSIRA's review on the 2017 *Ministerial Direction on Information Sharing with Foreign Entities* is an example. NSIRA is building on this previous review and strongly supports that review's findings and recommendations. It was essential to ensure that both NSIRA and the departments being reviewed met their obligations under the Avoiding Complicity Act and the NSIRA Act. The approach used to gather information during a global pandemic was purposely designed for this first and unique review period. The full 2019 review of the Avoiding Complicity Act has been redacted and released on its website.[42]

112. To capture a complete view on the departmental implementation, NSIRA requested information that related directly to every department's specific obligations under the Avoiding Complicity Act and the directions. The responses and associated information captured departmental activities related to the Avoiding Complicity Act during the review period, and what procedures, policies, tools, etc. (frameworks) were leveraged to support these activities. No case studies were undertaken for this review. However, the information gathered has helped establish a baseline for overarching issues the

community is facing. Building on this, future reviews will begin to examine specific sharing framework challenges and questions, and look closely at specific cases and departmental legal opinions to guide review findings.

113. While NSIRA was pleased with the considerable efforts made by many departments new to the Avoiding Complicity Act in building up their supporting frameworks, it was clear during this review that departments were employing very different approaches to guide their information handling activities. The responses received demonstrate various inconsistencies across the departments. Having a consistent and coordinated approach when addressing the concerns related the Avoiding Complicity Act is not a requirement for implementation, however, NSIRA believes that there is value in such an approach.

114. Additionally, as the directives received under the Avoiding Complicity Act do not describe the specific means by which departments 'implement' them, it is incumbent on the departments and agencies to ensure that they have sufficiently robust frameworks and programs in place to fully support an assertion of implementation. Therefore, the information gathered during this review went beyond a strict assessment of implementation, and also considered the aspects required to better support this implementation. Going forward, this approach will help establish the foundation for subsequent reviews. Drawing on the findings and concerns identified here, NSIRA will continue to consider aspects that will ultimately improve underlying frameworks, thereby supporting an improved implementation of the Avoiding Complicity Act across the community.

Disclosure of information under the *Security of Canada Information Disclosure Act*

115. Enacted in 2019, the purpose of the *Security of Canada Information Disclosure Act* (SCIDA) is to encourage and facilitate the disclosure of information between Government of Canada institutions in order to protect Canada against activities that undermine the security of Canada. NSIRA has a statutory requirement to conduct an annual review of disclosures made under the SCIDA.

116. In 2020, NSIRA completed the *2019 Annual Report on the Disclosure of Information under the* Security of Canada Information Disclosure Act.[43] The report covers the period from when SCIDA came into force on June 21, 2019 to December 31 of that year. During the reporting period, federal institutions made 114 disclosures of information under SCIDA. The report notes that institutions made good progress in institutionalizing this new legislation. The report provides historical and contextual information on SCIDA and how it fits alongside other legal mechanisms for the sharing

of information. The report also includes anonymized scenario examples of SCIDA disclosures, and criteria for future assessment. NSIRA intends to work closely with the OPC for future iterations of this report. Outcomes of NSIRA's subsequent review of disclosures under SCIDA will be discussed in the 2020 report on the disclosure of information under this SCIDA.

Biometrics

117. NSIRA has advanced its commitment made last year to map the collection and use of biometrics across the government in relation to its security and intelligence activities. A horizontal review of biometrics in the border continuum is currently underway, focusing on activities conducted by the CBSA, Immigration, Refugees and Citizenship Canada and Transport Canada. The activities under review include the issuance and verification of travel documents — with an emphasis on air travel — and the screening of foreign nationals seeking admission to Canada. A subsequent review will examine the use of biometrics in security intelligence and national security related policing activities.

Conclusion

118. Given the ongoing pandemic and lessons emerging from current reviews, in some instances NSIRA have modified the plan put forward in NSIRA's *2019 Annual Report*. Its work on economic security, for example, benefited from a scoping exercise involving several departments to help it better understand the authorities in this area, and to help it determine whether to pursue further work on this issue. Similarly, following a scoping exercise, a decision on whether to review public health intelligence awaited considerations of the conclusions of an independent report commissioned by the Minister of Health in this area that has now been released.

119. Over the next year, NSIRA will continue to engage with departments and agencies through focused reviews. Some of these will be organized around broad horizontal themes that may include multiple departments, requiring a coordinated approach. NSIRA is committed to working collaboratively with departments, particularly on the establishment of an access regime that supports independent verification and accountability.

03 //

Complaints investigations

3.1 2020 challenges

1. The pandemic has had an adverse impact on the timely conduct of NSIRA's investigations. As of March 2020, inevitable delays resulted from the provincial stay-at-home orders and public health guidelines that were issued. Just as NSIRA was affected by limited access to classified documents as a result, so too were the for federal government parties to investigations that are obliged to provide information to NSIRA. Consequently, in several ongoing matters, NSIRA granted adjournments and extensions of deadlines for procedural steps, including the filing of submissions and evidentiary material. While this was regrettable, NSIRA adapted to the challenging circumstances of the pandemic as best as possible and advanced investigative procedures in an innovative manner whenever possible, such as conducting some proceedings in writing and holding case management conferences and meetings virtually.
2. Despite the procedural setbacks in 2020, NSIRA was able to complete one complaint investigation and issue a final report. NSIRA also issued formal decisions to close three other files. In addition, it succeeded in completing a complex process reform initiative that will see the modernization and streamlining of the investigative process.

3.2 Complaints investigation process: Reform and next steps

3. While the pandemic affected complaints investigations, NSIRA made considerable progress on reforming the processes governing such investigations. In the course of the year, NSIRA undertook a process reform initiative to modernize the complaints investigation model to meet its goal of ensuring efficiency and transparency. Two priorities guided the modernization of the process, namely, access to justice for self-represented complainants and the creation of streamlined and less formal procedural steps.
4. NSIRA created new Rules of Procedures to reflect this new model and completed an extensive consultation exercise with stakeholders in the public and private

sectors to achieve the most effective and considered final product. These new Rules of Procedure have been in effect since July 2021.

5. NSIRA also implemented a new policy statement that provides a commitment to the public to increase transparency in its investigations by publishing redacted and de-personalized complaints investigation reports. [44]

6. In the year ahead, NSIRA will update its website to include improved procedural guidance to inform members of the public on how to make complaints and navigate the investigative process. Part of the update to NSIRA's website will involve implementing a secure portal for the online filing of complaints and for protected communications to assist in effectively managing NSIRA's complaints case load.

7. In the future, NSIRA also plans on conducting a trend analysis for complaints, which will involve a broad initiative to appropriately collect race-based and other demographic information. The objectives of this initiative are to improve access to justice by improving awareness and understanding of the investigation process. The overall aim is to document the different groups among civilian complainants and identify the frequency of complaints that include allegations of racial or other forms of bias, and to determine whether there are disparities; whether there are differences with respect to the types of complaints made against national security and intelligence organizations based on different groups; whether complaints investigation outcomes vary by group; and whether civilian satisfaction with NSIRA's investigation process varies by group.

NSIRA's investigation case load: The year ahead

8. On concluding efforts to case manage NSIRA's ongoing investigations in the context of the challenges presented by the pandemic in 2020, NSIRA will look ahead to the coming year with a reformed investigation process that will assist in implementing modern and fair procedures to advance these cases, complemented by an improved website that will promote access and transparency in the investigations process.

9. NSIRA will also see a substantial increase in its caseload in 2021as a result of close to 60 new investigations added to its existing inventory. These complaints were referred to NSIRA in April 2021 by the Canadian Human Rights Commission pursuant to subsection 45(2) of the *Canadian Human Rights Act*. This high-volume caseload will significantly challenge NSIRA's case management. NSIRA will be implementing procedural efficiencies as much as possible while meeting procedural fairness requirements.

3.3 2020 complaints

Summary of final report

Allegations against CSIS's role in cancellation/denial of site access clearance

Background

10. The Complainant filed a complaint against CSIS requesting an investigation of CSIS's role or involvement in the cancellation and/or denial of site access screening requests for employment with a private company at a government building.

Allegation

11. The Complainant alleged CSIS improperly used information collected and made an improper inference of a security threat which led to the denial of a site access clearance.

Investigation

12. NSIRA considered the evidence given by summoned witnesses, the documentation submitted by the parties as well as other relevant material made available during the course of the investigation of the complaint, including classified documents disclosed to NSIRA by CSIS. NSIRA also heard evidence provided by the Complainant.

13. Sections 13 and 15 of the *CSIS Act* give CSIS the authority to provide security assessments to departments of the Government of Canada and to conduct investigations as required. CSIS receives applications from government departments for persons seeking a security clearance or site access clearance and their role is defined in section 2 of the *CSIS Act*. CSIS presented evidence on the steps that are followed in CSIS's process, the Treasury Board Secretariat's Standard on Security Screening, and the fact that the client department decides whether to grant a clearance. As such, CSIS only provides background information and an assessment from a national security perspective so that government departments have the information it needs to make an informed decision.

