National Security and Intelligence Review Agency

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

UNCLASSIFIED

Review of the Communications Security Establishment's Disclosures of Canadian Identifying Information

Executive Summary

Subsequent to the collection of foreign signals intelligence by the Communications Security Establishment (CSE), any incidentally collected Canadian identifying information (CII) is suppressed in CSE's intelligence reporting to protect the privacy of Canadians and persons in Canada. However, the Government of Canada (GC) and foreign clients of such reports can request the details of this information if they have lawful authority and operational justification.

The National Security and Intelligence Review Agency (NSIRA) conducted a review of CSE's disclosures of CII to GC clients. In reviewing disclosures containing 2,351 Canadian identifiers over a five year period, NSIRA found that 28% of requests from all clients were not sufficiently justified to warrant the release of CII. . Nevertheless, during the period under review, CSE approved 99% of these requests for CII from its domestic clients. Given this and other findings related to CSE's internal practices, NSIRA found that CSE's implementation of its CII disclosure regime may not be in compliance with the *Privacy Act*.

Moreover, NSIRA found that CSE has released CII to GC clients from its technical and operational assistance to the Canadian Security Intelligence Service (CSIS) in relation to section 16 of the *CSIS Act,* in a manner that was likely not communicated to the Federal Court by CSIS.

This report is a summary of the more detailed, classified report provided to the Minister of National Defence on November 25, 2020.

P.O. Box / C.P. 2430, Station / Succursale "D"
Ottawa, Canada K1P 5W5
Tel: *1-833* 890-0293 Fax: *613* 907-4445

Introduction

1. The Communications Security Establishment (CSE) may incidentally acquire information about Canadians or persons in Canada in its collection of foreign signals intelligence (SIGINT). Canadian identifying information (CII) refers to any information that can identify an individual, ranging from names to email addresses and IP addresses. CII is suppressed in intelligence reports to protect the privacy of Canadians and persons in Canada. Government of Canada (GC) and foreign clients may subsequently request the details of this information if they have lawful authority and operational justification to collect it. This information sharing regime has been in place since the 2001 enactment of CSE's powers under the *National Defence Act*, and has been previously reviewed by the Office of the CSE Commissioner (OCSEC)

2. Following a review of CSE's disclosures of CII, the National Security and Intelligence Review Agency (NSIRA) concluded that CSE's implementation of its disclosure regime may not be in compliance with the *Privacy Act*. Therefore, pursuant to subsection 35(1) of the *NSIRA Act*, NSIRA submitted a compliance report to the Minister of National Defence on November 25, 2020.

3. CSE's disclosure regime, in place for nearly two decades, is one of the most important national security information sharing structures in the federal government, surpassing the volume of disclosures processed through the information sharing mechanism under the *Security of Canada Information Disclosure Act* (SCIDA). Unlike CSE's disclosure regime, information sharing processes under SCIDA have recently undergone comprehensive scrutiny and debate both in Parliament and by the public as part of the deliberation of Bill C-59.

4. CSE's work results in special responsibilities to protect the privacy of Canadians. In this context, NSIRA assessed CSE's operational structures, policies, and processes to determine the rigour of the CII disclosure regime. NSIRA found serious problems with several aspects of the governance and implementation of CSE's CII disclosure regime. NSIRA also found that CSE discloses information collected pursuant to the authority of Federal Court issued warrants as part of its assistance to the Canadian Security Intelligence Service (CSIS). NSIRA believes that although the Federal Court is aware of CSIS' disclosure of CII, the Court may not have been fully informed about the parallel disclosure process taking place at CSE. In January 2021, CSIS provided the Federal Court with a copy of NSIRA's full, classified review, excluding information protected by solicitor-client privilege.

Methodology

5. As part of its review, NSIRA examined a selected sample of CII disclosures and their associated intelligence reports – initially from July 1, 2018 to July 31, 2019, though the review period was later expanded to cover July 1, 2015 to July 31, 2019 for certain types of disclosures. Over that period, CSE received requests for 3,708 Canadian identifiers. NSIRA received information about the outcome of all of these requests. Additionally, NSIRA was able to closely review requests pertaining to 2,351 identifiers.

