National Security and Intelligence Review Agency

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

Notwithstanding any security markings appearing on this record, the information contained herein is declassified to UNCLASSIFIED

TOP SECRET // SI //

[redacted] CEO

CSE'S DISCLOSURES OF CANADIAN IDENTIFYING INFORMATION (CII)

(NSIRA REVIEW 08-501-3)

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

Notwithstanding any security markings appearing on this record, the information contained herein is declassified to UNCLASSIFIED

Notwithstanding any security markings appearing on this record, the information contained herein is declassified to UNCLASSIFIED

I EXECUTIVE SUMMARY

1. (U) CSE may incidentally acquire information about Canadians in its collection of foreign signals intelligence (SIGINT). The information is then suppressed in intelligence reports to protect the privacy of Canadians. Government of Canada (GC) client departments and foreign partners may subsequently request the details of this information if they have a lawful authority and a robust operational rationale to collect this information.

2. (U) The National Security and Intelligence Review Agency (NSIRA) examined a selected sample of CII disclosures and their associated intelligence reports – initially for the period of 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. NSIRA reviewed requests pertaining to [redacted] Canadian identifiers, from a total of [redacted] requests for identifiers processed by CSE in the review period. In all, NSIRA examined electronic records, correspondence, intelligence reports, legal opinions, policies, procedures, documents pertaining to judicial proceedings, Ministerial Authorizations, and Ministerial Directions of relevance to the disclosure sample. CSE also provided responses to NSIRA's questions throughout the review, delivering CSE's institutional positions on a range of issues related to the disclosure process.

3. (U) While the review began as a review of CSE's activities, it became evident that CII involves its GC client departments to a degree that required direct engagement with them. In the spirit of its founding legislation, NSIRA 'followed the thread' by engaging with a range of federal departments, from CSE's recurring clients such as the Canadian Security Intelligence Service (CSIS) and the Royal Canadian Mounted Police (RCMP) to less frequent clients such as Innovation, Science, and Economic Development Canada (ISED). As a result, NSIRA was able to understand the lifecycle of CII disclosures, from their origin within intelligence reporting to their eventual use by GC clients.

4. (U) NSIRA also assessed disclosures of CII by CSE that arise from its assistance to CSIS in relation to section 16 of the *CSIS Act*. While entities such as the Federal Court have jurisdiction over CSIS activities conducted pursuant to warrants, and previously the Office of the CSE Commissioner (OCSEC) held the mandate to review CSE, no organization until NSIRA had the opportunity to observe disclosures of CII arising from this program in both organizations. While CSIS' disclosures were not the subject of this review, they helped to contextualize those that occur within CSE. NSIRA also reviewed CSIS affidavits to the Federal Court in relation to Canadian information acquired through section 16 warrants.

5. (U) NSIRA found that while CSE has taken steps to improve its internal practices related to disclosure of CII, certain aspects of the disclosure regime lack rigour. CSE disclosure analysts and supervisors do not document the rationales for deciding to release CII, and the supervisor does not document any compliance issues as part of their monthly compliance checks of disclosures. This poses a challenge to assessing the validity of the decision-making.

6. (U) CSE has taken the position that it is not responsible for assessing how its clients' legal authorities allow for the collection of CII. The majority of the legal assessments presented to NSIRA by CSE's clients to substantiate their collection authorities were prompted by NSIRA's inquiries, and did not exist at the time of disclosure. NSIRA found this to be insufficient. All parties should be able to demonstrate that both a collection and disclosure authority exist prior to information about Canadians being shared among institutions. CSE and its GC clients should institute a more transparent and equitable governance structure for the disclosure of CII that puts both parties on equal footing. It is not sufficient for CSE to manage the regime in isolation, with its clients not privy to the policies, procedures, and legal principles that underlie this information sharing – especially if, as CSE views it, it is the clients that bear the ultimate responsibility for the lawfulness of their requests.

Notwithstanding any security markings appearing on this record, the information contained herein is declassified to UNCLASSIFIED

7. (U) NSIRA recommends that CSE and its GC clients can achieve this by developing Information Sharing Agreements in accordance with recognized best practices developed in this regard by the Treasury Board of Canada Secretariat (TBS). Until such a time, NSIRA believes CSE should cease disclosing CII to clients that do not meet *Privacy Act* standards in collecting CII through this disclosure regime.

8. (U) NSIRA has additionally found that CSE has applied an unsuitably low threshold for accepting the operational rationales provided by its clients in disclosure requests. Clients such as CSIS, RCMP, and CBSA generally demonstrated a clear link between the intelligence reporting and associated CII to their mandated activities. Other clients received CII from intelligence reports that did not relate to their mandate, and presented rationales that were insufficient to warrant the release of CII. As a result, NSIRA believes these disclosures may not have complied with the *Privacy Act* by not meeting the threshold for collecting information about Canadians.

9. (U) NSIRA has also observed that the Federal Court is unlikely to be aware of key characteristics of CSE's disclosures of CII obtained pursuant to section 16 of the *CSIS Act*. CSE's treatment and dissemination of this information differs substantially from the stringent standards communicated to the Court by CSIS, particularly when the information pertains to Canadian public officials. CSE's disclosures of CII from this program also result in the use of section 16 information for purposes of which the Court is unlikely to be aware, and which merit consideration as part of warrant applications.

10. (U) NSIRA has concluded that the CSE's implementation of the disclosure regime for CII may not comply with its obligations under the *Privacy Act*. Accordingly, this is a compliance report, as defined in section 35(1) of the *NSIRA Act*.

11. (U) Furthermore, NSIRA has found that CSE has released CII, including information about Canadian officials and other sensitive groups, in a manner that contradicts the procedures communicated to the Federal Court in support of warrants obtained by CSIS pursuant to section 16 of the *CSIS Act*.

12. (U) Pursuant to section 40 of the *NSIRA Act*, the Review Agency is of the opinion that it is in the public interest to submit a Special Report on this matter, for tabling before each House of Parliament.

Notwithstanding any security markings appearing on this record, the information contained herein is declassified to UNCLASSIFIED

II AUTHORITIES

1. (U) This review was conducted pursuant to paragraphs 8(1)(a) and 8(1)(b) of the *National Security and Intelligence Review Agency (NSIRA) Act*.

III INTRODUCTION

Review background and structure

2. (U) A review of CSE's disclosures of Canadian identifying information (CII) was a review undertaken annually by the Office of the CSE Commissioner (OCSEC), CSE's former independent review body. The current review, however, differs from those previously conducted by OCSEC given NSIRA's expanded mandate and ability to 'follow the thread' to other departments. In line with this mandate, NSIRA engaged with some of CSE's clients that received disclosures of CII within the review period to learn more about their involvement in the disclosure process. In all, NSIRA engaged eight other departments in relation to this review. Annex G contains a summary of NSIRA's engagement with all departments implicated in this review.

3. (U) Given the unique circumstances of NSIRA's recent establishment and the various logistical and procedural challenges associated with this transition, this review was only possible with the support of CSE staff, as well as those within its client organizations with whom NSIRA engaged. In addition, NSIRA faced the challenge of familiarizing itself with CSE's unique and complex operational environment, while simultaneously carrying out this review. This report was scheduled to be completed in the spring of 2020, but was delayed due to the COVID-19 pandemic that began when the review was in its final stages.

4. (U) This report is divided into three components: The first chapter presents an overview of the legal, policy, and operational foundation for the disclosure regime, as well as an overview of the disclosure process. The second chapter details NSIRA's observations, findings, and recommendations pertaining to the CII disclosure regime, including CSE's internal practices and CSE's assessment of clients' lawful authorities and operational rationales. The last chapter pertains to CSE's disclosure of CII based on its assistance, authorized by the *National Defence Act*, to the Canadian Security Intelligence Service (CSIS) in relation to s.16 of the *CSIS Act*.

What is Canadian identifying information?

5. (U) Canadian identifying information (CII) is a term that encompasses all information that can be used to identify a Canadian person or entity, in addition to foreign persons physically located within Canada. Identifiers can include everything from full or partial names to birth dates, telephone numbers, Internet Protocol (IP) addresses,[1] e-mail addresses, passport numbers, and physical addresses. It is not necessary for an identifier to be clearly linked to a person's name to constitute Canadian identifying information, as many types of recorded information, numbers, characteristics, and codes could possibly lead to the identification of a Canadian.[2] To protect the privacy of Canadians, CSE suppresses this information in its foreign intelligence reporting.

---

[1] The Supreme Court of Canada articulated that in some circumstances the use of an IP address may give rise to a reasonable expectation of privacy. "In my view, the identity of a person linked to their use of the Internet must be recognized as giving rise to a privacy interest beyond that inherent in the person's name, address, and telephone number." *R v. Spencer*, 2014 SCC 43, [2014] 2 S.C.R. 212, at para. 47. Emphasis by NSIRA.

[2] TBS Guidance on Preparing Information Sharing Agreements Involving Personal Information, Section 6.2.

Notwithstanding any security markings appearing on this record, the information contained herein is declassified to UNCLASSIFIED

6. (U) The same protections typically apply to corporations, non-profit organizations, and other entities such as universities.[3] While these types of identifiers do not constitute personal information that would typically be subject to the *Privacy Act*, CSE has committed to respecting the requirements of the *Act* in the disclosure of this information.[4]

7. (U) The Five Eyes intelligence alliance has agreed to incorporate these protections for one another's nationals into their intelligence reporting practices.[5]

Legal foundation for the disclosure regime

8. (U) Under the *National Defence Act* (NDA), CSE was prohibited from directing its foreign intelligence activities at Canadians, a restriction that remains in place today under the *CSE Act*.[6] CII may still be incidentally collected, meaning that the CII acquired was not itself deliberately sought and the collection activity was not directed at a Canadian or a person in Canada.[7] Should CII be incidentally collected, CSE must take "measures to protect the privacy of Canadians" in its use and retention, ensuring that private communications are only used or retained if they are essential to international affairs, defence, or security.[8]

9. (U) When writing an intelligence report, CSE will "suppress" the CII by substituting the identifying information with a generic term such as "Canadian 1" or "Canadian Company 1." Government of Canada (GC) clients[9] with the appropriate clearance and access to the system housing intelligence reporting may then read the reports with the suppressed information as part of their work related to the department's mandate.[10] Should a GC client want the suppressed information, they request its disclosure from CSE.

10. (U) Pursuant to the legal regime applicable to CSE disclosures for the period under review, the disclosure of Canadians' personal information had to comply with the *Privacy Act*:

a. (U) The *Privacy Act* sets a two-pronged test, whereby the institution holding the personal information must have a disclosure authority in order to disclose it to another institution, and the recipient institution must have a collection authority.

b. (U) On the side of the recipient department, collection has to comply with section 4 of the

---

[3] CSE has explained that while CII pertaining to corporations does not constitute personal information under the *Privacy Act,* CSE nevertheless has established policies and processes where the disclosure of CII, whether it constitutes personal information or not, is done in a manner that respects the requirements of the Privacy Act. CSE Response, "FINAL RESPONSE: RFI-22 (RE: Meeting with CSE DLS)," August 6, 2020.

[4] CSE Response, "FINAL RESPONSE: RFI-22 (RE: Meeting with CSE DLS)," August 6, 2020. [redacted]

[5] Five Eyes alliance members have also agreed that [redacted] in association with cyber security activities, [redacted] These identities will typically include [redacted] Such dissemination must be necessary to the analysis and mitigation of the cyber threat. Refer to "Release of 5-Eyes Identities associated with Cyber Security Activities," 2015.