14. NSIRA also heard evidence from CSIS with respect to some information shared with the client department that requested the site access clearance and how it pertained to both reliability and loyalty. CSIS acknowledged that some information shared with the client department took place in an informal setting and that it should not have

occurred in such way. It was noted that after open source information was shared, the client department cancelled its request and CSIS closed its file.

15. The Complainant expressed a belief that CSIS was responsible for denying his application for a site access clearance.

16. NSIRA acknowledged the Complainant's perception that CSIS denied his request for a site access clearance, but the evidence demonstrated that CSIS did not make the decision. The decision was made by the government department and CSIS had no further involvement in the matter.

Findings

17. NSIRA found that:

- CSIS did not improperly use the open source information that was shared;
- CSIS acknowledges that the sharing of information would not have been approved by management; and
- CSIS did not deny the Complainant's request for a site access clearance, but rather it was the government department that made the decision to cancel the request.

Conclusion

18. NSIRA determined that the complaint is unsupported.

Summaries of complaints deemed abandoned

Allegations against CSIS for sharing information with foreign authorities and impact on border crossing

19. The Complainant filed a complaint against CSIS about the sharing of information with foreign authorities that led to having difficulty with border crossings. NSIRA commenced its investigation and had an informal case management conference with the parties for the purposes of resolving the complaint. As a result of this resolution meeting, the Complainant undertook to take steps to resolve any ongoing issues. NSIRA attempted to communicate with the Complainant on several occasions to determine whether the ongoing issues were resolved. NSIRA determined that reasonable attempts had been made to communicate with the Complainant and issued reasons deeming the complaint abandoned as per NSIRA's Rules of Procedure. The complaint investigation file was closed.

Allegations against CSIS's role in delaying security assessment regarding a permanent residency application

20. The Complainant filed a complaint against CSIS alleging that it caused a significant delay in submitting the security assessment for a permanent residency application. During the investigation, NSIRA attempted to communicate with the Complainant on several occasions regarding the possibility of engaging in informal resolution discussions with CSIS. NSIRA determined that reasonable attempts had been made to communicate with the Complainant and issued reasons deeming that the complaint had been abandoned as per NSIRA's Rules of Procedure. The complaint investigation file was closed.

Allegations against the RCMP for improper conduct during arrest

21. This complaint was referred to NSIRA by the Civilian Review and Complaints Commission for the RCMP, pursuant to subsection 45.53(4.1) of the RCMP Act. The complaint alleged that members of the Royal Canadian Mounted Police (RCMP) failed to inform the Complainant of the Complainant's rights and obligations during an interaction that occurred the day before an arrest for a terrorism hoax and public mischief, use of excessive force and other allegations. During the course of launching its investigation, NSIRA attempted to establish contact with the Complainant on several occasions. NSIRA found that reasonable attempts had been made to communicate with the Complainant and had exhausted all options. Accordingly, NSIRA issued reasons deeming the complaint had been abandoned as per NSIRA's Rules of Procedure. The complaint investigation file was closed.

04 //

Conclusion

1. In 2020, NSIRA's teams worked under exigent conditions and yet were able to outperform. NSIRA is grateful to them for having conducted the reviews in an efficient manner. As mentioned in this annual report, NSIRA have ambitious plans for ongoing and future work, all while continuing to grow its own capacity and to strengthen its relationships with the departments and agencies under its review. In 2020, NSIRA's staff complement grew from 30 to 58 individuals, its CSE Review Team began operations in offices on site at CSE, and NSIRA neared completion of a new facility for staff, all while carefully and responsibly adapting to the challenges of the pandemic.
2. In the spirit of coordinating and complementing other review and oversight entities, NSIRA continued to strengthen its relationships with various counterparts, including the Five Eyes Intelligence Oversight and Review Council, the National Security and Intelligence Committee of Parliamentarians, and the Office of the Privacy Commissioner of Canada. NSIRA also remains dedicated to robust and mutually-beneficial engagement with non-governmental stakeholders. NSIRA hopes both to raise awareness of its mandate amongst various communities — including students — as well as to receive input to help us further its work and refine its agenda. NSIRA strongly encourages feedback and input and hopes you found this report useful and helpful. No matter your background, please reach out to us and share your thoughts about this report, as well as NSIRA's review and complaints work.
3. NSIRA is very grateful for the perseverance, diligence, and passion of its staff for continuing to produce meaningful work and achieve important results despite the challenges of the pandemic in 2020. As NSIRA grows as an organization, including in staff numbers, it looks forward to continuing to promote accountability in the Canadian security and intelligence community.

05 //

Annexes

Annex A: List of abbreviations

Abbreviation	Full Name
CAF	Canadian armed forces
CBSA	Canada Border Services Agency
CFNCIU	Canadian Forces National Counter-Intelligence Unit
CSE	Communications Security Establishment
CSIS	Canadian Security Intelligence Service
DND	Department of National Defence
FIORC	Five Eyes Intelligence Oversight and Review Council
HUMINT	human intelligence
MA	ministerial authorization
MO	Ministerial Order
NSICOP	National Security and Intelligence Committee of Parliamentarians
NSIRA	National Security and Intelligence Review Agency
OCSEC	Office of the Communications Security Establishment Commissioner
OPC	Office of the Privacy Commissioner
RCMP	Royal Canadian Mounted Police
SCIDA	*Security of Canada Information Disclosure Act*
SIGINT	Signals Intelligence
SIRC	Security Intelligence Review Committee
TRM	threat reduction measure

Annex B: Financial and administrative overview

Financial overview

1. NSIRA is organized according to three main business lines: Legal Services, Reviews, and Internal Services. The table below presents a comparison of spending between 2019 and 2020 for each of the three business lines above.

(in dollars)	Expenditures (2020)	Expenditures (2019)
Legal services and complaint investigations	1,859,924	1,042,117
Reviews	3,094,323	1,726,218
Internal services	4,625,860	2,820,115
Total	**9,580,107**	**5,588,450**

2. In the 2020 calendar year, NSIRA spent $9.6 million, a $4.0 million (82%) increase from the $5.6 million spent in 2019. This spending increase is mainly attributed to growth in personnel, the fit-up of secure facilities to house an increased number of staff, and investments in Information Management/Information Technology infrastructures such as classified network access, secure video teleconferencing, and equipment for NSIRA's personnel for working remotely.

Staffing

3. Over the course of the year, significant progress was made on the staffing front. NSIRA's personnel complement grew from 30 to 58 people for a net employee increase of 28 (93%). This achievement was made possible through the implementation of modern and flexible staffing strategies, procedures and practices. NSIRA's staffing activities made use of best practices to encourage inclusion and diversity and to recognize official languages representation imperatives.
4. In 2021 and beyond, NSIRA will continue its drive to hire talented and committed individuals to fulfil its mandate. To support this effort, NSIRA is putting in place onboarding, talent management and wellness programs aimed at attracting, retaining and supporting the development of its employees. As NSIRA grows toward a full complement of 100 employees, it will continue to make significant investments in

technology infrastructure, and in ensuring that employees are equipped to perform, while being able to count on the full support from internal services functions.

Pandemic

5. As discussed throughout this report, the pandemic continued to have a profound impact on NSIRA operations and activities throughout 2020. The NSIRA Secretariat responded quickly by developing and implementing new protocols to enable its efforts to continue in the midst of an ever-evolving public health crisis.
6. Considering the importance of on-site access to conduct NSIRA's mandate, the Secretariat took effective and timely measures to allow controlled, safe and timely access to the office. The last Public Service Employee Survey confirmed that employees felt confident with the approach taken by NSIRA when it came to protecting the health and safety of its employees. In 2021, NSIRA intends to continue to improve its health and safety practices by listening to concerns of employees and taking timely actions to address safety and health concerns.
7. To address some of the ill effects of the pandemic such as isolation, lack of human contact or restricted ability to develop bonds with new employees, NSIRA focused on increased digital communication and virtual contacts with staff through the release of regular newsletters, pandemic updates, virtual get-togethers, and the promotion of employee assistance programs.
8. However, stay-at-home orders and restricted office access, made some delays in the progress on reviews and complaints investigations inevitable given that the ability to retrieve and discuss classified material in a secure environment is central to NSIRA's work. Many of the departments and agencies responding to its review and investigation requests also faced similar challenges, including reduced staff complements and limited access to their workplaces, which contributed to the delays NSIRA experienced.

Cyber incident

9. In March 2021, NSIRA was affected by a cyber-incident. Unauthorized access was discovered on NSIRA's external network, which further contributed to delays in its work. This external network houses unclassified and protected information only, and was not used to store Secret or Top Secret information. With the help of its federal partners and, in particular, the efforts of the Privy Council Office, the Canadian Centre

for Cyber Security, and Shared Services Canada, NSIRA was able to address the issue and resume normal business operations in a timely way.

10. NSIRA has been working with the Office of the Privacy Commissioner and Treasury Board of Canada Secretariat to address a privacy breach that resulted from the cyber incident. NSIRA informed partners, notified the public through its website and social media, and issued direct notifications in accordance with requirements and recommendations of the Office of the Privacy Commissioner. Ensuring the privacy of Canadians and the protection of NSIRA's information are its top priorities.