6. In all, NSIRA examined electronic records, correspondence, intelligence reports, legal

opinions, policies, procedures, documents pertaining to judicial proceedings, Ministerial Authorizations, and Ministerial Directives of relevance to CSE's CII disclosure regime. CSE also responded to NSIRA's questions throughout the review.

7. While this began as a review of solely CSE, it became evident that NSIRA also needed to engage with CSE's Government of Canada clients of CII. In the spirit of its legislation, NSIRA "followed the thread" by engaging with a range of federal departments, from recurring clients of CII, such as CSIS and the Royal Canadian Mounted Police (RCMP), to less frequent clients, such as Innovation Science and Economic Development Canada (ISED). Through this engagement, NSIRA was able to understand the lifecycle of CII disclosures, from their origin within intelligence reporting to their eventual use by Government of Canada clients.

8. NSIRA also assessed CSE's disclosures of CII arising from its assistance to CSIS in relation to section 16 of the *CSIS Act*. When CSE assists CSIS in that context, it is bound by the applicable Federal Court warrants' conditions. While CSIS' disclosures were not the subject of this review, they helped contextualize the adherence of CSE's section 16 CII disclosures with the conditions and principles on which the Court issued the relevant warrants.

9. NSIRA also reviewed CSIS affidavits to the Federal Court in relation to Canadian information acquired through section 16 warrants, which served as the basis for a recent decision issued on this program by the Court (reported as 2020 FC 697). Given this window into the parallel practices and policy requirements of CSIS, NSIRA had the opportunity to contextualize CSE's disclosures of CII arising from section 16 collection in a way that was unprecedented for an external review body.

10. Based on the records provided by CSE, CSIS, and other federal government entities, NSIRA made several findings and recommendations to improve the governance of CSE's CII disclosure regime and to bring to the attention of the Federal Court important aspects of CSE's disclosures of information acquired in relation to section 16 of the *CSIS Act*.

Legal framework

11. For CSE to disclose Canadians' personal information without their consent, both CSE and the CII recipient must comply with relevant legislation, which, for the period under review, consisted of the *Privacy Act* and the *National Defence Act*:

GC client's authority to collect	CSE's authority to disclose	CSE's requirements
• *Privacy Act*, section 4 • "No personal information shall be collected by a government institution unless it relates directly to an operating program or activity of the institution."	• *Privacy Act*, paragraph 8(2)(b) • "Personal information under the control of a government institution may be disclosed ... in accordance with any Act of Parliament."	• *National Defence Act*, paragraph 273.64(2)(b) • CSE's activities were "subject to measures to protect the privacy of Canadians in the use and retention of intercepted information."

12. In assessing CSE's disclosures, NSIRA applied a two-pronged test in line with the *Privacy Act* requirements: the institution holding the personal information must have a disclosure authority to disclose it to another institution, and the recipient institution must have a collection authority. These thresholds derive from existing *Privacy Act* jurisprudence. In other words:

- CSE's CII clients are required to meet the section 4 collection requirement of the *Privacy Act* by establishing a direct and immediate relationship (with no intermediary) between the information to be collected through a CII request and their operating programs or activities.
- On CSE's side, its disclosures of CII had to comply with section 8 of the *Privacy Act*, and the *National Defence Act*, which was the governing statute for CSE during the review period.
- Because the disclosure authority within the *National Defence Act* required CSE to protect the privacy of Canadians, NSIRA assessed whether CSE evaluated each disclosure request rigorously on its own merits, including the operational justification provided by clients, to determine whether the requests were reasonable and whether the disclosure was appropriate under the *Privacy Act* regime.