[6] The *CSE Act* came into force on August 1, 2019

[7] This definition is now found in the new *CSE Act* at subsection 23(5).

[8] Paragraphs 273.64(2)(a) and 273.64(2)(b) of the NDA.

[9] There are over 2,300 Top Secret cleared and indoctrinated clients in 22 government departments and agencies who receive and use SIGINT in accordance with strict handling rules.

[10] SIGINT reporting by CSE and its Five Eyes allies is held in a restricted database called SLINGSHOT, and access to this system is a prerequisite to requesting the CII from such reporting. As per Canadian SIGINT Security Standard (CSSS), clients must request authorization from CSE to access SIGINT. Authorized departments must meet all security requirements (restricted access control, need to know, security clearances, yearly SIGINT security training) prescribed by CSE. Finally, individuals accessing SIGINT must be appropriately indoctrinated and their official duties must require consumption of SIGINT information.

Notwithstanding any security markings appearing on this record, the information contained herein is declassified to UNCLASSIFIED

Privacy Act, which prohibits the collection of personal information "unless it relates directly to an operating program or activity of the institution." Section 4 requires the collecting government institution to "establish a direct, immediate relationship with no intermediary between the information collected and the [institution's] operating programs or activities for which the personal information is collected."[11] The GC client has the responsibility to provide to CSE an explanation of the collection purpose and of the authority to collect for every request of personal information under section 4.

c. (U) In addition, CSE's disclosure must comply with section 8 of the *Privacy Act*. Generally, CSE relies on paragraph 8(2)(b), pursuant to which personal information about Canadians can be disclosed "for any purpose in accordance with any Act of Parliament [...]." In the period of review, CSE's disclosure authority was deemed implicit in paragraph 273.64(1)(a) of the NDA, which authorized CSE to acquire and use information from the global information infrastructure for the purpose of providing foreign intelligence. Moreover, paragraph 273.64(2)(b) instructed that CSE's foreign intelligence activities were subject to measures to protect the privacy of Canadians in the use and retention of intercepted information. This means that CSE relied on the expression "use" as its disclosure authority implied in the NDA to meet the requirements of paragraph 8(2)(b) of the *Privacy Act*.

d. (U) For the purposes of this review, NSIRA accepts that the double-pronged test sets the legal expectations for sharing of personal information. It therefore must be preoccupied with the standard of collection under section 4 of the *Privacy Act*. We note that the *Privacy Act* exists to protect the personal information of Canadians and has quasi-constitutional status. As acknowledged by the Department of Justice, [redacted][12] Similarly, personal information that has no apparent relevance to a disclosure request ought not to be disclosed.[13] Therefore, in order for a CSE disclosure to comply with the *Privacy Act* regime, CSE must evaluate, on the merits of each disclosure request, the justification invoked by the GC client prior to disclosing the personal information and be satisfied that it is reasonable.[14]

11. (U) The legal framework described above with respect to the applicability of the *Privacy Act* and the *National Defence Act* forms the basis of NSIRA's assessment of CSE's disclosure regime.

Ministerial Direction and policy framework

12. (TS) The 2012 Ministerial Directive on Privacy for CSE outlines three conditions under which information on or about Canadians or Canadian organizations may be disclosed: (1) it is essential to protect the lives or safety of individuals, (2) it contains evidence of serious criminal activity, or (3) it is required to understand or exploit foreign, security, or defence intelligence.[15] All requests reviewed by

---

[11] *UCCO-SACC-CSN v. Canada*, 2019 FCA 212.
[12] CSE DLS legal opinion, September 24, 2020
[13] *Minister of Public Safety and Emergency Preparedness v. Kahlon*, 2005 FC 1000.
[14] CSE DLS has opined that [redacted]
See CSE DLS legal opinion, July 9, 2013, page 2-3.
[15] *Ministerial Directive on the Privacy of Canadians*, November 20, 2012.

Notwithstanding any security markings appearing on this record, the information contained herein is declassified to UNCLASSIFIED

NSIRA fall under the latter two conditions.

13. (S) Moreover, CSE's Mission Policy Suite (MPS), the policy framework that guided its operational activities in the period of review, required CSE to:

- Assess the validity of requests, and whether the release could impact the operational interests of CSE and the GC or pose a risk to the privacy of a Canadian or person in Canada;
- Ensure the requester outlines their requirement for CII, identifies how it relates to their mandate and operational program, and confirms that the information will remain under the control of the requester; and
- Be satisfied that the requester has both the authority and operational justification to receive the information.[16]

14. (U) Building on the MPS, CSE has developed procedural guidelines that describe the processes that analysts are to follow to ensure that requesters of CII include a lawful authority and a robust operational justification for each request. These procedures include the steps to follow in releasing CII, examples of lawful authorities clients may cite, and examples of valid GC intelligence priorities that may be invoked for a request. We note that CSE's procedures require disclosure analysts to conduct more rigorous assessment of CII disclosures destined to foreign clients. For releases of CII to foreign clients, analysts are provided guidance as to the factors to be considered in assessing these requests, and are required to document their assessment.[17]

15. (U) Additionally, CSE has explained that disclosure analysts undergo training for up to six months prior to handling any requests independently, and in that time acquire experience from more experienced analysts and understand disclosure requirements. CSE expects trainees to demonstrate to their supervisor that they understand the requirements and are capable of analysing the information, working with colleagues and clients, and making decisions to action requests.[18]

16. (U) To comply with the above legal, Ministerial, and policy requirements, CSE must evaluate requesters' lawful authorities and operational rationales in its releases of CII.

Treasury Board of Canada guidance on information sharing between federal institutions

17. (U) The Treasury Board of Canada Secretariat (TBS) has developed guidance for federal institutions related to information sharing activities that involve personal information, which is based on an assessment of Canada's overarching privacy protection framework and universally recognized principles and standards. TBS states that when one party discloses personal information and the recipient party collects this information by way of such a disclosure, the parties are partaking in information sharing. Along with procedural guidance on how to ensure such information sharing reflects the letter and spirit of Canada's privacy protection framework, TBS encourages that this type of sharing occur on the basis of a written Information Sharing Agreement (ISA).[19]

18. (U) Additionally, TBS has developed policies and directives of relevance to CSE's disclosure

---

[16] Mission Policy Suite, Part A, s.28.7.2. Version 3, April 2019.

[17] D2 SOP 3: Releasing Suppressed Information, Section 5.2 "Rationale for the Request" and Section 5.3 "Advice to the Release Authority."

[18] CSE has stated that: "CSE also takes into consideration staff turnaround, time lapses, different learning styles, etc. when it comes to requests and training and works with the clients in order to better understand their needs and to ensure a complete request." CSE Factual Accuracy Comments, October 5, 2020.

[19] Treasury Board of Canada, *Guidance on Preparing Information Sharing Agreements Involving Personal Information.* This guidance, while non-binding, is designed for all institutions subject to the *Privacy Act*, of which CSE is one. While not a mandatory policy instrument, it outlined common principles for the sharing or exchanging of personal information.

Notwithstanding any security markings appearing on this record, the information contained herein is declassified to UNCLASSIFIED

regime, including the Policy on Privacy Protection, the Directive on Privacy Practices, and the Directive on Privacy Impact Assessment, all of which apply to government institutions such as CSE and its GC clients. Taken together, these tools guide institutions in ensuring their everyday operational practices comply with the intent of the *Privacy Act*.

CII disclosure process

19. (TS//SI) Suppression of CII, a key component of CSE's overall privacy protection framework, occurs when CII is initially acquired as part of foreign signals intelligence collection[20] and reporting and is deemed to be essential to understanding the intelligence. [redacted] When this happens, in order to protect the privacy of Canadians, any reference to information that can identify a Canadian or a person in Canada is suppressed in the report with a generic reference, such as 'Named Canadian 1.'

20. (U) When GC clients read intelligence reports containing suppressed CII,[21] based on the context of the report they may request the information for the furtherance of their own mandate and associated operational activities. In order for CSE to release this information to its GC clients, they must have their own lawful authority to collect it. Additionally, clients must acknowledge certain caveats and use restrictions prior to receiving the information. To request CII from CSE, GC clients must submit a request to CSE's Information Sharing unit,[22] which analyzes requests for CII from clients and releases the information if they have articulated an applicable lawful authority and a robust operational justification.

21. (U) Upon receiving the request, CSE assesses it to determine if the release of CII is appropriate. Disclosure analysts have a suite of options available to them, which can include:

- Conducting their own independent research into the requesters' mandates and authorities;
- Conferring with colleagues who may have specialized knowledge and experience; and
- Connecting back with the client to either clarify the content of the request or provide guidance to improve the request.

22. (S) Given the inherent legal disclosure risk associated with releasing information to the Royal Canadian Mounted Police (RCMP), all releases of CII to the RCMP require approval by the Supervisor of the Information Sharing unit.[23] As such, the RCMP must provide [redacted][24]

Disclosures of CII outside Canada

23. (S) Disclosures of CII made by CSE to foreign clients[25] were reviewed by NSIRA as part of the Foundational Review of Ministerial Authorizations and Ministerial Orders under the *CSE Act*. The

---

[20] [redacted] identifiers were also acquired through CSE's cybersecurity mandate in 2018, but, but these represented a small fraction of the CII collected through foreign intelligence gathering, and [redacted] appears to have occurred in 2019.

[21] These reports are typically read by clients through the application SLINGSHOT that is available on the Canadian Top Secret Network (CTSN) to authorized persons with the appropriate security clearance. Both CTSN and SLINGSHOT are centrally managed by separate units at CSE to ensure the appropriate protections are afforded to classified information.

[22] The Information Sharing unit at CSE, [redacted] is comprised of a Manager, a Team Lead, and [redacted] analysts.

[23] D2 SOP 3: Releasing Suppressed Information.

[24] This type of supplementary request is generally referred to as an 'action-on' request.

[25] Because SIGINT intelligence reports are available to authorized persons within the Five Eyes alliance, the suppressed Canadian identities may at times be requested by alliance partners, and vice versa. Similar procedures are in place for disclosure of CII to these partners. Often, disclosure requests to Five Eyes partners will also originate from GC entities such as CSIS who have a need to release the information to partners such as [redacted]

Notwithstanding any security markings appearing on this record, the information contained herein is declassified to UNCLASSIFIED

focus of this report is on disclosures of CII to domestic clients, due in large part to the far higher approval rate for domestic disclosures.

IV FINDINGS AND RECOMMENDATIONS

CSE's CII disclosure regime

24. (U) NSIRA expected to find that, as the steward of personal information about Canadians, CSE has in place privacy protection measures in line with its legal responsibilities, Ministerial Direction, and the rigour and diligence described in its messaging to the Canadian public. NSIRA also expected to find that disclosures of CII are subject to a thorough, well-documented evaluation and approval process that demonstrates each disclosure's compliance with legislation, Ministerial Direction, and CSE policy. As well, CSE's underlying policies and procedures must reflect both the letter and spirit of all applicable legislation, particularly as these are the operational tools used daily by employees delivering this program.