Foundational initiatives

11. In light of the current and planned growth in personnel and of the current pandemic physical distancing requirements, having access to secure space to conduct work of a classified nature is critical to the success of the organization. In 2020, NSIRA firmed-up its accommodation strategy and its funding, and made significant progress in the fit-up of short-term space. While long-term accommodation construction projects have been affected by the pandemic, NSIRA is developing strategies that encourage employees to work from home when it is possible and productive to do so.

12. Key to the success of NSIRA is the contribution, development and wellbeing of its employees, and the development of a culture that supports its important mandate. Being a new organization and a separate employer, NSIRA established, in consultation with its employees, the foundation of its human resource management philosophy through the development and implementation of a modern and grounded Human Resource Management Policy and of the related terms and conditions of employment.

13. In the same manner, NSIRA developed policies on occupational health and safety, workplace harassment and violence prevention, as well as established an awards and recognition program, a code of conduct for its employees and a three-year official languages action plan. NSIRA is also partnering with Health Canada to offer the Employee Assistance Services (EAS) and with other organizations for the maintenance of strong employee-employer relationships.

14. NSIRA employees and management alike engaged in discussions about systemic barriers to inclusion and diversity and on how, through its mandate, NSIRA could leverage its role for change in the security and intelligence community. Over the course of 2021, an action plan to that effect will be formalized and presented to the Clerk of the Privy Council.

What's ahead

15. In 2021, NSIRA intends to continue to develop policies and tools and implement initiatives that will foster a culture of excellence, transparency, respect and innovation.

16. In the short term, NSIRA will implement policies, tools, and programs to further attract, retain and develop talent; work to support NSIRA's and the Government of Canada's commitments to diversity and inclusion; take action to address employees concerns raised through the 2020 Public Service Employee Survey; complete the set-up of activities that can best be performed by NSIRA (such as finance and human resources) and seeking the support of partner departments for those activities best performed by larger organizations (such as some information technology and security functions); continue work to strengthen NSIRA's posture with respect to security, information technology and information management; and obtain increased access to secure facilities for NSIRA employees.

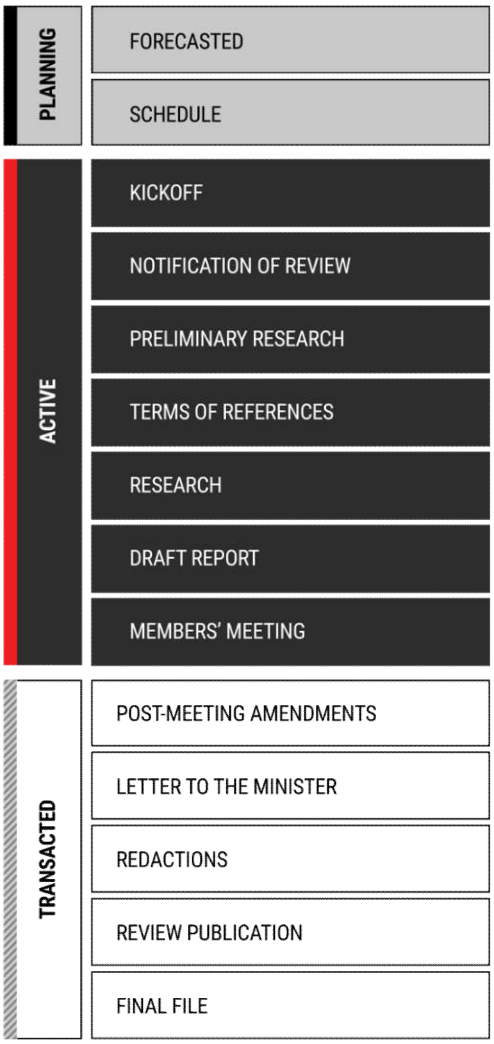
Annex C: NSIRA's review framework

1. NSIRA is developing a review framework that will ensure consistency in the way NSIRA execute its reviews. The framework is meant to provide systematic guidance on NSIRA's process and approach, from start to finish. Its review framework consists of review types, stages and steps.

Review stages and steps

2. There are three major stages of the review. The review stages represent the entire lifecycle of a review from beginning to end. These stages are the Planning, Active, and Transacted stages. The review steps represent the chronological process to be followed. Figure 2 provides depicts the Review Stages and their corresponding Review Process Steps.

Fig. 2 NSIRA review process: stages and steps



Review process

3. Although the steps in the review process represent a chronological process to be followed, but some steps may overlap. For example, while preliminary research may begin in the kickoff step, it might overlap with the main research step, or report drafting may begin at an earlier step in the overall process.

4. Each step in the review process incorporates a multitude of additional items that are required to conduct a review. NSIRA's goal is to continually refine and improve its review process to produce the most consistent, objective, and rigorous reviews possible.

Annex D: 2020 reviews at a glance

This annex presents a concise list of reviews that NSIRA completed, initiated or conducted during 2020. In the tables below, 'start date' refers to the month in which NSIRA finalized its terms of reference for a given review, while 'completion date' refers to the month that the final review report was approved by the NSIRA members.[45]

Reviews completed in 2020

Name of review	Start date	Completion date
Canadian Security Intelligence Service (CSIS) reviews		
CSIS-RCMP Relationship in a Region of Canada through the Lens of an Ongoing Investigation	10.2019	12.2020
CSIS Threat Reduction Activities	07.2020	12.2020
Communications Security Establishment (CSE) reviews		
Disclosure of Canadian Identifying Information to Canadian Partners	09.2019	10.2020
Ministerial Authorizations and Ministerial Orders under the CSE Act	12.2019	10.2020
Signals Intelligence Data Retention Policies and Procedures	07.2020	12.2020
Other government department reviews		
Canadian Forces National Counter-Intelligence Unit	12.2019	12.2020
Global Affairs Canada Review	02.2020	12.2020
Cross departmental		
Implementation of the *Avoiding Complicity in Mistreatment by Foreign Entities Act* for 2019	08.2020	12.2020
Disclosure of Information under the *Security of Canada Information Disclosure Act*	03.2019	11.2020

Annex E: Review findings and recommendations

This annex lists NSIRA's full findings and recommendations for the reviews discussed in this annual report, as well as reviewees' management responses to NSIRA's recommendations, to the fullest extent possible at the time of publication.[46] NSIRA intends to publish and track such information from all reviews on its website.

Canadian Security Intelligence Service reviews

Review of Canadian Security Intelligence Service-Royal Canadian Mounted Police (CSIS-RCMP) relationship in a region of Canada through the lens of an ongoing investigation

NSIRA's findings

1. Since 2019, there have been gaps in CSIS's intelligence collection on a threat in question.
2. Reliance on a narrow set of information resulted in gaps in the investigation into the threat in question.
3. A lack of usable and compatible secure communications tools is making CSIS-RCMP de-confliction in the region excessively burdensome and time-consuming.
4. Despite persistent challenges related to information sharing and governance structures, CSIS and the RCMP have developed a strong relationship that has fostered effective tactical de-confliction in the region.
5. Fundamental issues related to the intelligence-to-evidence problem remain unresolved. In the regional investigation in question, despite frequent verbal disclosures of information between CSIS and RCMP's headquarters, CSIS's formal disclosures of information have been limited and not always useful. CSIS intelligence has not been shared or used in a way that has significantly advanced the RCMP's investigations.
6. The Operational Improvement Review (OIR) has the support of senior management of both CSIS and the RCMP and work is underway to assess and implement its recommendations.

NSIRA's recommendations, and CSIS-RCMP's response

Recommendations	CSIS-RCMP Response (June 2021)
NSIRA recommends that CSIS invest the resources needed to develop a broader range of sources of information in order to prevent further serious damage to the reviewed investigation.	Due to the variety of factors inherent in each investigation, CSIS always considers how best to collect information and mitigate threats, drawing on a number of tools and resources - in accordance with the CSIS Act and ministerial direction - dependent on the situation.
NSIRA recommends that CSIS and the RCMP prioritize the deployment of usable and compatible secure communications systems in order to make regional de-confliction more efficient.	CSIS and the RCMP are prioritizing the deployment of compatible secure communication. The CSIS Director and the RCMP Commissioner approved the development of a CSIS-RCMP Secure Communications Strategy, the implementation of which is already underway.
NSIRA recommends that both CSIS and the RCMP continue to prioritize the timely implementation of recommendations from the Operational Improvement Review (OIR) in order to help address the operational shortcomings reported by the OIR and further illustrated in this review.	CSIS and the RCMP remain committed to implementing the OIR recommendations as well as the implementation of One Vision 3.0. The OIR resulted in 76 recommendations, some of which include enhanced collaboration and information sharing in national security investigations, additional training for national security personnel, as well as the improved handling and disclosure of sensitive and classified information. Significant effort has been undertaken to ensure recommendations are adopted and implemented within both organisations. Some of the early successes include pilot projects such as the Leads Pilot that has resulted in enhanced CSIS-RCMP de-confliction within national security areas of focus. The RCMP and CSIS continue to be fully supportive of implementing these needed changes to our organisations. This work, and efforts of the broader community, will ensure

	that the Government of Canada has a strong foundation of enhanced collaboration and the best tools available to mitigate threats and ensure public safety. This complex work however, is ongoing and challenges remain, particularly as it relates to the issue of intelligence and evidence. These significant challenges will require a whole-of-government approach in order to address.
NSIRA recommends that CSIS and the RCMP develop a properly resourced complimentary strategy to address the threat examined in this report. In accordance with the vision set out in the Operational Improvement Review, the strategy should consider the full range of tools available to both agencies.	CSIS and the RCMP coordinate and collaborate on national security threats and use strategies and resources best suited to individual operations. As a result of the OIR, discussions between CSIS and the RCMP are more frequent and occur earlier in the process which has reduced the duplication of efforts between both of our agencies.