CSE's internal practices

13. NSIRA assessed CSE's privacy protection measures for compliance with its legal responsibilities and Ministerial Direction. NSIRA assessed whether CSE's CII disclosures are subject to a thorough, well-documented evaluation and approval process that demonstrates each disclosure's compliance with legal and operational requirements. Specifically, NSIRA assessed whether CSE's clients demonstrated their legal authority to collect CII, and did so in compliance with section 4 of the *Privacy Act* by showing a direct and immediate relationship between their mandated activities and the requested CII.

14. During the period under review, CSE received requests for 3,708 identifiers from 15 domestic departments, releasing 3,671 – which represents a release rate of 99%. This release rate was also reflected in the eventual sample of disclosures selected for detailed review by NSIRA. NSIRA expected to find disclosure requests of a consistently high quality commensurate with their near-absolute approval by CSE. Nevertheless, the findings below represent several areas in which NSIRA observed shortcomings.

Employee training and documentation requirements

15. CSE employees generally decide whether to release CII. NSIRA did not find evidence of written guidance or training to guide employees' assessment of the substance of disclosure requests; instead, the training materials and procedures that employees receive primarily focus on the logistical processes to release CII.

16. In their assessment of CII requests, CSE personnel can take a range of actions, including conducting further research into a requesting department and its mandate or communicating with the requester to obtain clarity. NSIRA found that these actions are generally not documented for requests from domestic clients, and the approved disclosures only contain the requested CII without the reasons for approving the request. NSIRA was unable to confirm that CSE personnel were taking steps to communicate with a requestor to clarify incomplete or unclear disclosure requests.

17. While this is not a requirement in CSE's policies for domestic requests, NSIRA observed detailed rationales provided by personnel responsible for approving and denying CII requests originating from foreign clients for CII. NSIRA believes CSE should require employees to document their assessment of requests from domestic clients, including the rationale for their approval.

18. In sum, NSIRA found that CSE's employees do not receive sufficient written training and guidance on assessing the substance of disclosure requests and are not required to document mandatory actions and assessments they make when releasing CII. NSIRA recommended that CSE require, through procedures and policy, that employees document their decision-making and rationales and train them to assess the substance of disclosure requests in light of applicable legal obligations.

Management oversight

19. Certain types of disclosures are elevated for review and approval at a higher level within the organization. This is another process that lacked the appropriate documentation. Based on data compiled by NSIRA, all requests for CII reviewed at this level were approved, with no documentation of the rationale behind the decision to approve the remainder.

20. An internal monthly compliance check is conducted to confirm that releases of CII follow sufficient justification, that only the requested CII is released, and to determine whether any procedural errors have occurred. The compliance checks reviewed by NSIRA did not contain any analysis of the disclosure requests. While CSE explained that employees are informally coached if disclosures do not meet requirements, this is not documented within the compliance checks, which provide only statistical summaries of CII disclosures.

21. NSIRA found that personnel responsible for approving certain CII disclosures and conducting periodic compliance checks did not document their decision-making and assessment of requests. NSIRA recommended that similar to employees at the working level, CSE management must document their decision-making and rationales.