25. (U) NSIRA initially assessed 283 disclosures representing 2,023 pieces of identity information (henceforth 'identifiers')[26] released during the initial review period.[27] NSIRA later expanded the sample with a further [redacted] disclosures representing [redacted] further identifiers to cover an expanded review period for disclosures made in relation to the *Investment Canada Act* (ICA) and CSE's assistance to CSIS under section 16 of the *CSIS Act*. For disclosures unrelated to these two activities, the review period remained unchanged. In totality, NSIRA reviewed 396 disclosures of CII representing 2,316[28] released identifiers.

26. (U) During the initial period under review, CSE received requests for a total of [redacted] identifiers from 15 departments, releasing 3,671 – which represents a release rate of 99%.[29] The majority of identifiers were released to law enforcement and security agency clients.[30]

CSE's internal practices related to disclosure of CII

27. (S) During the period under review, CSE implemented a new information management system, [redacted] to track CII requests and deliver it to clients. The new system contains a form clients must fill out in order to receive CII, including a new field for the elaboration of the client's lawful authority. CSE explained that [redacted] was developed to ensure clients' authorities are properly

---

[26] The term 'identifier' relates to individual pieces of information that constitute identifiable information. NSIRA focuses its statistics on identifiers rather than disclosure requests, because even one disclosure request can contain multiple (and in some cases dozens or hundreds) of identifiers. Therefore, statistics pertaining to identifiers are more demonstrative of the volume and scale of identities implicated in CSE's disclosure regime. Some identifiers may at times pertain to the same individual.

[27] The ratio of identities to disclosures is higher for the initial review period (7 identities per disclosure, on average), [redacted] Not accounting for disclosures related to such incidents, CSE released, on average, approximately 5 identities per disclosure.

[28] NSIRA's "Review Tracking Document." NSIRA manually calculated the total number of identifiers, and accounted for cases where more than one identifier was released in response to a single suppression, while CSE in those cases may have counted the disclosure as one identity.

[29] NSIRA's "Review Tracking Document." For a listing of all GC clients that requested CII in the review period, refer to Annex F.

[30] This refers to CSIS, CSE, CBSA, RCMP.

Notwithstanding any security markings appearing on this record, the information contained herein is declassified to UNCLASSIFIED

cited and to improve the efficiency of the disclosure process.[31]

28. (S) NSIRA had the opportunity to review disclosures that occurred before and after the implementation of [redacted] and is satisfied that the new system improves information management and notes it is a positive step toward soliciting better responses from CSE's clients. Prior to [redacted] 39% of requests did not contain the client's legal authority; post [redacted] only 8% of requests did not state an authority.[32] However, because some clients continue to leave the lawful authority field blank, NSIRA notes that this field should be made mandatory in request forms both for completeness of requested documentation and to ensure clients receive CII based on an applicable legal authority.[33]

29. (S) During the review period, CSE's Client Relations Officers (CROs) embedded within client organizations submitted 18% of CII requests reviewed by NSIRA. By engaging with clients that receive CII, NSIRA learned that CROs may proactively bring intelligence reporting to their clients, but will generally only request CII if directed by a client.[34] Still, CSE policy enables CROs to proactively request CII to be shown to clients in the event they request to see it.[35] NSIRA believes that without clearer guidelines governing these advance releases, this structure could contribute to broader consumption of CII within government. In NSIRA's view, the most appropriate role for the CROs would be to facilitate the process from a technical perspective by accessing intelligence reports and requesting CII based on clear direction from a client.

30. (S) Within NSIRA's sample, 30% disclosures were elevated for approval to the supervisor level,[36] of which only one request was denied.[37] Of these, none contained an analysis of the requester's lawful authority or operational rationale.[38] Further absent were rationales for the approval of RCMP, GAC, and ICA-related requests, which explicitly require supervisor approval.

31. (U) The supervisor also conducts monthly compliance checks to confirm that releases of CII follow sufficient justification, that only the requested CII is released, and whether any procedural errors have occurred.[39] For instance, the supervisor's active monitoring e-mail contains fields such as "Observations/notes relating to review of requests from Canadian clients" and "overall comments." Both of these fields were left empty for [redacted] compliance checks in the review period. CSE explains that the supervisor coaches analysts informally in the event that disclosures do not meet requirements, but this is not documented within the supervisor's reports – which provide only

---

[31] CSE Response, "FINAL ANSWERS – RFI-4 – CII Review 2018-19," Q6. CSE states: "In an effort to ensure the necessary information is included on each request, CSE has implemented [redacted], which requires clients to fill in separate fields indicating the legal authority for requesting the information, and the operational requirement. As capability development on [redacted] proceeds, D2 will continue to explore avenues to minimize oversights such as those highlighted in the review."

[32] Pre-[redacted] example: [redacted]. Post-[redacted] example: [redacted].

[33] More specifically, NSIRA believes clients should not be able to write 'N/A' in the lawful authority field and still submit the form.

[34] Meeting with PCO, February 4, 2020.

[35] D2 SOP 3: Releasing Suppressed Information, Section 4, "Advance Releases to Canadian Recipients."

[36] Supervisor approval is required for disclosures to [redacted] and for disclosures made in relation to the *Investment Canada Act*. These requirements were a result of internal compliance checks and previous reviews by OCSEC, respectively, which found that these types of disclosures tended to contain insufficient rationale. See [redacted] SOP3: Releasing Suppressed Information and CSE Response, "PARTIAL RESPONSES TO Q 3, 4, 5, 6, 11 RFI-14 - NSIRA Disclosures Review – ICA," January 31, 2020.

[37] Disclosure [redacted] and NSIRA's "Review Tracking Document."

[38] Prior to the implementation of [redacted], the process to obtain supervisor approval was for analysts to forward the request to [redacted] supervisor, and for the supervisor to respond accordingly. Of the approvals reviewed by NSIRA, the analysts' recommendations for approval were of a formulaic nature. [redacted] cases reviewed by NSIRA, the analyst recommended [redacted] the supervisor responded simply with "Approved."

[39] D2 SOP 3: Releasing Suppressed Information, Section 2.5, "Active Monitoring."

Notwithstanding any security markings appearing on this record, the information contained herein is declassified to UNCLASSIFIED

statistical summaries of CII disclosures.[40]

32. (U) NSIRA believes this structure, if used fully, can provide assurance of disclosures' overall compliance with requirements, but this would require the rationale behind the supervisor's actions to be documented.

33. (U) CSE discloses CII at the analyst level, and relies primarily on analysts' discretion,[41] independent research,[42] and independent relationships with clients, which grants them substantial latitude in making everyday decisions that engage the privacy rights of Canadians. Analysts are not required in CSE's policies to document these activities for domestic requests, and as a result NSIRA could not assess the degree of validation that takes place in relation to those requests where lawful authorities are missing or operational rationales weak. Further, the training and operational materials that analysts receive do not provide guidance on assessing the substance and validity of disclosure requests, and rather focus on the logistical and technical procedures to release CII.[43] Finally, because the training analysts undergo occurs on the job, NSIRA was not able to assess whether or to what degree disclosure analysts are trained to assess the substance and validity of requests.

34. (U) While not directed at CSE's activities, the Federal Court has recently commented on the treatment of incidentally collected information about Canadians, specifically cautioning against deference to individual discretion in releasing personal information in place of operational policies and procedures to guide consistent and effective decision-making.[44] NSIRA highlights this judicial perspective of relevance to CII disclosure, and notes that CSE's current disclosure regime relies on analysts' individual discretion, background activities, and knowledge that they do not document.

35. **(U) Finding no. 1: NSIRA finds that CSE has developed policies and procedures designed as an internal oversight mechanisms for the disclosure of CII. However, NSIRA finds that CSE's implementation of these mechanisms was inadequate. The practices that NSIRA singles out for particular concern include:**

a. **CSE has accepted requests that do not state a lawful authority, even after the implementation of a new system meant to address this issue.**

b. **The analysts responsible for CII disclosures did not receive written guidance related to assessing the substance and validity of disclosure requests, as the guidance and training materials currently in place focus only on logistical procedures for releasing CII to domestic clients.**

c. **The analysts responsible for CII disclosures are not required to document their rationales and assessment of domestic requests, which could provide insight into how analysts have validated specific disclosures. As such, NSIRA was not able to assess if any further validation occurred for those disclosures where the clients did not state**

---

[40] CSE Response, "NSIRA Disclosures of CII Review (2019-003) - Formal Response to RFI-8," October 30, 2019.

[41] For example, CSE explains: [redacted] analysts may decide to de-conflict requests and disclosures from different departments if they believe it would assist them in the reviewing the information at hand, however, this is not a requirement." CSE Response, "FINAL ANSWERS – RFI-4 – CII Review 2018-19," October 15, 2019, Q10b.

[42] CSE Response, "FINAL ANSWERS – RFI-4 – CII Review 2018019," Q5a.

[43] Refer to D2 Identity Release Manual. The manual guides disclosure analysts through the technical steps to follow in order to disclose CII, and does not provide guidance related to assessing the substance or validity of disclosure requests.

[44] "Greater protection should be granted to information about Canadians incidentally collected in the gathering of foreign intelligence. As mentioned, there are no formal criteria guiding Service employees or others on unminimizing identities of Canadians. Without guidelines, decisions about the retention, disclosure, and distribution of this information is left to individual discretion. More is required, especially since this is information that is acquired merely as a by-product of the Service's mandate to collect foreign intelligence." See 2020 FC 697, June 16, 2020, Para. 72. Emphasis by NSIRA.

Notwithstanding any security markings appearing on this record, the information contained herein is declassified to UNCLASSIFIED

legal authorities or offered weak operational rationales.

d. **CSE's current procedures do not provide Client Relations Officers sufficient guidelines in relation to advance releases of CII.**

e. **The CSE supervisor responsible for approving requests and conducting compliance checks did not document their rationale for request approvals, and did not identify any concerns regarding disclosures as part of their monthly compliance checks.**

(U) Recommendation no. 1: CSE should enhance the rigour of its internal practices related to CII. Firstly, CSE should update its policies to require that supervisors and analysts document their assessments and rationales for approving or denying disclosure requests.

(U) Recommendation no. 2: 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.

(U) Recommendation no. 3: CSE should ensure that the role of its Client Relations Officers is limited to facilitating the release of CII only when clients explicitly request it.

(U) Recommendation no. 4: 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's assessment of clients' authorities

36. (U) Disclosures of CII must be made to departments that have the lawful authority to collect it, based on the section 4 requirement of the *Privacy Act* that limits government institutions' collection of personal information to only that which is related to their operating programs or activities. NSIRA expected to find that CSE has assessed and understood its clients' lawful authorities for collecting personal information prior to releasing CII.

37. (TS) A majority of CSE's clients cited the same legislation in their requests for CII.[45] Clients such as CSIS, RCMP, and CBSA, which together comprise CSE's most frequent clients, tended to

[45] This included legislation such as the *Security Offences Act, CSIS Act, Immigration and Refugee Protection Act, Investment Canada Act, Charities Registration (Security Information) Act, Exports and Imports Permits Act,* and *Special Economic Measures Act*, in addition to the invocation of Crown Prerogative by [redacted] and [redacted]

Notwithstanding any security markings appearing on this record, the information contained herein is declassified to UNCLASSIFIED

correctly cite legal authorities that were applicable to the collection of the requested CII. NSIRA also observed numerous disclosure requests by other clients that either cited an authority not applicable to that department,[46] did not cite an authority,[47] or cited authorities that did not relate to the associated intelligence report or the requested CII.[48] In light of this, NSIRA set out to understand how CSE evaluated the lawful authorities invoked by its clients.