Review of CSIS threat reductions activities

NSIRA's findings

1. For the types of threat reduction measures (TRMs) reviewed, NSIRA finds that CSIS met the requirements set out in ministerial direction as articulated in CSIS Policy and Procedures.
2. NSIRA finds that CSIS conducted a small number of interviews in a manner that was not reasonable and proportional as required by section 12.1(2) of the CSIS Act.
3. For a particular TRM, NSIRA finds that CSIS's selection of individuals for inclusion in the TRM reflected a strong rational link between the threat and the measure.
4. NSIRA finds that CSIS does not have a formalized and documented process to help guide the identification and selection of subjects for inclusion in TRMs that ensures proper accountability for these activities.
5. NSIRA finds that the implementation of certain TRMs was reflective of individual circumstances.

6. For a certain type of TRM, NSIRA finds that the requirements set out in Ministerial Direction were met.
7. NSIRA finds that CSIS did not adequately consider whether a *Charter* right would be limited by the reviewed TRM.
8. *Finding not releasable in public report.*
9. *Finding not releasable in public report.*

NSIRA's recommendations, and CSIS's response

Recommendations	CSIS Response (August 2021)
NSIRA recommends that CSIS create an accountability framework for information related to TRMs, and that this information be documented and retained in a central, easily retrievable location.	CSIS's robust governance framework for its TRM authorities has been the subject of review by both SIRC and NSIRA. As a result of these reviews, considerable adjustments have been made to the governance of TRMs. CSIS is developing an improved organisational case management tool. While that work occurs, CSIS is implementing interim measures to respond to NSIRA's recommendations. Finally, CSIS is leveraging additional communication methods to ensure awareness of the TRM specific requirements.
NSIRA recommends that CSIS create a formalized and documented process that ensures pertinent facts regarding TRM subjects are provided to the National Security Litigation and Advisory Group (NSLAG) to ensure that it has the information necessary to provide considered legal advice on the identification and selection of interviewees for inclusion in TRMs.	CSIS and the Department of Justice have a collaborative relationship that fosters discussion and allows for continuous engagement. When parliament established CSIS's threat reduction mandate, CSIS worked closely with the Department of Justice to develop an appropriate and robust governance framework. This framework includes a formal and documented process to seek a legal risk assessment as well as practical guidance regarding relevant information and level of detail required for TRM submissions.

	CSIS engages the Department of Justice to ensure all requirements of the CSIS Act are met including consideration that measures are reasonable and proportional to the threat and warrants are obtained if required. CSIS ensures this guidance is applied so that TRMs remain lawful and respect all Canadian laws, including Charter rights and freedoms.
NSIRA recommends that CSIS develop an accountability framework for compliance with legal advice on TRMs, including documenting when and why legal advice was not followed.	CSIS's compliance framework provides an opportunity to report instances of potential non-compliance with Ministerial Direction, internal policies or procedures, and the law. In instances where this may occur, CSIS's Compliance program remains well situated to complete requisite fact-finding and engage with the Department of Justice. The Department of Justice provides advice to ensure TRMs remain lawful and respect the right of Canadians. CSIS diligently applies these principles and guidance from the Department of Justice in the execution of all TRMs. While advice from the Department of Justice does not provide explicit and tactical directions on the execution of TRMs, CSIS considers all Justice advice during its operational deliberations.
NSIRA recommends that, when considering whether a Charter right is limited by a proposed TRM, NSLAG should undertake a case-by-case analysis that assesses factors identified in our report.	The Department of Justice will further consider this recommendation and factor it into its work related to TRM under the CSIS Act. CSIS and the Department of Justice will continue to build their long-established and collaborative relationship in order to improve and refine the governance of TRMs.

Communications Security Establishment reviews

Review of CSE's disclosures of Canadian identifying information to Canadian partners

NSIRA's findings

1. NSIRA found that CSE's disclosure personnel do not receive sufficient written training and guidance, and are not required to document key actions and assessments they make when releasing CII.
2. NSIRA found that CSE has not sufficiently assessed the legal authorities invoked by its clients.
3. NSIRA found that CSE's implementation of its disclosure regime may not have complied with its obligations under the *Privacy Act*.
4. NSIRA found that the management of CSE's CII disclosure regime does not foster an arrangement where its clients can take equal responsibility for the disclosure and collection of Canadians' personal information.
5. NSIRA found that the Federal Court has not been fully informed about CSE's disclosure of personal information about Canadians, particularly relating to Canadian officials, derived from the warrants it issues to CSIS in relation to section 16 of the *CSIS Act*. NSIRA found that CSE's disclosure practices contradict key principles previously outlined to the Court by CSIS.

NSIRA's recommendations, and CSE's response

Recommendation	CSE Response (June 2021)
CSE should enhance the rigour of its internal practices related to Canadian identifying Information (CII). Firstly, CSE should update its policies to require CSE personnel to document their assessments and rationales for approving or denying disclosure requests.	CSE accepts the recommendation. CSE is in the final stages of implementing an updated version of its CII request software. The new software will require a capture and documentation of the rationale for decisions relating to the disclosure of CII.
CSE should further improve the CII request system to ensure that clients are obligated to articulate clearly the legal collection authorities and operational rationales for receiving CII.	CSE accepts the recommendation. CSE is in the final stages of implementing an updated version of its CII request software, which will ensure that necessary information is mandatory and captured.

CSE should ensure that the role of its Client Relations Officers (CROs) is limited to facilitating the release of CII only when clients explicitly request it.	CSE accepts the recommendation. CROs will continue to facilitate the release of CII only in response to client requests. Additional training is currently being developed to ensure proper documentation of such requests.
CSE should train disclosure analysts to assess the substance and validity of CII disclosure requests. CSE should especially train disclosure analysts in applicable privacy law and policies, and the limitations on the sharing of personal information.	CSE accepts the recommendation. CSE, in working with Legal Services, has developed additional training materials to enhance its existing training for disclosure analysts. This additional training will be rolled out in the following few weeks.
CSE and its Government of Canada clients that request CII should obtain legal advice from the Department of Justice regarding the collection authorities that may justify the collection of personal information.	CSE accepts the recommendation. CSE is currently working on revising its standard operating procedures, which will be informed by the responses CSE received to the correspondence sent in relation to recommendation 5.
CSE should revise its Standard Operating Procedures to reflect the legal advice it receives in response to Recommendation 5.	CSE accepts the recommendation. CSE has sent correspondence to its client departments, highlighting areas of responsibility and suggesting that the client, together with their own Legal Services, confirm their lawful authority to request and receive CII.
NSIRA recommends that CSE cease disclosing CII to clients other than CSIS, RCMP, and the Canada Border Services Agency (CBSA) until it implements the recommendations contained throughout this report.	CSE accepts the recommendation. Requests to departments other than CSIS, the RCMP and the CBSA are being processed in collaboration with DLS to review the authorities provided by the requesting institutions.
NSIRA recommends that CSE work with the Department of Justice, the Treasury Board of Canada Secretariat, and its regular Government of Canada clients to establish Information Sharing Agreements. These agreements should clearly address each party's roles, responsibilities, and legal authorities related to collecting and disclosing CII, as well as the standards that each disclosure must meet.	CSE accepts the recommendation. CSE has already sent correspondence to its client departments highlighting areas of responsibility and suggesting that the client, together with their own Departmental Legal Services, confirm their lawful authority to request and receive CII. Discussions have taken placed with TBS on the use of ISAs with clients.
NSIRA recommends that a Privacy Impact Assessment be undertaken in relation to CSE's CII disclosure regime.	CSE accepts the recommendation. CSE has initiated a Privacy Impact Assessment.

CSIS, CSE, and the Attorney General of Canada should fully inform the Federal Court of CSE's practices related to the disclosure of CII and associated practices deriving from warrants issued by the Court.	CSE accepts the recommendation. CSE has coordinated closely with CSIS to provide the Federal Court with the necessary information.
NSIRA recommends that CSE cease disclosing CII collected pursuant to section16 of the CSIS Act until the Federal Court is fully informed about CSE's sharing of information derived from CSIS section 16 warrants. Until such a time, CSE should include a message in its section 16 intelligence reports directing requesters of CII to CSIS.	CSE accepts the recommendation. All s.16 CII requests are reviewed and approved by CSIS.