CSE's assessment of CII disclosure requests

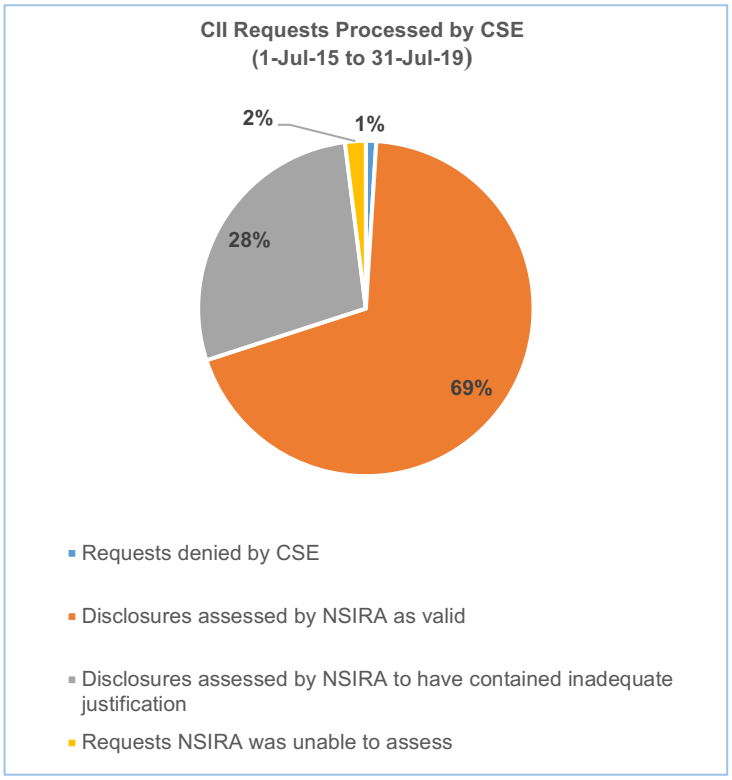
22. CSE's CII disclosure request form requires that the requestor state an applicable legal authority for collecting the information. NSIRA observed requests where this information was not provided. In this context, NSIRA expected that CSE would follow up with requestors or assure itself through its own assessment that the requestor had the appropriate legal authority for collecting CII. NSIRA found no evidence that this process was taking place.

23. NSIRA used its ability to follow the thread of a disclosure and engaged some of CSE clients for CII regarding their legal authority to collect Canadians' personal information. Where these departments had not indicated a legal authority to receive CII, NSIRA inquired directly with them about their legal authorities, receiving detailed legal assessments prepared in response to NSIRA's questions. NSIRA found no documented evidence that CSE had similarly assured itself of the clients' legal authorities at the time of disclosure.

24. As the custodian of incidentally collected CII, CSE has the responsibility to assure itself and document that both a collection and disclosure authority exist before sharing it with third

party clients.

25. Next to a legal authority, the second key component of a disclosure request is the recipient's operational justification for collecting the CII. A demonstrable operational nexus is required to justify a requester's collection of CII in line with the *Privacy Act* regime.



26. NSIRA found that CSIS, the RCMP, and the Canada Border Services Agency (CBSA) generally demonstrated a clear link between the intelligence reporting and associated CII to their mandated activities, with some exceptions. This was a result of the strong operational justifications provided proactively by these clients, and does not reflect a more rigorous process on CSE's end. Disclosures to these departments comprised approximately half of NSIRA's sample.

27. CSE has accepted operational justifications provided by these and other clients that NSIRA found to be inadequate. In these cases, the clients' justifications pertained to CII that was not demonstrably related to their mandate or operations.

28. From the sample of all disclosures reviewed by NSIRA, we found 69% to be justified, 28% to be insufficiently justified to warrant the release of CII, 2% that could not be evaluated, and 1% that CSE denied. Nevertheless, within this sample, CSE had approved these disclosure requests at a 99% rate.[1]

29. CSE also released additional personal information to clients beyond that which was requested and explained this to be a standard practice. For example, NSIRA observed cases where CSE disclosed Canadians' names and other personal information even when the recipient only asked CSE for a company's identity. NSIRA observed other types of scenarios where CSE disclosed more identifiers than requested.

30. In sum, NSIRA found that CSE has not sufficiently assessed the legal authorities invoked by its clients and recommended that CSE and these clients obtain legal advice from the Department of Justice to determine the extent of their legal authority to collect CII. NSIRA further found that CSE's implementation of its CII disclosure regime may not have been in compliance with the *Privacy Act* framework and recommended that CSE cease disclosing CII to clients other than CSIS, RCMP, and CBSA until it addresses the findings and recommendations contained in NSIRA's review.

[1] These figures, in addition to the figures in the chart, are rounded.