38. (U) On this matter, TBS provides relevant guidance:

> When first considering a data sharing initiative, institutions should satisfy themselves that it is lawful. This means that once an organization has defined what, how, why, and with whom it wants to share personal information, it should conduct an analysis of all applicable federal laws, including regulations, to ensure that is has the legal authority to do so. The recipient would also be required to ensure that it has its own statutory authority to carry out the proposed data sharing activity.[49]

39. (TS) Throughout this review, CSE has consistently taken the position that [redacted][50] CSE explains that analysts assessing requests must be "satisfied that the requester has identified a lawful authority and a robust operational justification for obtaining the information,"[51] that analysts have the discretion to research legislation further if they wish,[52] and that they are also able to defer to previous approvals of similar disclosures when considering requests.[53] CSE has not demonstrated how it assesses whether a request meets the threshold of 'reasonable.'

40. (U) NSIRA notes the *Privacy Act* does not specify which entity is to assess collection authorities when information is to be disclosed. However, CSE is the department that exercises discretion in its releases of information about Canadians, not its recipients. In NSIRA's view, CSE's clients do not have inherent lawful authority for all personal information in CSE's holdings, and it is CSE that must assess whether a particular disclosure to a client can be made based on the client's authority to collect information about Canadians. That is not to say that CSE must conduct a stringent legal assessment for every disclosure – rather, a documented overarching assessment of the most prevalent legal authorities by CSE and its clients would provide the required background for disclosure analysts to be able to make informed decisions.

41. (TS) To that end, CSE has developed Standard Operating Procedures (SOP) that are used by disclosure analysts in their assessments of CII requests, which contains a list [redacted] legal instruments that have been essentially 'pre-cleared' for citation by [redacted] requesters. This section of the SOP can be found in Annex C. As per the SOP, analysts can consider these instruments sufficient when clients invoke them as lawful authority.[54]

---

[46] E.g. Disclosures [redacted]
[47] E.g. Disclosures [redacted]
[48] E.g. Disclosures [redacted]
[49] *Treasury Board of Canada, Guidance on Preparing Information Sharing Agreements Involving Personal Information.* Emphasis by NSIRA.
[50] CSE DLS opinion dated March 10, 2017; CSE Response, "FINAL RESPONSE: RFI-22 (RE: Meeting with CSE DLS)," Q2, August 6, 2020; and CSE Response, "PARTIAL RESPONSE: Q9, 10 a-d - RFI-15 NSIRA CII Disclosures Review," 14 February 2020. Specifically, CSE states that it [redacted]
[51] CSE Response, "PARTIAL RESPONSES TO Q 3, 4, 5, 6, 11 RFI-14 - NSIRA Disclosures Review – ICA," 31 January 2020.
[52] CSE Response, "FINAL ANSWERS – RFI-4 – CII Review 2018019," Q5a.
[53] CSE Response, "PARTIAL RESPONSE: Q9, 10 a-d - RFI-15 NSIRA CII Disclosures Review," Q10c, February 14, 2020.
[54] D2 SOP 3: Releasing Suppressed Information, Section 3.3.

Notwithstanding any security markings appearing on this record, the information contained herein is declassified to UNCLASSIFIED

42. (TS) CSE did not demonstrate that it has assessed all legal instruments prior to their inclusion in the SOP. Some statutes are inaccurately named in the SOP, and are approved for invocation by clients who do not have explicit administration or enforcement responsibilities within them – which warrants an analysis as to whether they can serve as collection instruments for those clients.[55] When asked how CSE assessed the instruments before listing them in the SOP, CSE responded [redacted][56] CSE has not demonstrated that it has assessed and documented the ability of any other department to invoke any of the other legal mechanisms listed in the SOP.[57]

43. (U) The Crown prerogative is one of the authorities [redacted] a collection authority for [redacted][59] NSIRA notes the previously described section 4 requirement of the *Privacy Act* that personal information about Canadians only be collected in direct relation to an institution's operating programs or activities, which TBS has stated typically derive from an Act of Parliament or Parliamentary approval of expenditures. At the same time, the Crown prerogative stems from the common law. In this context, the extent to which the Crown prerogative may be relied upon as a direct collection authority under section 4 of the *Privacy Act* remains unclear, and NSIRA believes this question has not been sufficiently considered as part of CSE's disclosure regime. Annex A contains an assessment on the use of the Crown prerogative as a collection authority for personal information.

44. (S) The *Investment Canada Act* is another legal instrument [redacted] invoked by federal departments to collect CII. Throughout this review, CSE presented conflicting internal interpretations of the collection authorities derived from the ICA.[60] This inconsistent understanding of the ICA was mirrored in statements provided to NSIRA by CSE's clients, some of whom stated that the ICA serves as a collection authority for CII while others explained that it does not provide them with any authorities outside their core mandate.[61] NSIRA believes that the ICA does not grant the authority to collect CII in the broad manner in which it has been applied by requesters and accepted by CSE. Annex B contains an assessment of the ICA in the context of disclosures of CII.

45. (S) By engaging with departments that request CII, NSIRA learned that CSE's clients themselves did not have a consistent understanding of the lawful authorities upon which they requested information. While some clients presented a strong understanding of their authorities to

---

[55] Both the *Special Economic Measures Act* and the *Export and Import Permits Act* are erroneously written as '*Special Export Measures Act*' and '*Import and Export Permits Act,*' respectively. Further, SEMA does not appear to create an operating program or activity [redacted] which warrants an analysis of whether this legislation grants [redacted] the power to collect personal information.

[56] CSE DLS opinion dated March 10, 2017, [redacted]

[57] [redacted]

[58] Requests from [redacted] did not explicitly cite the prerogative, typically citing "N/A" for lawful authority. [redacted] See CSE Response, "FINAL ANSWERS – RFI-4 – CII Review 2018-19," October 15, 2019, Q6.

[59] Refer to [redacted] SOP3: Releasing Suppressed Information, which states that [redacted] may invoke the Crown Prerogative as lawful authority to collect CII.

[60] CSE's acceptance of the ICA as a collection authority is demonstrated through its approvals of disclosures citing the Act. See also CSE Response, "PARTIAL RESPONSE Q1: NSIRA Disclosures Review - RFI-04," 7 October 2019; CSE Response, "FINAL ANSWERS – RFI-4 – CII Review 2018-19," October 15, 2019, Q7a; and, in disclosure [redacted] CSE Response, "PARTIAL RESPONSES TO Q 2, 2a, 11, 11a, 12b,c,d, 14 of RFI-14 – NSIRA Disclosures Review – ICA," Q2a. This was further reiterated in a briefing to NSIRA on January 28, 2020 and in the Management Direction for the Investment Canada Act Program, s.2.1.

[61] Meetings and responses with GC entities, as well as [redacted] response, Annex B [redacted] Response to NSIRA RFI – March 2020.

Notwithstanding any security markings appearing on this record, the information contained herein is declassified to UNCLASSIFIED

collect CII,[62] others could only describe their collection authorities following discussions with their legal counsel that were prompted by our inquiries.[63] NSIRA notes that in most cases this assessment did not take place at the time of, or prior to, CSE's disclosure of CII to these clients.

46. (U) As a result, the CII disclosure regime as presented to NSIRA has demonstrated inconsistencies in CSE and clients' understanding of the lawful authorities underpinning the sharing of CII. CSE has shifted the onus of responsibility for legal authorities onto its clients without developing a governance structure that would foster the equal sharing of this responsibility. While CSE benefits from its internal policies, procedures, and legal opinions on the subject, its clients are simply instructed on how to submit a CII request form,[64] and may on an ad-hoc basis provide contextual information for their request.[65] This imbalance is not appropriate if the main burden of responsibility for the disclosures rests with the client.

47. **(U) Finding no. 2: NSIRA finds that CSE has not sufficiently assessed the legal authorities its clients invoke to collect CII. CSE has preapproved within its Standard Operating Procedures a number of legal authorities that clients can invoke to request CII, without conducting an underlying assessment. As a result, CSE has accepted clients' invocation of the Crown prerogative and the *Investment Canada Act*, that NSIRA believes may not grant departments powers to collect personal information about Canadians in the broad manner in which they have been applied.**

(U) Recommendation no. 5: 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.

(U) Recommendation no. 6: CSE should revise its Standard Operating Procedures to reflect the legal advice it receives in response to Recommendation 5.

CSE's assessment of clients' operational rationales

48. (U) In keeping with the earlier discussion on the *Privacy Act*, NSIRA expected to find that CSE released CII where clients established a direct and immediate relationship (with no intermediary) between the information and their mandated activities. NSIRA expected to find documented evaluation of clients' rationales that clearly demonstrated how each disclosure meets this requirement, in the context of the intelligence reporting upon which requests are made. NSIRA further expected that clients do not receive any more CII than is necessary.[66]

49. (TS) CSE operational guidance requires that any element of the suppressed CII that is not required by the requesting organization to accomplish its mandated role be withheld. For example, "if

---

[62] For example, the RCMP explained that its collection authority derives from its responsibilities under the *Security Offences Act*. Briefing with RCMP, February 10, 2020.
[63] Briefings with and responses from [GC entities withheld]. Some of the clients NSIRA engaged were not aware that the legislation cited in their request had to constitute an authority to collect personal information about Canadians.
[64] Briefing with CSE, August 12, 2019.
[65] CSE Response, "FINAL ANSWERS – RFI-4 – CII Review 2018-19," Q5a,d.
[66] DOJ ILAP opinion, July 30, 2007, page 17.

[redacted] then extraneous information [redacted] will be withheld."[67] NSIRA believes this privacy protection measure meaningfully reflects the intent of *Privacy Act* and *National Defence Act* requirements, and expected to find it rigorously enforced by CSE as part of its disclosures.

50. (TS) To reflect the intent of the *Privacy Act*, when read in whole, discretionary releases of personal information should not reach such a magnitude as to resemble a "fishing expedition." [redacted]

[redacted]

51. (U) CSE has further explained that "the Courts have found that a "fishing expedition" is when a request for information is not likely to be relevant."[69] NSIRA agrees with this characterization of the term, and finds that it can describe some of CSE's disclosures of CII.

52. (U) Based on the disclosures reviewed by NSIRA, departments such as CSIS, RCMP, and CBSA consistently demonstrated the relevance of the requested CII in relation to their lawful authorities. The RCMP in particular generally provided [redacted] and articulated [redacted] that strengthened its rationales for the suppressed CII.[70] In NSIRA's view, these clients' collection of CII complied with the *Privacy Act*, with rare exceptions.

53. (U) At the same time, NSIRA has observed the scenario [redacted] playing out in relation to CII disclosures made to other clients. CSE has released CII where, in NSIRA's view, the clients did not establish a direct and immediate relationship between the requested information and their mandated activities, and thus facilitated clients' collection of CII that may not have complied with the *Privacy Act*. Some of these disclosures also met the Courts' interpretation of the term 'fishing expedition'; that is, the information was not likely to be relevant.

54. (TS//SI) For example, identifiers such as [redacted] CSE explained that [redacted] CSE later reiterated its view [redacted] without further explaining how [redacted]

---

[67] CSE Response, "PARTIAL RESPONSES TO Q 3, 4, 5, 6, 11 RFI-14 - NSIRA Disclosures Review – ICA," 31 January 2020.
[68] [redacted] Emphasis by NSIRA.
[69] CSE Factual Accuracy Comments, October 5, 2020.
[70] E.g. Disclosure [redacted]
[71] E.g. Disclosures [redacted]
[72] CSE Response, "FINAL ANSWERS – RFI-4 – CII Review 2018-19," Q12. For example, see disclosure
[73] CSE Factual Accuracy Comments, October 5, 2020.