Review of CSE's ministerial authorizations and ministerial orders under the *CSE Act*

NSIRA's findings

1. The application requests from the Chief of CSE presented the Minister with sufficient information to meet the conditions of subsection 33(2) of the CSE Act. The new applications provide more information than previous applications under the *National Defence Act*, and allow for better transparency of CSE's activities.
2. Although these activities have not yet occurred, there is no indications that CSE has fully assessed the ramifications — legal or otherwise — of the activities authorized in a certain kind of authorization.
3. The 2019 letters in relation to the Minister of National Defence's consultation with the Minister of Foreign Affairs for Active and Defensive Cyber Operations were not dated. That specific consultation event with Global Affairs Canada was not sufficiently documented.
4. CSE was unable to provide an assessment of its obligations under international law relevant to the conduct of Active Cyber Operations.
5. The *Ministerial Order Designating Recipients of Canadian Identifying Information Obtained, Used, and Analyzed Under a Foreign Intelligence Ministerial Authorization* was insufficiently detailed.

NSIRA's recommendations, and CSE's response

Recommendation	CSE Response (May 2020)
CSE should seek a fulsome legal assessment on activities authorized by a specific Foreign Intelligence Authorization prior to undertaking any collection activities under this ministerial authorization (MA). The legal advice should address whether there is an implicit justification regime created in the MA.	CSE accepts this recommendation in principle. CSE believes that all the activities authorized by this MA have an explicit authority as stated in section 3 of the *Communications Security Establishment Act* (CSE Act), with the view that these activities are reasonable and proportionate, and fall under an Authorization issued by the Minister and approved by the Intelligence Commissioner. Furthermore, legal assessments form an integral part of the Authorization development process, with Legal Services Counsel forming part of the Authorization development team.
CSE should ensure that the Active Cyber Operations and Defensive Cyber Operations consultation process with Global Affairs Canada is documented as precisely as possible to allow for an easy verification of its compliance with the sequencing required in the CSE Act.	CSE acknowledges this recommendation and considers it resolved.
CSE should seek a formal legal assessment of the international legal regime applicable to the conduct of active cyber operations prior to undertaking any such operations.	CSE does not accept this recommendation. CSE agrees that its operations should be assessed with respect to compliance with international law but continues to dispute NSIRA's assertion that is was unable to provide an assessment of its obligations under international law. CSE will continue to work diligently with the Department of Justice legal counsel and Global Affairs Canada in respect of foreign cyber operations.
An order issued under section 45 of the CSE Act should be as precise as possible in clearly detailing the list of persons or classes of persons designated to receive Canadian Identifying Information disclosed by CSE.	CSE accepts this recommendation and notes that CSE's updated Ministerial Orders (MOs) have addressed this issue. In an effort to promote increased transparency and ease of external communications, CSE's three MOs were rewritten in 2020 at an unclassified security level. Issued to CSE by the Minister in August 2020, CSE MOs met the purpose and spirit of this recommendation well before the finalization of NSIRA's review report.

Review of CSE's Privacy Incidents File (2019)

Note that this review examined CSE's Privacy Incident File (PIF) in 2019, but is included in this Annex because it presents information that NSIRA was previously unable to publish—namely, CSE responses to NSIRA's recommendations. Findings for this 2019 review of CSE's Privacy Incidents File can be found published in the review online.[47]

Recommendation	CSE Response (March 2020)
CSE should look at the totality of all privacy incidents with the view to identifying systemic trends or any areas of weakness in existing policy or practices.	CSE accepts this recommendation. CSE will work to bolster its use of the privacy incidents management regime as a source of information to contribute to policy development and to identify potential improvements to existing practices.
The Operational Compliance teams should emulate best practices from each other for uniform reporting on privacy incidents so that an incident report is completed for every incident with a Canadian privacy interest.	CSE accepts this recommendation. CSE is pursuing a standardized mechanism for capturing, recording and reporting on incidents with a privacy interest. CSE is investigating a range of policy, procedural and technical solutions to reach more uniform reporting between business lines where applicable and necessary. Such a mechanism would also account for operational differences between foreign signals intelligence and Canadian Centre for Cyber Security activities.
CSE should always examine what may have already been done with the information with a Canadian privacy interest in order to determine if further mitigation measures are warranted in the circumstances of a specific privacy incident.	CSE accepts this recommendation. In assessing how to best achieve the outcome called for in this recommendation CSE is investigating a range of policy, procedural and technical solutions.
CSE should standardize the policy on how to assess whether a privacy incident constituted a material privacy breach. Furthermore, after an assessment of sensitive personal information occurs, CSE should develop methods for analyzing whether serious harm or injury has occurred that is not triggered solely on whether an action-on request was processed.	CSE accepts this recommendation. CSE will seek to enhance and standardize its documentation of whether a privacy incident constitutes a material privacy breach. CSE will also re-examine the elements used in its assessment to ensure they are effective and reasonable.

CSE should rescind a specific practice. Should it continue to use this practice as a mitigation measure, CSE should obtain a legal opinion on the lawfulness of the practice.	CSE accepts this recommendation. CSE abolished the practice in November 2019.

Reviews of other government departments

Review of the Canadian Forces National Counter-Intelligence Unit

NSIRA's findings

1. NSIRA found that a major impediment to the sustainability of CFNCIU investigative expertise is a high staff turnover rate and an overreliance on mentoring.
2. NSIRA found that CFNCIU adhered to internal policies used to initiate investigations, and these determinations were reasonable and necessary under the particular circumstances.
3. NSIRA found that CFNCIU does not have a formalized and documented process to help guide investigation prioritization.
4. NSIRA found that DND/CAF institutional structure and managerial decisions do not allow CFNCIU to make full use of its lawful investigative capabilities.
5. NSIRA found that, when considering the nature of a subject's privacy interest, CFNCIU does not adequately assess its activities with regard for the totality of the circumstances.
6. NSIRA found that investigative durations run contrary to the sound safeguarding of DND/CAF information, people and assets.
7. NSIRA found that CFNCIU's information sharing regime is not consistently compliant with Government of Canada policies for safeguarding information.
8. NSIRA found that the CFNCIU and other DND/CAF security components have been organized into narrowly focused vertical silos that are not aligned to work in an integrated manner.
9. NSIRA found that the CFNCIU does not have clarity on their legal authorities to share information in support of administrative and criminal processes.
10. NSIRA found that an absence of a finalized report shared with affected stakeholders does not ensure proper accountability over the Unit's investigative activities.

11. NSIRA found that there is insufficient oversight for CFNCIU investigations.
12. NSIRA found that white supremacy/Ideologically Motivated Violent Extremism (IMVE) poses an active Counter-Intelligence threat to the DND/CAF, and that the CFNCIU's mandate to proactively identify this threat is limited.

NSIRA's recommendations

1. NSIRA recommends that CFNCIU should create a formalized and documented process that assists with the prioritization of investigations based on relevant criteria (e.g. resources, value, institutional priorities, operational, legal and foreign policy concerns).
2. NSIRA recommends that DND/CAF empower CFNCIU to make full use of its lawful investigative capabilities, which may include less intrusive activities.
3. NSIRA recommends that CFNCIU should seek advice from the Office of the Privacy Commissioner of Canada to ensure that investigative activities adhere to all privacy protection best practices.
4. NSIRA recommends that CFNCIU sharing and accountability structures be compliant with the Policy on Government Security.
5. NSIRA recommends that CFNCIU investigative activities be aligned with the efforts of security screening activities to reduce redundancies.
6. NSIRA recommends CFNCIU seek advice on the legal authorities to share information in support of administrative and criminal processes.
7. NSIRA recommends CFNCIU must create an accountability framework that includes approved written products that are shared with affected stakeholders.
8. NSIRA recommends CFNCIU update is oversight mechanism to ensure that it is independent, meets routinely, and is supported by a secretariat that properly records pertinent information.
9. NSIRA recommends that DND/CAF clarify the CFNCIU's role within the larger DND/CAF strategy on addressing hateful conduct and extremism.

DND/CAF response to NSIRA's recommendations (June 2021)

Below is DND/CAF's response to NSIRA's recommendations contained in the review:

"DND/CAF recognizes the importance of review, and welcomes this report. DND/CAF agrees with the recommendations in this report, and is taking action to address them. All activities

of the Canadian Forces National Counter Intelligence Unit must adhere to all applicable Canadian laws and respect the provisions of the Charter of Rights and Freedoms. Although CFNCIU currently has no role with regard to the identification and elimination of Hateful Conduct, DND/CAF have taken a robust approach to dealing with hateful conduct, including a new CAF policy that will better enable us to deal with this issue. As recommended by NSIRA, DND/CAF will clarify the Unit's role within the context of the broader DND/CAF response to Ideologically Motivated Violent Extremism

The Unit has taken steps over the last years to improve its capacity, some of which directly pertain to the report. CFNCIU continues to evolve and improve to meet the demands of the ever-changing international, domestic and CAF-related security environment. The recommendations in this report range from unit-level changes to institutional considerations, and DND/CAF agrees that action will be taken at the appropriate levels in conjunction with required expertise and offices. DND/CAF has commenced this work and many of the recommendations in this report are already being addressed. This includes an interim tracking mechanism for information disclosure, a review of relevant policies and operational procedures. Additionally, work is underway to complete a Privacy Impact Assessment on Defence Intelligence activities including Counter-Intelligence investigation which will assess any risks to personal information with the CFNCIU investigation process and propose mitigations where necessary. DND/CAF will engage the Office of the Privacy Commissioner once the Privacy Impact Assessment is finalized to seek input on privacy protection considerations where necessary. Implementing NSIRA's recommendations will further improve our practices.