CSE's governance of the disclosure regime

31. Many of the systemic issues presented in NSIRA's review arise from CSE's CII disclosure regime governance. CSE develops its internal policies, procedures, and legal assessments to which its disclosure clients are generally not privy. CSE's existing arrangements with its clients govern operational issues such as security standards, information handling and system access. However, at an institutional level, NSIRA has not found a consistent understanding among CSE's CII disclosure clients of the legal requirements underlying this practice.

32. A more transparent governance structure would allow all parties to understand and formally acknowledge at an institutional level the legal and operational requirements behind disclosing and collecting CII. It is not sufficient for CSE to manage the regime with its clients not privy to the policies, procedures, and legal requirements that underlie it.

33. NSIRA found that CSE's governance of the CII disclosure regime does not foster an environment where its clients can take equal responsibility for CII disclosures. NSIRA recommended that CSE work with the Department of Justice and the Treasury Board of Canada Secretariat to establish Information Sharing Agreements with its regular domestic clients.

CSE's disclosure of CII collected through its assistance to CSIS

34. Throughout the review, NSIRA encountered reporting and associated disclosures that pertained to activities of foreign persons within Canada. As CSE is prohibited from directing its activities at such persons, NSIRA submitted a series of questions and received briefings on the subject. NSIRA learned that CSE discloses CII collected as part of its assistance to CSIS in relation to section 16 of the *CSIS Act*.

35. Under section 16 of the *CSIS Act*, CSIS may assist the Minister of Foreign Affairs or the Minister of National Defence by collecting foreign intelligence within Canada in relation to Canada's defence or international affairs. In turn, CSIS can apply to the Federal Court for a warrant, under section 21 of the *CSIS Act,* to obtain judicial authorization for intrusive collection powers in support of the section 16 investigation. Subsequently, CSIS may request CSE assistance if it does not have the tools or capacity to carry out this collection. CSE's assistance takes the form of developing tools and techniques, intercepting target communications, decryption, report writing, and translation.

36. In its assistance to CSIS, CSE must respect the legal authorities and limitations imposed on CSIS by law and Federal Court warrants. In its documented requests for CSE assistance, CSIS does not explicitly request that CSE disclose the CII collected under warrant. Such disclosures are also absent from internal CSE plans that set out CSE's support parameters. At the same time, both agencies insist that CSE can disclose such CII using its regular disclosure policies and procedures.

37. The practice of handling CII incidentally collected pursuant to section 16-related warrants has been the subject of ongoing treatment by the Federal Court. CSIS has described its own practices to the Court, including detailed summaries of how section 16 information is

collected, its processing for intelligence reporting, and the rigorous disclosure regime associated with this reporting. CSIS also noted, in less detail and with omissions, some aspects of CSE's parallel disclosure of CII collected through its assistance to CSIS under these warrants.

38. Overall, the stringent practices described by CSIS to the Court do not present a complete picture. For instance, CSIS's limited distribution of section 16 intelligence reports and associated CII is not mirrored in CSE's wider release of this information. Additionally, the senior approval levels that CSIS has in place for disclosing information about Canadian officials are also not reflected in CSE's practices. In fact, CSE does not have a policy on how to treat Canadian officials' information through its assistance mandate, and generally releases it at the working level. Further, CSE personnel are not generally aware that the information they are releasing originates from section 16 collection, and its associated Federal Court warrants and conditions. Moreover, CSIS has communicated to the Court that its own disclosure practice includes an assessment of a disclosure request by the operational branch responsible for the warrant, while CSE discloses such CII independent of CSIS operational branches.

39. In recent testimony before Parliament, CSE was asked how it operationalizes its assistance mandate. In its response, CSE stated that information collected under assistance is segregated, returned to CSIS, and belongs to CSIS, emphasizing that CSE effectively acts as an agent of CSIS in supporting section 16 activities.[2] NSIRA is of the view that this is not a complete representation of the lifecycle of information collected by CSE in its assistance. By approving CSE's section 16 intelligence reports, CSIS effectively releases ownership of this information to CSE, which was not conveyed to the Federal Court by CSIS in its affidavits detailing the reporting and use of section 16 information.