Notwithstanding any security markings appearing on this record, the information contained herein is declassified to UNCLASSIFIED

requested could [redacted]

55. (TS) This view aligns with [redacted] recurring rationale that this type of CII may be used to [redacted] NSIRA notes that [redacted] does not have the mandate or technical capacity [redacted] or to conduct granular investigations into threats to the security of Canada. In fact, departments such as CSIS exist to serve this function, and in many cases, CSIS requested the same information [redacted] As a result, NSIRA believes in these cases CSE released CII where [redacted] had not established a direct and immediate relationship between the information to be collected.

56. (TS//SI) In another instance, received [redacted] stated its intent was to [redacted] In NSIRA's view, this request is demonstrative of a 'fishing expedition' described above, especially given that CSE's response does not state whether [redacted] stating that it would be "useful" is not convincing when taking into account the context of the intelligence report, [redacted] does not have [redacted] mandate or the technical capacity to carry out activities such as [redacted]

57. (U) These releases contrast with other disclosures [redacted] that, in NSIRA's view, were appropriate in the context of the reporting and suppressed information, and pertained to [redacted][77]

58. (TS//SI) NSIRA also observed a trend in which [redacted] requested CII based on [redacted] The rationales typically stated a [redacted] While, in NSIRA's assessment, this rationale was valid for a minority of disclosures made [redacted][78] in the majority of cases the content of the report did not contain a clear correlation with [redacted] as to establish a direct relationship to the [redacted] mandated activities.[79]

59. (TS//SI) At times, clients received more identifiers than they requested.[80] In the example above, [redacted] requested the suppressed [redacted] but [redacted] also released [redacted] In another instance, [redacted]

---

[74] Even if [redacted] analysts had access to such databases, NSIRA believes it would be wholly outside the mandate of this organization to investigate such threats. From the perspective of reasonableness and necessity, departments such as CSIS, and in the case of clear violations of Canadian law, the RCMP, should request and receive such types of CII.

[75] Disclosure [redacted] The rationale states, [redacted] Emphasis by NSIRA. NSIRA interprets [redacted] as intending to confirm [redacted]

[76] NSIRA notes it could be appropriate for [redacted] to be aware if the identities pertained to [redacted] although CSE should have denied the request if they did not. It is unclear why [redacted] would need to know [redacted] apart from open-source research.

[77] E.g. Disclosures [redacted]

[78] E.g. Disclosures [redacted]

[79] E.g. Disclosures [redacted]

[80] E.g. Disclosures [redacted]

[redacted] noted that it only required [redacted] if they were also accompanied with [redacted] alone would not be sufficient. Despite this precision, CSE nevertheless released [redacted] without accompanying [redacted]

60. (U) In other cases, CSE denied disclosures on the basis that the associated reporting did not sufficiently [redacted][82] While this is not the sole criteria for evaluating disclosure requests, NSIRA believes it is an important one when the requester states an intent to [redacted] the requests must be carefully considered.[83]

61. (TS//SI) In one case, [redacted] requested the identifier to potentially [redacted] without stating how [redacted] could serve this purpose. [redacted] on the other hand, discussed [redacted] and explained that it would use the specific identifiers to determine [redacted] NSIRA believes [redacted] request was sufficiently detailed to demonstrate that it was justified even though [redacted] did not necessarily [redacted] while [redacted] did not provide a sufficient rationale for this information.

62. (TS//SI) NSIRA has also observed the disclosure of Canadians' personal information even when the client requested only the suppressed name of a corporation.[85] CSE explains that [redacted][86] and in the cases reviewed by NSIRA, clients also received [redacted] NSIRA notes that even if CSE or a partner included this [redacted] within the suppression, CSE has the discretion to decide if specific identifiers warrant release – in the cases reviewed by NSIRA, the client did not request [redacted] and the request itself did not warrant its release.

63. (TS) Finally, [redacted] of identifiers reviewed by NSIRA were released to clients in relation to the administration and enforcement of the *Investment Canada Act* (ICA). In these cases, clients [redacted] cited the ICA in relation to reporting that did not pertain to economic activity, and some clients' mandates did not align with the disclosed CII. Departments also cited the ICA as an authority to

---

[81] Disclosure [redacted]

[82] E.g. Disclosures [redacted] In disclosure [redacted] requests information to a Canadian [redacted] CSE releases the identity stating, [redacted] (Analyst Comment: [redacted] In NSIRA's view, this disclosure is inappropriate because (1) the individual's name only possibly belongs to the Canadian involved in nefarious activities, and (2) it is not appropriate to [redacted] on incomplete and possibly inaccurate information pertaining to Canadians. Further, an entity such as CSIS can tangibly ascertain whether the individual poses a threat to the security of Canada, while [redacted] must take the information at face value.

[83] E.g. Disclosures [redacted]

[84] Disclosure [redacted] A caveat placed by CSE within associated report [redacted] states: [redacted] Emphasis by NSIRA.

[85] E.g. Disclosures [redacted]

[86] CSE Response, "PARTIAL RESPONSE: Q9,10, 13f,g,h RFI-14 - NSIRA Disclosures Review – ICA," March 3, 2020.

receive CII that did not pertain to a specific foreign investment review. Because the ICA does not authorize general security intelligence investigations, these disclosures should only have been approved for the clients' own mandated investigations related to economic security independent of the ICA. Finally, clients received CII that did not relate to the ICA investment reviews cited in their requests. Annex B contains further details of these types of disclosures.

64. (TS) In response to NSIRA's questions regarding requests that did not adequately articulate a rationale for accessing supressed CII, CSE explained:

> When working on a particular file, [redacted] In this case, [redacted]

65. (TS) When asked about requests with insufficient operational rationales, CSE articulated its general approach: namely, [redacted][88] Specifically, CSE states that [redacted][89] Finally, CSE has stated that in cases of ambiguous requests, disclosure analysts "operate on the premise that the requestor is acting in good faith."[90]

66. (U) The above principles articulated by CSE translate to its assumption of some collateral evidence in the holdings of its clients that is not articulated in requests as a means to justify insufficient requests. CSE also accepts that clients may simply test hypotheses as to the relevance of CII to their operational activities. As the custodian of CII, NSIRA expected to find that CSE makes decisions to release CII based on the documented facts contained in intelligence reports and disclosure requests, and not on an assumption of the existence of some validating information elsewhere in the client's holdings.

67. (U) NSIRA highlights one of the important principles elaborated by TBS in its guidance related to information sharing:

> Institutions should only consider discretionary disclosures in circumstances where [...] there is a clear and justifiable purpose. The recipient's need to obtain the information should not be confused with administrative convenience [...] The underlying principle is that personal information should not be shared just because it would be useful or "nice to know."[91]

68. (U) In short, to meet the requirements of section 4 of the *Privacy Act*, a request must, on its face, demonstrate a direct and immediate relationship between the CII and the client's operational programs or activities. Simply stating a general mandate or program is not sufficient when the report or the specific CII requested appears to be superfluous to a client's mandate. NSIRA believes

---

[87] CSE Response, "FINAL ANSWERS – RFI-4 – CII Review 2018-19," Q11. Emphasis by NSIRA.

[88] E.g. Disclosures [redacted] See also CSE Response, "FINAL RESPONSE: RFI-19 NSIRA CII Disclosures Review - follow up on RFI-15," 10 March 2020; and CSE Response, "FINAL RESPONSE - RFI-14, Q 7, 8," Q8.

[89] CSE Factual Accuracy Comments, October 5, 2020.

[90] CSE Response, "PARTIAL RESPONSES TO Q 3, 4, 5, 6, 11 RFI-14 - NSIRA Disclosures Review – ICA," 31 January 2020.

[91] Treasury Board of Canada (TBS): Guidance on Preparing Information Sharing Agreements Involving Personal Information. Section 2.4. Emphasis by NSIRA. While the guidance is directed toward institutions seeking to establish formal Information Sharing Agreements (ISAs) with one another, in NSIRA's review it became evident that many aspects of CII disclosure closely resemble the information sharing practices to which this guidance applies.

Notwithstanding any security markings appearing on this record, the information contained herein is declassified to UNCLASSIFIED

disclosures in the examples above do not demonstrate a direct relationship to the clients' activities, and thus fall within the realm of what TBS has qualified as "nice to know."[92]

69. (TS//SI) CII was disclosed in the review period internally within CSE, to employees working under the foreign intelligence mandate. This can occur for legitimate reasons, such as requesting the identities of known Canadian selectors to protect those selectors from being targeted in the future.[93] NSIRA believes this can be an acceptable internal use of CII within CSE to protect the privacy of Canadians and prevent the targeting of known Canadian selectors. At the same time, NSIRA has also observed CII released within CSE to supplement its foreign intelligence analysis.[94] In these cases, [redacted] CSE further explains:

> (TS//SI) The CII [...] [redacted]

70. (TS) The identifiers released in these cases were [redacted] NSIRA believes [redacted]

71. (U) NSIRA notes that the NDA did not authorize CSE to research Canadians using publicly available materials,[98] and in fact, open-source research on Canadians was a key issue deliberated as part of the development of the *CSE Act,* which now does authorize this activity. However, it remains unclear how open-source research on Canadians was authorized under the NDA, and NSIRA believes it is important that CSE thoroughly assess the parameters in which this activity can be lawfully conducted under its new legal framework.

---

[92] *Ibid.*

[93] E.g. Disclosure [redacted]

[94] E.g. Disclosures [redacted]

[95] CSE Response, "FINAL ANSWERS – RFI-4 – CII Review 2018-19," October 15, 2019, Q8.

[96] E.g. Disclosure [redacted]

[97] CSE Factual Accuracy Comments, October 5, 2020.

[98] In relation to its foreign intelligence mandate, the *National Defence Act* authorized CSE to "acquire and use information from the global information infrastructure for the purpose of providing foreign intelligence, in accordance with Government of Canada intelligence priorities." These activities "shall not [have been] directed at Canadians or any person in Canada, and shall [have been] subject to measures to protect the privacy of Canadians in the use and retention of intercepted information." *National Defence Act* section 273.64(1) and section 273.64(2)(a).

Notwithstanding any security markings appearing on this record, the information contained herein is declassified to UNCLASSIFIED

72. **(U) Finding no. 3: NSIRA finds that CSE's most frequent requesters of CII (CSIS, RCMP, and CBSA) articulated strong operational rationales that showed a direct relationship between the requested CII and their mandated activities, generally translating to their justified collection of CII from CSE.**

73. **(U) Finding no. 4: NSIRA finds that CSE's implementation of its disclosure regime may not have complied with its obligations under the *Privacy Act*. CSE has released CII to clients other than CSIS, RCMP, and CBSA that did not articulate a lawful authority and did not demonstrate a direct and immediate relationship between the CII and their mandated activities. Clients also at times received more information than they requested. CSE has not demonstrated that it has conducted a sufficient case-by-case evaluation of the justification invoked by the requesting clients prior to disclosing personal information.**

(U) Recommendation no. 7: NSIRA recommends that CSE cease disclosing CII to clients other than CSIS, RCMP, and CBSA until it implements the recommendations contained throughout this report.