CFNCIU is a unit of the Canadian Forces Intelligence Group, under the Canadian Forces Intelligence Command. The Unit's mandate is to provide security intelligence and counter-intelligence to the Department of National Defence and Canadian Armed Forces, both at home and abroad. The Unit's mandate focusses on security threats in the domains of Terrorism, Espionage, Subversion, Sabotage and security threats posed by Organized Crime. CFNCIU investigates through its particular lens, and is part of the wider group of investigative and security bodies that exist within DND/CAF. CFNCIU is not a law enforcement agency, and does not have the authority to investigate disciplinary or criminal infractions. However, it often collaborates with law enforcement agencies such as the Military Police or the RCMP and will engage in further actions to improve that collaboration."

Cross-departmental reviews

Review of departmental implementation of the avoiding complicity in mistreatment by Foreign Entities Act

NSIRA's findings

1. NSIRA found that several departments, new to the considerations of the Avoiding Complicity Act, described considerable progress being made during the review period and afterwards to build out formalized frameworks to support implementation.
2. NSIRA found that departments conducting minimal information exchanges with foreign entities have not yet fully addressed the importance of having an official information sharing framework in place.
3. NSIRA found that the differences and variability in departmental frameworks demonstrate a previous lack of coordination across the community and a need to identify best practices.
4. NSIRA found that there are inconsistencies in the application of existing sharing frameworks between departments, specifically concerning information evaluation thresholds, and decisions being elevated for senior level determinations.
5. NSIRA found a lack of unification and standardization in the country and entity assessments being leveraged by departments, resulting in inconsistencies in approach/stance by the community when interacting with Foreign Entities of concern related to the Avoiding Complicity Act.

NSIRA's recommendations

1. NSIRA recommends that all departments in receipt of directions under the Avoiding Complicity Act have an official framework that ensures they can fully support the implementation of the directions.
2. NSIRA recommends that departments coordinate to identify best practices for all essential components of information sharing frameworks and that the Information Sharing Coordination Group is leveraged to ensure these practices are shared where possible across the community to support the implementation of the Avoiding Complicity Act.
3. NSIRA recommends that departments establish consistent thresholds for triggers in their information sharing frameworks, including initial evaluations against the

concerns of the Avoiding Complicity Act, when a case is to be elevated in the decision process, and how this is documented.

4. NSIRA recommends that departments identify a means to establish unified and standardized country and entity risk assessment tools to support a consistent approach by departments when interacting with Foreign Entities of concern under the Avoiding Complicity Act.

Response to NSIRA's recommendations (July 2021)

The Government of Canada generally agrees with the overall substance and spirit of the recommendations. Below is the government's response to the four recommendations contained in the review and a description of how the implicated departments and agencies intend to implement these recommendations over the coming months:

''The Government of Canada agrees with the report's first recommendation that all departments in receipt of directions under the Avoiding Complicity Act must have an official framework in place to ensure they can fully support implementation of the directions. As acknowledged in the report, within the first four months of the Avoiding Complicity Act coming into force, all twelve implicated departments and agencies had frameworks in place. These frameworks are tailored to the distinct circumstances of each department or agency. As the report highlights, there is still room for these frameworks to mature. To that end, the subject departments and agencies will continue to modify and formalize their respective frameworks where necessary to address the findings and support full implementation of the directions.

The Government of Canada agrees with the report's second recommendation that departments should work together to identify best practices for all essential components of information sharing frameworks and Public Safety Canada's Information Sharing Coordination Group will continue to be a well-placed forum to facilitate this work. The security and intelligence community will continue to leverage the Information Sharing Coordination Group to share best practices, lessons learned, and common interpretations to further enhance information sharing practices and fulfill obligations under the directions.

The Government of Canada only partially agrees with the report's third and fourth recommendations. These recommendations stress the importance of establishing consistent approaches across the security and intelligence community. The Government of Canada appreciates the view that consistent approaches can help to ensure reliable implementation of directions. Similarly, standardizing the community's country and entity risk assessment tools would promote a consistent starting point for assessing generalized risk of a foreign country or entity, potentially minimizing duplication of effort across

organizations. Subject departments and agencies will continue to leverage the Information Sharing Coordination Group to determine where consistency can be established in their processes, in line with the report's second recommendation. Departments and agencies will further work to identify where country and entity risk assessment tools can be standardized, and ensure that all organizations have access to baseline risk assessment tools.

That said, standardized approaches are not always feasible in practice. This is particularly true when applying one approach to twelve departments and agencies with diverse operational activities and mandates. The information sharing activities of these organizations all serve either an intelligence, law enforcement, or administrative purpose with each carrying different risk profiles, privacy concerns and legal authorities. Individual departments and agencies are responsible for establishing specific thresholds or triggers in their information sharing frameworks that are appropriate for their operational contexts.

It is the view of the Government of Canada that applying the same threshold across all organizations for triggering, evaluating and elevating cases is not necessarily practical nor essential to ensuring that each department or agency is operating in compliance with the Avoiding Complicity Act. Similarly, given the variety of legal mandates, operational activities, and sensitivity of information available to some departments but not others, it may not be feasible to produce an entirely standardized suite of risk assessment tools available to all organizations under the Avoiding Complicity Act."

Review of disclosure of information under the *Security of Canada Information Disclosure Act*

In 2020, NSIRA completed its *2019 Annual Report on the Disclosure of Information under the Security of Canada Information Disclosure Act*.[48] This inaugural report made no findings nor recommendations, but established criteria for future assessment.

Annex F: Statistical table: Complaint investigations

Complaint investigations: Final statistics

January 1, 2020 to December 31, 2020

INTAKE INQUIRES	**69**	
New complaints filed	**26**	
NSIRA Act, s. 16 (CSIS Complaints)	15	
NSIRA Act, s. 17 (CSE Complaints)	1	
NSIRA Act, s. 18 (Security Clearances)	8	
NSIRA Act, s. 19 (RCMP Complaints)	2	
NSIRA Act, s. 19 (Citizenship Act)	0	
NSIRA Act, s. 45 (CHRC Act)	0	
Complaint files NSIRA determined to investigate	**24**	
	Accepted:	**Declined:**
(CSIS)	s. 16: 3	s. 16: 10
(Security Clearances)	s. 18: 0	s. 18: 6
(RCMP)	s. 19: 4	s. 19: 1
Active complaint investigations during this time period	**19**	
Once NSIRA makes its determination to investigate…		
Complaint investigations carried over from previous calendar year	**12**	
(CSIS)	s. 16: 9	
(Security Clearances)	s. 18: 2	
(RCMP)	s. 19: 1	
Total complaint investigations closed	**5**	
Withdrawn / deemed abandoned	3	
Resolved informally	1	

Investigations completed (final report issued)	1
(CSIS)	s. 16: 3
(Security Clearances)	s. 18: 1
(RCMP)	s. 19: 1
Complaint investigations to be carried forward to the next calendar year	**14**
(CSIS)	s. 16: 9
(Security Clearances)	s. 18: 1
(RCMP)	s. 19: 4

Annex G: Values and goals

1. NSIRA is committed to:

   - being open and transparent, to keep Canadians informed about the lawfulness and reasonableness of its country's national security and intelligence activities;
   - maintaining methodological excellence, to ensure the rigor and quality of its approach;
   - fostering forward- and innovative-thinking, to keep abreast and, ideally, stay ahead of new technology and an ever-changing national security environment;
   - engaging regularly with partners, stakeholders, and community members; and,
   - being, as well as being seen to be, objective and independent.

   In its first full year of operation, NSIRA have continued to make strides in meeting these objectives and a full description of its values and goals can be found in the *2019 Annual Report*.

2. NSIRA wants Canadians to feel confident that the country's national security and intelligence activities are thoroughly reviewed for lawfulness, reasonableness and necessity.

Transparency

3. The *National Security Act, 2017*, states that "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."[49] NSIRA is therefore committed to keeping the public informed about the results of its reviews, investigations, and activities, while still protecting sensitive information. This includes efforts to improve public access to its reports and communicating clearly about how NSIRA delivers its mandate.

4. To that effect, NSIRA continues to work with departments and agencies to ensure that unclassified versions of its review reports, with findings and recommendations, are published and made available to the public. Some of NSIRA review reports are now on the agency's new, revamped website.[50]

5. Since its last annual report, NSIRA has proactively released unclassified review reports on:

   - CSE's self-identified privacy incidents and procedural errors;

- Departmental implementation of the *Avoiding Complicity In Mistreatment By Foreign Entities Act* for 2019; and,
- the sharing of Canadian-identifying information by the Communications Security Establishment.