40. CSE's treatment and dissemination of this information differs from the stringent standards communicated to the Court by CSIS, particularly when it pertains to Canadian public officials and other sensitive groups. NSIRA believes that fully describing the CII disclosure process during warrant applications is necessary to support the process of imposing any terms and conditions advisable in the public interest, as contemplated by paragraph 21(4)(f) of the *CSIS Act*.

41. Given the findings of the review, NSIRA recommended that the Federal Court be fully informed of CSE's disclosure practices and that, in the interim, CSE cease disclosing CII incidentally collected under the authority of federal court warrants related to section 16 investigations.

Conclusion

42. NSIRA's findings and observations over the course of this review indicate that CSE's implementation of its disclosure regime may not be in compliance with its obligations under the *Privacy Act*. Throughout this review, CSE has defended practices that NSIRA believes do not reflect a commitment to rigorous implementation of the *Privacy Act*. Finally, CSE has released

[2] Standing Committee on Public Safety and National Security, Number 101, 1st Session, 42nd Parliament, Thursday March 22, 2018. https://www.ourcommons.ca/DocumentViewer/en/42-1/SECU/meeting-101/evidence

CII as part of its assistance to CSIS in a manner that contradicts the procedures communicated to the Federal Court.

43. Accordingly, NSIRA made a number of recommendations as outlined above, to improve the governance of CSE's CII disclosure regime and to bring to the attention of the Federal Court important aspects of CSE's disclosures of information acquired in relation to section 16 of the *CSIS Act*.

CSE Management Response to NSIRA Review of 2018-2019 Disclosures of Canadian Identifying Information

May 31, 2021

NSIRA delivered its classified review to the Minister of National Defence in November 2020.

Throughout NSIRA's review of CSE's disclosure process, CSE responded to NSIRA requests in a timely manner and offered to provide additional context and briefings to NSIRA regarding CSE processes.

Importance of independent external review

CSE values independent, external review of our activities, and we remain committed to a positive and ongoing dialogue with NSIRA and other review and oversight bodies.

This oversight frameworks allows us to deliver our important mission of foreign intelligence, cyber security and foreign cyber operations in a way that demonstrates accountability, and that builds trust and confidence with Canadians.

CSE operates within a culture of compliance, grounded in our understanding of and commitment to our legal and policy regime, and evidenced by our record of self-reporting and addressing incidents and errors that may occur.

We appreciate NSIRA and their continued work to provide Canadians with greater insight and understanding of the important work that CSE does on a regular basis to keep Canadians safe.

We accept the recommendations aimed at improving our processes, yet are concerned that the overall conclusions do not fully appreciate CSE's commitment to, and work on protection of privacy.

Canadian Identifying Information and CSE's Commitment to Privacy

CSE is Canada's national lead for foreign signals intelligence and cyber operations, and the national technical authority for cybersecurity. We provide critical foreign intelligence and cyber defence services for the Government of Canada (GC). Protecting Canadian information and the privacy of Canadians is an essential part of our mission.

CSE does not direct its foreign signals intelligence activities at Canadians or anyone in Canada. The *CSE Act*, however, recognizes that incidental collection of Canadian communications or Canadian information may occur even when targeting only foreign entities outside Canada. CSE takes very seriously our responsibility to protect Canadian privacy interests that may occur as a result of this incidental collection.

In the event that Canadian information is incidentally acquired in foreign signals intelligence collection, CSE may include obfuscated references to Canadian individuals or organizations in intelligence reporting if those references are essential to understand the foreign intelligence.

The obfuscation of this Canadian Identifying Information (CII) in reporting represents one of many layered privacy measures that are applied at different points in CSE's end-to-end intelligence process. These include, among others, legal and policy training and on-site support for intelligence analysts, mandatory annual privacy tests for all operational employees, data tagging and auto-deletion, strict retention limits, specific handling guidelines, escalating approvals for reporting that includes CII, compliance spot checks, and separate vetting processes for disclosing obfuscated information and taking action on intelligence reporting.