Toward a more balanced governance structure

74. (U) NSIRA has observed that neither its clients nor CSE have a consistent, well-documented understanding of the lawful authorities and operational conditions necessary for disclosure of CII – a key tenet of Canada's privacy legislation and policy requirements issued by TBS. As a result, for clients other than RCMP, CSIS, and CBSA, operational rationales are often poor, misaligned with clients' mandates, and often are simply are not sufficient to warrant the disclosure of CII. At the same time, the number of disclosures processed through CSE's disclosure regime dwarfs those processed through a similar regime implemented in support of the *Security of Canada Information Disclosure Act* (*SCIDA*), which was the subject of substantial public scrutiny and concern in its development.[99]

75. (U) Many of the systemic issues presented in this review arise from CSE's isolated governance of the disclosure regime. CSE develops its own internal policies, procedures, and legal assessments to which its clients are generally not privy. Instead, CSE trains its clients on how to use the intelligence reporting system and fill out CII requests, sometimes working with them on individual requests. However, at an institutional level, NSIRA has not found a consistent understanding across the community of the legal requirements underlying this practice, which engages Canadians' privacy rights on a daily basis. In fact, some clients could only produce an assessment of their lawful authorities in response to NSIRA's inquiries, which did not exist at the time disclosures were requested.

76. (U) In response to the themes covered in this section, CSE stated: "the terms by which CSE discloses CII are well documented in our policies."[100] This further reinforces NSIRA's view that CSE's internal policies alone are not enough to put both parties to a disclosure of information on equal footing – particularly if CSE takes the position that clients are ultimately responsible for the validity of their requests. CSE and its clients must equally acknowledge and be accountable for the gravity of CII disclosures in relation to both parties' legal responsibilities, and this should be reflected in a

[99] Whereas in a 6-month period departments would exchange approximately 100 requests for information related to *SCIDA*, CSE can be expected to process over 450 requests in the same timeframe.
[100] CSE's Factual Accuracy Comments, October 5, 2020. Emphasis by NSIRA.

Notwithstanding any security markings appearing on this record, the information contained herein is declassified to UNCLASSIFIED

transparent governance system that is known and agreed to by both parties.

77. (U) Within *SCIDA,* Parliament articulated the general principle that regular sharing of personal information from the same government institution to another is an appropriate situation for the two parties to enter into an information sharing arrangement.[101] TBS guidance in this domain reiterates and promotes the concept of written, documented Information Sharing Agreements (ISAs) to govern the sharing of personal information between departments,[102] and highlights the benefits of a Privacy Impact Assessment in relation to activities that carry high privacy risks.[103]

78. (U) NSIRA believes the CII disclosure regime closely resembles such an arrangement,[104] even if it is not formally established. TBS guidance in this domain outlines a number of essential best practices, legal and operational assessments, and interdepartmental discussions that should occur in the development of such an arrangement to make it both effective and lawful. Applied to the CII disclosure regime, taking this step would improve all parties' understanding of their information-sharing relationship and respective roles, responsibilities, and lawful authorities. It would also make the arrangement resilient to changes at the working level, where the disclosure regime largely takes place, by providing a defensible point of reference that does not rely primarily on the maintenance of ad-hoc client relationships.

79. (U) Such a documented arrangement would be particularly beneficial for clients other than CSIS, RCMP, and CBSA. NSIRA has observed that it is these clients, particularly PCO, GAC, CRA, and others, to whom CSE released CII where a direct and immediate relationship was not clearly demonstrated, and thus where the highest disclosure risks for both parties lie.

80. (U) CSE's CII disclosure regime has also not been subject to a Privacy Impact Assessment (PIA), which should be considered for new or substantially modified programs or activities involving the creation, collection, and handling of personal information.[105] The Office of the Privacy Commissioner (OPC) developed guidelines for assessing the privacy risks posed by a program or activity, and outlines a number of high-risk characteristics that would merit the conduct of a PIA.[106] NSIRA notes a PIA has not been applied to CSE's disclosure regime even though it fits nearly all identified high-risk criteria. The formalization of CSE's disclosure regime as part of the *CSE Act*, and its new associated requirements, serves as an appropriate juncture at which to conduct a PIA for CII disclosures.

---

[101] *Security of Canada Information Disclosure Act*, Preamble.

[102] An Information Sharing Agreement (ISA) is recommended by the TBS whenever government institutions share personal information about Canadians among one another. The document serves as a written record of understanding between government parties that outlines the terms and conditions under which personal information is shared between parties. Information sharing, in this context, may mean that one party is disclosing information while the other party is collecting information. Refer to TBS Guidance on Preparing Information Sharing Agreements Involving Personal Information, Section 1.2

[103] TBS, Guidance on Preparing Information Sharing Agreements Involving Personal Information.

[104] Such agreements are already in place even for relatively uncontroversial initiatives, such as the consent-based sharing of Canadians' banking information between Service Canada and the Canada Revenue Agency. CSE's disclosures of CII originate from indirect collection, which can be considered more intrusive and occurs without consent, and which is subject to the same *Privacy Act* limitations and related best practices as any other information sharing initiative.

[105] Treasury Board of Canada Secretariat, *Interim Directive on Privacy Impact Assessment*, section 3.1. Specifically: "In recent years, Canadians and parliamentarians have been concerned with the complex and sensitive privacy issues that stem from proactive anti-terrorism measures, use of surveillance and privacy-intrusive technology, sharing of personal information across borders, and threats to privacy posed by security breaches. Canadians want to be informed of how their personal information is handled and assured of its protection."

[106] Office of the Privacy Commissioner, "Expectations: OPS's Guide to the Privacy Impact Assessment Process," March 2020. Characteristics that pose a higher risk are that the program involves a large amount of personal information of many individuals, including sensitive personal information; the context in which it is obtained is sensitive; it involves information of one or more vulnerable populations; has a major impact on individuals (e.g. high stakes); is long term in nature; and involves additional risk factors such as collecting personal information for secondary purposes and collecting it without the individual's consent.

Notwithstanding any security markings appearing on this record, the information contained herein is declassified to UNCLASSIFIED

81. (U) In summary, NSIRA believes that CSE's continued disclosure of CII should be governed by Information Sharing Agreements (ISAs) with its regular clients. Existing arrangements with these clients govern operational issues such as security standards, information handling, and using the system required to complete requests. NSIRA believes a stronger governance structure is required to afford both sides an opportunity to understand and formally acknowledge at an institutional level the legal and operational requirements behind disclosing and collecting CII.

82. **(U) Finding no. 5: NSIRA found that the management of CSE's CII disclosure regime did not provide its community of clients a sufficient understanding of the structures and responsibilities underlying the sharing of Canadians' personal information. This regime does not foster an arrangement in which clients and CSE can take equal responsibility for the disclosure and collection of Canadians' personal information.**

(U) Recommendation no. 8: 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.

(U) Recommendation no. 9: NSIRA recommends that a Privacy Impact Assessment be undertaken in relation to CSE's CII disclosure regime.

Notwithstanding any security markings appearing on this record, the information contained herein is declassified to UNCLASSIFIED

Disclosure of CII resulting from CSE's assistance to CSIS

What is the s.16 program?

83. (TS) Under s.16 of the *CSIS Act*, CSIS may provide assistance to the Minister of Foreign Affairs (MFA) and Minister of National Defence (MND), by collecting foreign intelligence within Canada in relation to the nation's defence or the conduct of its international affairs.[107] In turn, CSIS requests the assistance of CSE if it does not itself have the tools or capacity to carry out the s.16 assistance. CSE's assistance takes the form of developing tools and techniques, intercepting target communications, decrypting [redacted] as well as report writing and translation.[108] In its assistance, CSE acts as an "agent" of CSIS, with the same authorities and responsibilities as a CSIS employee,[109] and is therefore obligated to respect the parameters of CSIS' warrants and legal authorities.

84. (TS) The collection of information or intelligence relating to the capabilities, intentions, or activities of foreign states within Canada pursuant to s.16 of the *CSIS Act* typically takes the form of [redacted] This type of collection may be authorized by warrants issued by the Federal Court under s. 21 of the *CSIS Act* and subject to terms and conditions imposed by the issuing judge. One of the key conditions included in every warrant is that incidental collection of information about Canadians through s.16 [redacted][110]

How CSIS requests CSE's assistance

85. (TS) In order to obtain CSE's assistance in relation to s.16 of the *CSIS Act*, CSIS submits a Request for Assistance (RFA) form to CSE, [redacted] RFAs typically outline CSIS' assistance requirements and the warrants to which they relate. [redacted][111]

86. (TS) Subsequently, CSE [redacted] in response to an RFA. [redacted][113] In relation to CII, [redacted] state that regular naming and suppression procedures are to be employed and that the privacy of Canadians is to be protected through suppression.[114] During the review period, no RFA [redacted] reviewed by NSIRA included a

---

[107] As part of this review, NSIRA only observed s.16 warrants made in response to requests from the MFA.

[108] Under the *National Defence Act*, para. 273.64(3), activities conducted by CSE as part of its assistance mandate were (and continue to be, under the *CSE Act*) subject to any limitations imposed by law on the agencies assisted.

[109] CSIS, DDO Directive on Section 16 of the *CSIS Act*.

[110] "Condition 1 [typically] states that information about Canadians shall be destroyed unless it (a) relates to activities constituting a threat to national security; (b) could be used to prevent, investigate, or prosecute a crime; or (c) relates to the capabilities, intentions or activities of any foreign state, person, or corporation for which Ministerial assistance has been requested." 2020 FC 697, June 16, 2020, Page 10.

[111] E.g. [redacted]

[112] Mission Policy Suite, Assistance Chapter, section 1.3.6. (Version September 24, 2019)

[113] [redacted]

[114] E.g. [redacted]

Notwithstanding any security markings appearing on this record, the information contained herein is declassified to UNCLASSIFIED

request by CSIS for CSE [redacted]

87. (TS) CSE takes the position that the statement pertaining to normal suppression procedures implicitly includes disclosure of CII,[115] and that disclosure is a 'post-publication' activity undertaken separate from the reporting process.[116] At the same time, CSE considers CII to be a result of its assistance activities when [redacted] under s.16 warrants.[117]

88. (TS) Further, CSE analysts disclosing CII from s.16 reports are not generally aware of the reports' origins as part of CSIS' warranted activities.[118] [redacted] correctly identifying s.16 reports is not a straightforward matter. Even after CSE indicated that it had provided all s.16 reports to NSIRA, NSIRA found other s.16 reports.[119] CSE explained this omission [redacted]

89. (U) NSIRA notes that suppression and disclosure are entirely separate activities because suppression occurs during publication, and the disclosure of CII – as explained by CSE itself – is a post-publication activity. Further, one exists to protect the privacy of Canadians while the other serves to provide clients with meaningful intelligence. Finally, CSE is still acting under its assistance mandate in relation to s. 16 of the *CSIS Act* in the full spectrum of collection, retention, and disclosure of personal information it obtains in the course of providing that assistance. As such, the practice of disclosing CII merits explicit inclusion in CSE's [redacted] for CSE to comply with its policy requirements.