6. Moreover, NSIRA has begun to redact, declassify, and release previous reports from the Security Intelligence Review Committee, the review body previously dedicated to reviewing activities of the Canadian Security Intelligence Service (CSIS). NSIRA has already published a decade's worth of reviews and continues to collaborate with CSIS to declassify the remaining reports and publish them as soon as available. NSIRA has experienced delays in these efforts, however, due to the pandemic.

7. NSIRA plans to introduce new search tools on its website, which houses these reports, to enable easy navigation of its online databases for both newly released and historical reviews and publications. Its new website also aims to raise awareness of NSIRA and its mandate, explain its review process, provide an easy process for submitting complaints online, and encourage stakeholders to engage with us. NSIRA has also established a twitter account to keep the public informed of NSIRA's activities.

8. Finally, NSIRA recently published a new policy statement on its commitment to declassify and de-personalize all complaints investigation reports going forward.[51] The aim of this policy is to improve access to NSIRA's investigations process, thereby enhancing its public accountability mandate. By making declassified and de-personalized reports publicly available, NSIRA hopes to encourage open discussions and debate.

9. In addition to its own initiatives to enhance accountability and transparency, NSIRA will continue to encourage departments and agencies to promote transparency of their national security and intelligence activities, including to fulfil the National Security Transparency Commitment.[52]

Anticipation of risk

10. As an organization that has recently expanded, acquiring talents from diverse backgrounds, NSIRA has the advantage of being able to influence attitudes that result in a culture of its own. NSIRA employees possess a diversity of backgrounds, cultural and professional, that allows it to ensure a plurality of expertise and experience, hence, a plurality of ideas and opinions. This range of expertise, experience, ideas and

opinions is complemented by looking for the best review practices based on other countries' experiences and relying on original internal training.

11. Thus, NSIRA possesses the tools required to anticipate the various risks that are part of each of the reviewed entities' mandate. The reviewers can ask the right questions, allowing them to recognize the reviewed entities entrenched ways and systemic behaviours, and to report to stakeholders with transparency and in a way that is consistent with their expectations. Specifically, to do that, the reviewers not only need to have clear expectations concerning the policies and procedures the entities should have adopted and implemented, but they also need to anticipate the risks the entities face and those they are or should be working on, be it for intelligence or prevention purposes. In other words, anticipation is part of the reviewer culture.

12. In summary, the culture of anticipation is inherent to NSIRA's quest for methodological excellence and to its recruitment and training program, and as well as being part of its relationship with foreign partners and stakeholders.

Objectivity and independence: An impartial approach

13. NSIRA's goal is to approach all of its reviews with unbiased objectivity. It does not look for particular outcomes in a review; instead, the focus and concern is only on how the review is conducted and presented. This professional ''indifference' to outcomes means NSIRA is free to concentrate on the information it requests and evaluates.

14. Each review explores specific questions; the information NSIRA seeks from departments and agencies is examined to help it find answers. NSIRA asks both the questions that the public trusts it to ask and those that NSIRA is obligated to ask under the provisions of its mandate. The continual strengthening of NSIRA's review process and methodology will ensure that this approach is executed in the most consistent way possible across all its reviews.

15. While public trust and transparency are important, it is also important that those being reviewed trust that NSIRA will engage with them in an impartial manner; reviewees must trust that when they open up their programs and operations to scrutiny, they will be evaluated in an unbiased fashion. This type of relationship provides the foundation for a review product that can provide value to both the public, and the government.

16. In this sense, NSIRA believes there is as much value in a review that has positive conclusions as there is in a review highlighting issues requiring attention.

17. A truly impartial approach goes hand in hand with principles like independence, transparency, and the trust but verify methodology. There must be obligations and considerations on both sides of the review and oversight relationship if NSIRA is to maximize the value and effectiveness of its reviews. NSIRA is aware of its obligations in this regard and will continue to consider ways it can improve and better hold up its side of this vital relationship.

Methodological excellence

18. NSIRA wants to improve the capacity of Canada's national security and intelligence community to conduct its activities in a manner that complies with the law, ministerial directions and appropriate operational policies. To do this, NSIRA must:

    - have the requisite understanding of the operational environment and the applicable legal requirements;
    - continuously engage in iterative learning;
    - ensure that its review and investigations processes are transparent and clear;
    - ensure that all relevant information is made available when conducting reviews;
    - be clear and precise when articulating findings and recommendations; and
    - monitor, document, and assess department and agency follow-up on recommendations.

19. To accomplish these objectives, NSIRA is focused on enhancing staff expertise in the national security operational environment, including the relevant legal and policy instruments, and building knowledge through iterative learning. To this end, NSIRA is developing a structured training program for NSIRA's review analysts, with a focus on sound and objective methodological principles, and establishing expert networks.

20. NSIRA is also developing a review framework to ensure consistency and clarity in the way it executes reviews. The framework is meant to provide systematic guidance on its approach and make its processes as transparent as possible.[53]

21. In 2020, NSIRA also reformed its complaints investigation model to better meet the goals of ensuring efficiency and transparency. Two priorities guided its efforts to modernize this process, namely, access to justice for self-represented complainants and the creation of streamlined, less formal procedural steps. NSIRA created new Rules of Procedures to reflect this new model, following extensive consultations with stakeholders in both the public and private sector. These new Rules have been in effect since July 2021.

Stakeholder and community engagement

22. NSIRA engages with expert, academic, and community stakeholders to raise awareness of its mandate, receive input on completed reports and guide future priorities, and create a shared understanding of best practices in reviews and investigations. The pandemic, however, required a rethink in its efforts to engage. NSIRA is currently seeking to expand its public engagement with various non-governmental stakeholders, including to receive input related to review topics and reporting, as well as to share information and awareness.

23. NSIRA is committed to cooperating with other federal review bodies with potentially overlapping mandates or objectives, namely, the National Security and Intelligence Committee of Parliamentarians (NSICOP), and the Civilian Review and Complaints Commission for the RCMP, as set out in the NSIRA Act. Additionally, as the NSIRA Act authorizes, NSIRA is committed to coordinating efforts with the Office of the Privacy Commissioner of Canada (OPC). NSIRA regularly engages with officials at all levels within these organizations to avoid unnecessary duplication with their respective mandates.[54]

24. For example, NSIRA has concluded a memorandum of understanding with the OPC to coordinate efforts, and to define respective roles, responsibilities and areas of expertise where there are potential areas of overlap. Similarly, NSIRA and NSICOP have agreed to share their respective review planning information to avoid overlap. In the context of their respective reviews of the Royal Canadian Mounted Police (RCMP), NSIRA and NSICOP staff attend joint information briefings to reduce duplication in requests to the RCMP.

25. NSIRA and NSICOP are seeking to harmonize their approaches to their separate duties to inform Cabinet ministers when they suspect that national security and intelligence activities may not comply with the law. The statutes that govern NSIRA and NSICOP each outline a duty to either report or inform using very similar language. To promote consistency in their approach, NSIRA and NSICOP have agreed to work toward a common standard.

Forward and innovative thinking with our FIORC counterparts

26. NSIRA also participates in international fora, including the Five Eyes Intelligence Oversight and Review Council (FIORC). FIORC brings together review bodies from Canada, Australia, New Zealand, the United Kingdom and the United States to discuss

international trends in national security and intelligence matters and to share best practices through unclassified conversations. Some of these conversations are meetings held at the multilateral level with all FIORC partners in attendance, while others are bilateral conversations on topics of shared interest.

27. NSIRA participates in three FIORC thematic working groups looking at key issues across jurisdictions. The artificial intelligence (AI) working group looks at the impact of AI technology in the context of national security and what it means for bodies that review how these technologies are implemented. This working group is also considering whether review bodies themselves can leverage new AI tools to improve their review capabilities.

28. The information sharing assurances working group is reviewing the practices in place to ensure that intelligence sharing does not lead to an increased risk of mistreatment for the subjects of the information shared.

29. Finally, the accountability gaps working group explores the remaining statutory and practical gaps in various jurisdictions with regard to the mandate, powers, access and resources of review bodies. NSIRA will continue to work with its Five Eyes partners through FIORC to encourage collaboration on transparency and accountability, and to address any potential gaps in accountability that exist with respect to international cooperation.

---

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

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

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

[4] NSIRA Act, subsection 38(1).

[5] Tabling of the National Security and Intelligence Review Agency's first Annual Report – NSIRA (nsira-ossnr.gc.ca)

[6] See also *2019 Annual Report*, pp. 20–51.

[7] The full reports are available in redacted form on NSIRA's website: https://nsira-ossnr.gc.ca/reviews

[8] This includes, but is not limited to: remaining independent and objective at all times while performing the work of the NSIRA Secretariat; embracing collaboration, new technologies and continuous learning; striving to maintain a high level of professional competence and expertise to fulfill duties and responsibilities; and, treating members of the

public, employees of other government departments and external stakeholders in a respectful and professional manner.

[9] Although presented as segments of a continuum, the stages of the information cycle are not necessarily distinct or unidirectional. Rather, they overlap and are often intertwined. Their grouping here simply assists in identifying and analyzing common themes that may emerge across government.