Pursuant to the *Privacy Act*, government clients who receive CSE foreign intelligence reports may ask for obfuscated CII to be "disclosed" to them if that information relates directly to their department's operating program or activities. Any disclosed CII is provided solely to inform their understanding of the foreign intelligence presented in the report. Government officials may not take action, share or otherwise use the CII disclosed to them under the disclosure process.

CSE continually refines its CII disclosure process. For example, to help support audit and review, CSE implemented a requirement for government clients to provide an operational justification to support their CII disclosure requests. It is important to note, however, that this is a matter of internal policy and that the *Privacy Act* does not require the documentation of legal authorities before information can be collected and disclosed.

Review Recommendations

CSE is committed to continuous improvement. We know that the recommendations from independent external review play an important role in that improvement. CSE has 25 years of experience working with the Office of the CSE Commissioner and now NSIRA to help improve our processes. We thank these review bodies for their work to help build trust and confidence with Canadians.

CSE continuously refines our privacy-protection measures, including those associated with the disclosure process. Improvements made over the past decade have been informed by the recommendations made by the CSE Commissioner as part of his annual reviews of CSE's CII disclosures. Prior to NSIRA taking over review duties, CSE had accepted and implemented 95% of the recommendations made by the CSE Commissioner. Those not adopted were duplicative or overtaken by events such as new legislation. In his final 2018-2019 review, the Commissioner confirmed that CSE's disclosures of CII complied with the law and were done in accordance with ministerial direction.

In this NSIRA review, as with previous CSE Commissioner reviews, we appreciate and have accepted the recommendations aimed at improving our internal policies and practices.

Given the overlap in this review period between the two bodies, certain NSIRA recommendations duplicate some presented in the CSE Commissioner's reviews. As a result,

we are pleased to note that many have already been implemented at this time; other NSIRA recommendations are in the process of being implemented.

Review Findings

Throughout this CII disclosure review, CSE provided extensive feedback and context to NSIRA, and sought clarification regarding the assessment criteria used to determine adequacy or inadequacy of specific records, the vast majority of which were deemed adequate by NSIRA. Without explaining the methodology used to support the findings, we are concerned that broad generalizations based on specific aspects of certain records within a single privacy measure may leave the reader with an incorrect impression about CSE's overall commitment to privacy protections for Canadians.

CSE's case-by-case process for disclosing CII to authorized GC recipients is part of robust and comprehensive internal measures that protect Canadians' privacy. We balance the sharing of our intelligence with the privacy and safety of Canadians at all times. CSE disclosure analysts receive training and follow internal policies, guidelines and standard operating procedures to guide decision making.

While committed to implementing the recommended process improvements contained in the report, CSE remains concerned by NSIRA's overall conclusions and characterization of the disclosure process and its role in the broader privacy framework, which we have expressed to NSIRA.

Referral to Attorney General of Canada

The Minister of National Defence submitted NSIRA's classified report to the Attorney General of Canada in January 2021, supported by a comprehensive analysis of each record identified by NSIRA in its review.

The analysis supports the view that our activities, including applying protections for the privacy of Canadians, were conducted within a robust system of accountability, including compliance with the *Privacy Act*.

Additional Information

Top Secret-cleared and special intelligence-indoctrinated GC clients received thousands of foreign intelligence reports via CSE's mandate under the *CSE Act*. These reports corresponded to Cabinet-approved intelligence priorities and were delivered to government clients who had both the authority to receive them and the 'need to know' their contents.

These reports reflect a wide range of intelligence requirements, from support to Canadian military operations, espionage, terrorism and kidnappings to geostrategic concerns, cyber threats, foreign interference and global crises, among others. While only a very small percentage of these reports contain obfuscated CII, the underlying Canadian information is often essential for GC officials to understand the context of the threat and its Canadian nexus.