Federal Court questions regarding information about Canadians

90. (TS) The practice of incidentally collecting, retaining, suppressing, and disclosing CII pursuant to s.16 has been the subject of inquiries from the Federal Court. In [redacted], this practice was presented by CSIS to the Court,[120] including a detailed summary of how s.16 information is collected, its processing for eventual intelligence reporting, and the disclosure regime associated with this reporting.[121] In these affidavits, CSIS described to the Federal Court the rigorous procedures in place in relation to incidentally collected CII pursuant to s.16. CSIS also described, in less detail and with omissions, the portion of reporting and disclosures that takes place within CSE arising from its

---

[115] CSE Response, "PARTIAL RESPONSE Q1,2,3,4,5,7: RFI-15 NSIRA CII Disclosures Review," January 29, 2020, Q1 and !4b.
[116] This is a term used regularly by CSE in briefings and in correspondence with NSIRA on the topic, which NSIRA has understood to mean that disclosures of CII are considered separate from processes that take place in the reporting phase, during which suppression/minimization procedures apply. Also see CSE Response, "FINAL RESPONSE: RFI-16 NSIRA CII Disclosures Review," February 18, 2020, Q4b.
[117] CSE Response, "PARTIAL RESPONSE Q1,2,3,4,5,7: RFI-15 NSIRA CII Disclosures Review," January 29, 2020.
[118] CSE Response, "PARTIAL FOLLOW UP: FINAL RESPONSE: NSIRA Disclosures Review - RFI-05," November 4, 2019, Q1. CSE explains: [redacted] CSE has further stated that CSE Factual Accuracy Comments, October 5, 2020. NSIRA notes this response is strictly hypothetical, and does not state [redacted]
[119] CSE Response, "PARTIAL FOLLOW UP: FINAL RESPONSE: NSIRA Disclosures Review - RFI-05," November 6, 2019.
[120] In internal correspondence between CSIS and CSE, the Service explained [redacted] dated January 6, 2014,
[121] CSIS affidavits to the Federal Court dated [redacted]

Notwithstanding any security markings appearing on this record, the information contained herein is declassified to UNCLASSIFIED

assistance to CSIS under this program.[122]

91. (TS) [redacted][123] Further, CSE has also recently testified before the House of Commons, and emphasized that in collecting information as part of its assistance to CSIS, CSE ultimately segregates and returns the information to CSIS.[124] Yet, CSIS' policy is that its approval of s.16 reports results in the report and the information it contains effectively belonging to CSE.[125]

92. (TS) Additionally, the Court was told that CSE [redacted] in the course of this review it emerged that CSE follows its own, different procedures for the disclosure of CII, independent of any direction or approval from CSIS.

93. (TS) As part of the [redacted] affidavit process, [redacted] For its part, CSE described its requirements related to disclosure of CII, including that the CII must be rationally connected to a GC intelligence priority, that the requesting entity must have legal authority, and can "demonstrate the essentiality of the information to the achievement of its mandate," in addition to *Privacy Act* and *Access to Information Act* stipulations.[127]

94. (TS) In 2017, the Federal Court asked CSIS more questions regarding the treatment of CII, particularly with regard to information pertaining to Canadian public officials. [128] This series of questions resulted from the Court's concerns regarding officials' parliamentary privilege.[129]

95. (TS) CSIS again presented affidavits outlining in detail its treatment of CII, [redacted] CSIS described its processing of s.16 information, and the protection of information about Canadians, including a detailed explanation regarding its treatment of information about Canadian officials.[130] NSIRA did not

---

122 [redacted] The affidavit [redacted]

123 [redacted]

124 Standing Committee on Public Safety and National Security, meeting of March 22, 2018. CSE stated: "any information we collect is segregated and is given back to [CSIS] and is their information. Effectively, we're acting on behalf of CSIS."

125 DDO Directive on Section 16 of the *CSIS Act*. [redacted]

126 [redacted]

127 Email, [redacted] January 15, 2014. Emphasis by NSIRA.

128 The direction issued by Noel J on June 20, 2017 states, [redacted]

129 NSIRA notes the following in relation to Parliamentary privilege: "The House has the authority to invoke privilege where its ability has been obstructed in the execution of its functions or where Members have been obstructed in the performance of their duties. It is only within this context that privilege can be considered an exemption from the general law. Members are not outside or above the law which governs all citizens of Canada." Refer to "House of Commons Procedure and Practice", Chapter 3.

130 [redacted]

Notwithstanding any security markings appearing on this record, the information contained herein is declassified to UNCLASSIFIED

find evidence that CSIS consulted CSE in relation to this affidavit,[131] even though, in our review it emerged that CSE's practices in relation to s.16-collected CII differ substantially from the stringent standards presented to the Court.

96. (TS) The Court subsequently issued a decision. In its decision, the Court [redacted] did not mention any aspect of CSE's disclosure of Canadian identities. Specifically, the Court emphasized the safeguards and processes in place at CSIS in relation to incidentally collected CII, particularly the limited distribution of external reports, detailed minimization practices, and sensitive treatment of information about Canadian officials.[132]

97. (TS) While the Court did not rule definitively on the assertion that parliamentarians enjoy immunity from incidental interception of their communication, it did consider whether the warrant applications for, and the fruits of those interceptions, merit special treatment, noting:

> The concern about gathering information about public officials is that the Service may be intercepting highly sensitive communications emanating from persons charged with the governance of Canada. That information, particularly information about the identity of the Canadian persons involved, must be carefully handled.[133]

98. (TS) In its decision, the Court noted its consideration of the Service's procedures in place in relation to CII. Given that CSIS and CSE's treatment of CII differs, it stands to reason the Court would have also made a determination in relation to CSE's treatment of s.16 collected CII. There is no such determination in the decision and NSIRA has observed this may be a result of incomplete information provided by CSIS in its affidavits on the subject. As such, NSIRA believes the Court reached its decision without the benefit of having a complete understanding of CSE's processes occurring alongside those of CSIS in the execution of Federal Court warrants.[134]

99. (TS) In relation to the Service's own treatment of s.16 collected CII, the Federal Court recommends that:

> ...the Service must develop guidelines for distributing and minimizing the identities of Canadians whose communications have been incidentally intercepted. It should advise the Court of the content of those guidelines and permit the Court an opportunity to comment on them. In individual warrant applications, the Service should continue to inform the Court when there may be incidental interceptions of Canadians' communications. It should also specifically disclose when there is a possibility that the communications of an elected official or other public servant may be intercepted. This disclosure requirement will permit the Court, where appropriate, to attach terms and conditions on the execution of the warrants it issues. Those terms and conditions could include imposing a requirement on the Service to return to the Court for directions on the handling of information collected...[135]

100. (TS) It is clear that the Court is distinctly interested in information relevant to the Service's handling of Canadian identities collected pursuant to s.16 warrants that it issues, and by requiring the Service to present its updated guidelines and practices, it makes clear that these practices will form

---

[131] CSE Response, "[Initials withheld] Affidavit consultation: RFI-16 NSIRA CII Disclosures Review," March 2, 2020.
[132] 2020 FC 697, June 16, 2020, Paras 26 to 42.
[133] 2020 FC 697, June 16, 2020, Para. 73.
[134] 2020 FC 697, June 16, 2020, Para. 51. Specifically, the Court stated, "...the Service's current procedures relating to the treatment of incidentally intercepted communications of all Canadians, described above, including public officials and senior public officials, under s 16 warrants are generally adequate and consonant with the Service's s 16 mandate. However, as discussed below, I agree with the amici that the Service should develop criteria and guidelines on the unminimization of identifying information about Canadians."
[135] 2020 FC 697, June 16, 2020, Para. 74.

part of the rationale for the approval of future s.16 warrants. The Court is also concerned about the handling and dissemination of this information and notes that terms and conditions may need to be attached in relation to this practice moving forward.

101. (TS) The Federal Court has expressly identified its concerns regarding the Service's own treatment of CII collected pursuant to s.16 warrants, and NSIRA believes it is likely that it would also find it essential to know how CSE treats s.16 collected CII. In this context, NSIRA believes it is a substantial omission that CSE's [redacted] process for releasing CII described throughout this report,[136] particularly pertaining to Canadian politicians, was not provided to the Court prior to reaching its conclusion.

Treatment of s.16 collected CII

102. (TS) CSIS described to the Federal Court several aspects of its s.16 collection and reporting regime that NSIRA has observed to differ from those of CSE. Annex D contains a summary of the differences NSIRA observed between the two organizations' treatment of CII.

103. (TS) For instance, NSIRA notes that CSE's treatment of CII pertaining to Canadian public officials did not follow the same processes that CSIS has presented to the Federal Court. CSE stated that it does not have a specific (stricter or otherwise) policy in place for the treatment of CII that pertains to Canadian officials,[137] while CSIS repeatedly explained to the Court that this information is treated with high sensitivity in its reporting and disclosure.

104. (TS) Nearly all of the identities of Canadian officials collected pursuant to s.16 and released by CSE were different from those released by CSIS in the review period. Identities released by CSE included [redacted] CSIS approval of these identities tended to take place at the senior management level, with [redacted]. Meanwhile, [redacted] of the identities of public officials were released by CSE at the analyst level.[138] [redacted]

[136] For example, CSE's disclosures of s.16 collected CII also intersect with the previously identified issues related to the *Investment Canada Act*. During the period under review, CSE disclosed [redacted] Canadian identifiers acquired through s.16 to [redacted] different departments for the purposes of the ICA. [redacted]. This is a far wider distribution of Canadian identities, and for purposes substantially different than those that have been communicated to the Court.

[137] CSE Response, "PARTIAL RESPONSE: Q6, 10f. - RFI-15 NSIRA CII Disclosures Review," 25 February 2020.

[138] NSIRA's "Review Tracking Document."

[139] CSIS Response, "Supplementary Response for NSIRA on Suppressed IDs," March 3, 2020; and CSE's disclosure [redacted]

Notwithstanding any security markings appearing on this record, the information contained herein is declassified to UNCLASSIFIED

July 1, 2015 to July 31, 2019	CSIS	CSE
Overall s.16 identities released	[redacted]	[redacted]
Officials' identities released		
Denials of requests for public officials' identities		
Officials' identities approved by ADI or ADM		
Officials' identities approved by Head or Manager		
Officials' identities approved by Analyst		
Unknown approval level[140]		

105. (TS) CSE's releases of CII from s.16 reporting spanned a substantially wider audience. During the review period, CSIS only released [redacted] identities outside of the core requesters [redacted] to just [redacted] departments.[141] This data largely aligns with the distribution of identities CSIS presented to the Court. Conversely, during the same review period, CSE released [redacted] identities to [redacted] departments other than [redacted][142]

106. (TS) The scale of identity sharing by CSE from s.16 reporting increased substantially from the first presentation of this information to the Court in 2013, when the Court was informed of [redacted] requests for identities released by CSE in a one year period (of which [redacted] were made to CSIS itself).[143] By contrast, NSIRA notes that in the one year period from July 1, 2018 to July 31, 2019, CSE processed [redacted] requests, resulting in the release of [redacted] identities to [redacted] departments.[144]

107. (TS) In the presentation of its own practices related to s.16 CII to the Federal Court, CSIS did not account for a far wider distribution of identities resulting from its own warranted activities, at substantially lower approval levels, by CSE. In response to this observation, CSIS provided a statement that implied [redacted] in relation to the treatment of this information.[145] Based on the Court's sustained inquiries on this subject and the rationales elaborated in its most recent decision on the subject, NSIRA believes this component of s.16 merits an immediate and complete disclosure to the Court by both CSIS and CSE.