[10] In the 2019 Annual Report, we noted that future annual reports might adopt a different structure from the information continuum, depending on recommendations NSIRA receives and the information it wishes to communicate. (see *2019 Annual Report* p.21).

[11] S.C. 2019, c. 13 (former Bill C-59), s. 168.

[12] NSIRA Act, s. 32.

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

[14] *Canadian Security and Intelligence Service Act, R.S.C. 1985 c. C-23* (CSIS Act), subsection 12.1(1)

[15] An external review of the CSIS-RCMP operational relationship, titled the "Operational Improvement Review" (OIR), was completed by an external consultant. The OIR set out ambitious recommendations to improve the way in which CSIS and the RCMP cooperatively manage threats while managing the risks of CSIS disclosure to the RCMP. NSIRA recommends that both CSIS and the RCMP continue to prioritize the timely implementation of the OIR, which has the support of senior management in both organizations. NSIRA will, in the coming years, launch a review of CSIS's and the RCMP's implementation of the OIR to assess progress and take stock of the results.

[16] Published on July 16, 2020, the Federal Court's judgment in Sections 12 and 21 of the Canadian Security Intelligence Service Act, RSC 1985, c C-23 (Re), 2020 FC 616 found that CSIS had breached its duty of candour to the Court by failing to proactively identify and disclose that information used in support of warrant applications was likely derived from illegal activities. Following the recommendation of the Court that this matter receive further independent scrutiny, the Ministers of Public Safety and Emergency Preparedness and the Minister of Justice referred the matter to NSIRA. In response to the referral letter and pursuant to its own review mandate, NSIRA commenced a review of CSIS and the Department of Justice.

[17] Under the CSIS Act, CSIS is required to provide NSIRA information regarding the conduct of certain CSIS activities throughout the year: Reports by Director (CSIS Act, subsection 6(4)), Ministerial Direction (CSIS Act, subsection 6 (2)), the Justification Regime (*CSIS Act*, subsections 6(6) (a), (b) and (c)), Datasets (CSIS Act, subsections 11.25 (a), (b) and (c)), Threat Reduction Measures (CSIS Act, subsection 12 (3.5)), Cooperation Arrangements (CSIS Act, subsection 17(2)), Disclosure of Identity (CSIS Act, subsection 19(3)), and Unlawful Conduct of a CSIS employee (CSIS Act, subsection 20(2)).

[18] NSIRA is obligated under section 32 of the NSIRA Act to produce an annual classified report on CSIS activities for the Minister of Public Safety and Emergency Preparedness. One of NSIRA's predecessor organizations, the Security Intelligence Review Committee (SIRC), was required under the *CSIS Act* to certify the Director of CSIS's Annual Report to the Minister of Public Safety and Emergency Preparedness. The certification process drew on a range of information provided to SIRC, pursuant to the *CSIS Act*,

including reports of unlawful conduct by CSIS employees and CSIS's cooperation agreements with foreign organizations and governments. The certification process was also supported by the examination and assessment of large volumes of supplemental information requested by SIRC, which typically focused on CSIS activities of high risk with respect to lawful compliance.

[19] NSIRA Act, section 33.

[20] The Office of the Communications Security Establishment Commissioner was the organization tasked with reviewing CSE's legal compliance from 1996-2019.

[21] The Canadian-Identifying Information review: https://www.nsira-ossnr.gc.ca/wp-content/uploads/2021/06/10397868-001-EN-CII-Review-2018-19-1.pdf.

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

[23] This review did not examine the effectiveness of CSE's CII program with respect to its impact on national security.

[24] Section 16 of the *CSIS Act* refers to the collection of information concerning foreign states and persons.

[25] For further information, see section 1.5.

[26] In the case of CSE's foreign intelligence and cybersecurity mandates, the Intelligence Commissioner must approve these ministerial authorizations (MAs). The Intelligence Commissioner does not need to approve MAs issued under CSE's active cyber operation / defensive cyber operation mandates, nor does it approve activities under CSE's technical and operational assistance mandate — which themselves are not required to operate under an MA.

[27] *Communications Security Establishment Act* (S.C. 2019, c. 13, s. 76)(CSE Act), subsection21(1).

[28] Unlike many of Canada's allies, including all four of Canada's Five Eyes partners, the Government of Canada has not outlined its position on how international law applies in cyberspace.

[29] The PIF review, which reported a sample of incidents reported in the PIF from July 1, 2018 to July 31, 2019: https://www.nsira-ossnr.gc.ca/wp-content/uploads/2021/05/PIF_Report_Sept_2020_EN.pdf

[30] CSE was not able to provide all the data that NSIRA hoped to present in this Annual Report. For example, CSE was not willing to permit the publication of data related to the value of CSE reporting, numbers related to private communications, and ultimate use of collected communications and traffic items. In future annual reports, NSIRA will continue to push for permission to publish data of greater detail and variety, provided that the publication of this data is not deemed to be injurious to national security

[31] While NSIRA has no reason to dispute these assertions, NSIRA's mandate—in general—does not examine the impact of CSE's programs on national security outcomes.

[32] CSE uses the term FCOs to refer to both Active Cyber Operations (ACOs) and Defensive Cyber Operations (DCOs), which are authorized under sections 19 and 18 of the *CSE Act*, respectively. See CSE's 2020-2021 annual report: https://www.cse-cst.gc.ca/en/accountability/transparency/reports/communications-security-establishment-annual-report-2020-2021

[33] The Canadian Centre for Cyber Security (Cyber Centre, or CCCS) is Canada's unified authority on cybersecurity. The Cyber Centre provides expert guidance, services, and education, while working in collaboration with stakeholders in the private and public sectors. The Cyber Centre, which is a part of CSE, houses CERT-CA, which is comprised of the National CSIRT (Computer Security Incident Response Team), and the Government of Canada CIRT (Computer Incident Response Team).

[34] For example, New Zealand's Office of the Inspector-General of Intelligence and Security is required to evaluate and certify the 'soundness' of agencies' compliance systems in its annual reporting.

[35] NSIRA invites those with concerns related to CSE and its functions to contact us: https://nsira-ossnr.gc.ca/contact-us

[36] Under section 43 of the *CSE Act*, CSE may disclose to certain designated persons or classes of persons, information that could be used to identify a Canadian or a person in Canada, and that has been used, analyzed, or retained under certain kinds of authorizations — so long as CSE concludes that the disclosure is essential to international affairs, defence, security or cybersecurity.

[37] NSIRA has such access, for example, to CSIS' repositories. While NSIRA was generally satisfied with its access to CSIS in 2020, it felt that access to CSE in the same year was in need of improvement.

[38] Information that CSE is required to provide to NSIRA is referred to as "pushed" information, while information drawn from CSE by NSIRA is known as "pulled" information.

[39] As of June 2021, NSIRA's CSE Review Team comprised one manager and six analysts, in addition to significant assistance from several expert legal, technical, and other employees. The staffing of NSIRA's CSE Review Team continues in 2021.

[40] NSIRA Act, subsection 8(1)B

[41] This review is one of many NSIRA reviews that have examined, or will examine, various aspects of the safeguarding of Government of Canada people, information, and assets. 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*.

[42]Review Of Departmental Implementation Of The *Avoiding Complicity In Mistreatment By Foreign Entities Act* For 2019: Review Of Departmental Implementation Of The Avoiding Complicity In Mistreatment By Foreign Entities Act For 2019 - NSIRA (nsira-ossnr.gc.ca)

[43] *2019 Annual Report on the Disclosure of Information under the* Security of Canada Information Disclosure Act: https://nsira-ossnr.gc.ca/security-of-canada-information-disclosure-act

[44] NSIRA's webpage with complaints investigations reports: https://nsira-ossnr.gc.ca/complaints

[45] Note that sometimes work on reviews, including requests for information, began prior to finalizing the Terms of Reference. For example, substantive work began on the CSE Canadian-Identifying Information review in July 2020, and on the CSE Information Use and Sharing review in January 2020.

[46] For some reviews, NSIRA was unable to publish some or all such information in this year's annual report. Full executive summaries of most reviews discussed in this annual report are available upon request, should they not already be published on NSIRA's website at the time of this report's publication.

[47] Review of CSE's Self-Identified Privacy Incidents and Procedural Errors: https://nsira-ossnr.gc.ca/wp-content/uploads/2021/03/PIF_Report_Sept_2020_EN.pdf

[48] *2019 Annual Report on the Disclosure of Information under the* Security of Canada Information Disclosure Act: https://nsira-ossnr.gc.ca/wp-content/uploads/2020/12/SCIDA-NSIRA-Eng-Final.pdf

[49] National Security Act, 2017, Preamble.

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

[51] Policy statement to declassify and de-personalize complaints investigation reports (Microsoft Word): https://nsira-ossnr.gc.ca/wp-content/uploads/2021/02/Declassifed-depersonalize-policy-english.pdf#:~:text=POLICY%20STATEMENT%20NSIRA%20is%20committed%20to%20the%20fundamental,all%20classified%20content%20from%20every%20final%20investigation%20report.

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

[53] Further details on NSIRA's review framework are discussed in Annex C.

[54] NSIRA Act, sections 13 –15.