Assessment of CSE's disclosures

108. (S) NSIRA did not review in detail the Service's own s.16 disclosures, only its policies, procedures, and statistical information so as to better understand whether CSE's disclosures, as the subject of this review, achieved compliance with these standards. Nonetheless, NSIRA also assessed CSE's s.16 disclosures for compliance with its own policies and for their reasonableness and

---

[140] CSIS explained that [redacted] CSIS Response, "RE: RFI-2 - NSIRA Review on CII Disclosures," March 6, 2020.

[141] CSIS Response, "Supplementary Response for NSIRA on Suppressed IDs," March 3, 2020. Departments [redacted]

[142] CSE Response, "FINAL RESPONSE: RFI - 13 - NSIRA Disclosures Review - S.16," January 10, 2020; and NSIRA's "Review Tracking Document." Departments other than [redacted]

[143] See para 25 in CSIS 32-13, 30 January 2014.

[144] NSIRA's "Review Tracking Document"

[145] [redacted]

Notwithstanding any security markings appearing on this record, the information contained herein is declassified to UNCLASSIFIED

necessity.

109. (S) NSIRA observed that approximately [redacted]% of requests for CII originating from s.16 were approved by CSE even though the clients did not articulate a lawful authority.[146] NSIRA also found that clients cited lawful authorities that were inapplicable to the requesting department, or not sufficiently clear in relation to the associated reporting.[147] As is the case with CSE's disclosures writ large, the operational justification provided by the clients was at times insufficient, unpersuasive, or unclear.[148] NSIRA notes that [redacted]% of releases were justified – [redacted][149]

110. (TS) Several disclosures highlight problematic elements in CSE's treatment of s.16 collected CII. In relation to a disclosure to [redacted] CSIS stated that it would likely not have approved that disclosure itself.[150] At the same time, CSIS accepts that CSE will have discretion in its decisions to release identities, and that CSE does not necessarily err if its decisions to release CII are not identical to those of the Service.[151] In NSIRA's view, if CSE is free to follow its own policies and reach its own conclusions regarding the release of identities stemming from CSIS' warrants, these procedures and associated disclosure statistics must be presented to the Federal Court for its consideration as part of s.16 warrant applications.

111. (TS//[redacted]) In another instance, information pertaining to [redacted] was disclosed to [redacted] at the request of [redacted] The request stated that the receiving [redacted] had a requirement to know the information as it relates to [redacted] does not have a statutory responsibility or an operational program related to the [redacted] and thus could not feasibly require [redacted] for the department's operational activities.[152] When questioned about this disclosure, CSE [redacted] stating: [redacted] was deemed to be sufficient."[153]

112. (S) CSE has further elaborated its view of the nature of this request by explaining that the [redacted] may not have received information [redacted] Rather, [redacted] requested that information be given to [redacted] to conduct [redacted][154] NSIRA is concerned about CSE's introduction of [redacted] as an authority on which personal information about Canadians can be collected. These concerns are elevated on the basis that this collection is derived from [redacted] warranted activities. Given the earlier stated concerns of the Federal Court, NSIRA believes it is imperative that the Court be informed regarding the disclosure of information about [redacted] collected through its warrants [redacted]

---

[146] E.g. Disclosures [redacted]
[147] E.g. Disclosures [redacted]
[148] E.g. Disclosures [redacted]
[149] The [redacted] SOP on information sharing states that [redacted]
[150] CSIS Response, "RFI-3 – CSIS – Follow Up Questions – with Answers," February 4, 2020, Q2.
[151] CSIS Response, "RFI-3 – CSIS – Follow Up Questions – with Answers," February 4, 2020, Q2.
[152] Disclosure [redacted] relating to report [redacted]
[153] CSE Response, "PARTIAL RESPONSE: Q9, 10 a-d - RFI-15 NSIRA CII Disclosures Review," Q10b.
[154] CSE Factual Accuracy Comments, October 5, 2020.

Notwithstanding any security markings appearing on this record, the information contained herein is declassified to UNCLASSIFIED

113. (TS) NSIRA has also observed CSE's disclosure of [redacted][155] In the rationale for its request, [redacted] explained that it required the identities in order to [redacted] The report's contents are incompatible with [redacted] does not fall under a program or operating activity under [redacted] authority. NSIRA further notes that while the report [redacted] the intended results of s.16 collection – the contents of the report are based on a [redacted] without any indication of [redacted]

114. (U) Given the sensitivity of [redacted] NSIRA views CSE's disclosure [redacted] through the s.16 program to be just as (if not more) sensitive as disclosures [redacted][158] It is imperative that CSIS describe these types of disclosures to the Federal Court as part of any further affidavits or warrant applications related to the s.16 program.

The way forward

115. (TS) In NSIRA's view, for the Federal Court to have complete visibility as to the use and dissemination of s.16 warranted collection – including Canadian identities – it must have complete facts pertaining to CSE's disclosure policies, practices, and statistics, as well as specific disclosure exhibits to demonstrate its disclosures in practice. The Service's affidavits on the subject matter have not presented a complete depiction of the treatment of incidentally collected identities pertaining to [redacted] and, of equal sensitivity in NSIRA's view, [redacted] deriving from Federal Court warrants.

116. (TS) Moreover, it is clear from the Court's recent ruling that [redacted]

---

155 [redacted]

156 In a meeting with NSIRA, [redacted] confirmed this to be a potential reason for the making of this request.

157 [redacted]

158 [redacted]

Notwithstanding any security markings appearing on this record, the information contained herein is declassified to UNCLASSIFIED

117. **(U) Finding no. 6: NSIRA finds that the Federal Court has not been fully informed about CSE's disclosure of personal information about Canadians, particularly relating to Canadian officials and other sensitive groups, derived from the warrants the Federal Court issued to CSIS in relation to s.16 of the *CSIS Act*. CSE has disclosed information collected pursuant to the Court's warrants in a manner that contradicts key principles previously outlined to the Court by CSIS.**

(U) Recommendation no. 10: 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, particularly when it pertains to Canadian officials and other sensitive groups described in this report.

(U) Recommendation no. 11: NSIRA recommends that CSE cease disclosing CII collected pursuant to s.16 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.

V CONCLUSION

118. (U) NSIRA has found that the processes and legal instruments facilitating CSE's disclosure of CII are many and interwoven, involving numerous federal institutions – many of which do not operate on a complete and equal understanding of the disclosure regime as that of CSE, even as they regularly partake in it.

119. (U) At the same time, the scale of CII disclosure is such that it has warranted the establishment of a dedicated unit and technical systems at CSE, demonstrative of this program's importance and stature in the organization. Finally, CSE's processes far more disclosures than those disclosures taking place under the *Security of Canada Information Disclosure Act*, which has been subject to significant public scrutiny.

120. (U) NSIRA believes this sort of systematic sharing of personal information among government institutions should occur under formalized Information Sharing Agreements (ISAs) that put all parties to the exchange on equal footing. NSIRA believes the continued disclosure of this information should take place based on principles, operational thresholds, and lawful authorities that CSE and its regular clients understand and acknowledge at an institutional level by way of a formal agreement.

121. (U) CSE and its clients should also engage with the Department of Justice[159] to assess the legal instruments invoked by clients to collect Canadians' personal information. This engagement should include concrete examples of disclosure requests citing each type of legal authority used to collect CII, to better contextualize the theoretical assessment of legal authorities.

[159] This includes the Constitutional, Administrative, and International Law Section, the Public Safety, Defence, and Immigration Portfolio, and the Centre for Information and Privacy Law.

Notwithstanding any security markings appearing on this record, the information contained herein is declassified to UNCLASSIFIED

122. (U) Finally, the Federal Court must have full visibility into CSE's treatment of Canadian identities acquired pursuant to s.16 warrants it authorizes. The Court's recent decisions have emphasized that [redacted]

123. (U) While this review was conducted under the *NDA*, NSIRA would be remiss not to situate its findings as part of CSE's current, more restrictive, legal requirements.[160] The explicit essentiality standard now found in the *CSE Act* in relation to disclosures of CII is stronger than CSE's requirements under the NDA. In NSIRA's view, this new statutory limitation demonstrates a clear intent by Parliament[161] to ensure that a high threshold is applied to justify each disclosure of CII. NSIRA will revisit this matter in a future review.

124. (U) Given its findings and observations, NSIRA is of the opinion that CSE's implementation of its disclosure regime may not comply with its obligations under the *Privacy Act*. Therefore, NSIRA has an obligation under section 35 of the *NSIRA Act* to submit this review as a compliance report to the Minister of National Defence. NSIRA is also of the opinion that CSE's practices implicate the duties and functions of the Federal Court, and it is therefore in the public interest that this review be released expeditiously. As such, NSIRA invokes its authority under section 40 of the *NSIRA Act* to submit this as a Special Report to the Minister of National Defence and Minister of Public Safety, for tabling in each House of Parliament.

---

[160] The *CSE Act* contains a dual essentiality test: Firstly, CII must only be retained in intelligence reporting with suppression if it is essential to international affairs, defence, security, or cybersecurity. Following the essentiality of its retention, any subsequent disclosure of CII must also only be made if CSE determines the disclosure itself is essential to the same goals.

[161] The Federal Court has articulated that legislation that infringes on civil liberties, a definition that CII disclosure likely meets, must be interpreted cautiously to ensure minimal infringement of Canadians' civil liberties. See *X(Re)*, 2018 FC 738.

Notwithstanding any security markings appearing on this record, the information contained herein is declassified to UNCLASSIFIED

ANNEX A: The Crown Prerogative

125. (U) During the period under review, [redacted] received CII under the authority of the Crown Prerogative, which CSE has preapproved as an authority that these and other clients may invoke in order to receive CII.[162] As this is the only authority invoked by clients that did not derive from an Act of Parliament, NSIRA set out to better understand this complex legal instrument.

126. (U) The Crown prerogative is a source of Canadian executive authority that is not derived from statute and has its origins in the common law. With the development of legislation to govern many activities conducted by government institutions, the historic powers of the prerogative have been over time limited or displaced by statute. As such, the "residue" of these powers constitute the prerogative exercised by the executive today.[163] At present, the prerogative power most relevant to the disclosures of CII reviewed by NSIRA is the prerogative over foreign affairs.[164]

127. (U) As a creature of common law, prerogative is liable to be constrained or fully displaced by statute. It is also subject to well-established common law limitations and must be exercised in accordance with our Constitution, and in particular the *Charter*. No new prerogative powers may be created, and therefore a fine line must be walked to adapt historical prerogative powers to contemporary circumstances.[165] NSIRA did not find evidence of such an assessment of the prerogative's historical powers or their subsequent displacement within CSE's disclosure requests.

128. (U) CSE [redacted] have put forward the view that:

[redacted]

129. (U) In NSIRA's view, the section 8 provision of *SCIDA* simply preserves unnamed existing prerogative powers, and cannot create new prerogative powers. Rather, it signals the intention of Parliament not to displace the general prerogatives of the Crown, but is not specific enough to prove a particular prerogative power exists. [redacted] NSIRA is [redacted] concerned about [redacted] to create a free-standing prerogative for "sharing national security information," which is not a recognized prerogative of the Crown in any of the available literature or jurisprudence.

130. (U) NSIRA highlights that reliance on the Crown prerogative as a collection authority for CII

---

[162] Refer to [redacted] SOP3: Releasing Suppressed Information, which states tha[redacted] may invoke the Crown Prerogative as lawful authority to collect CII.

[163] Hogg defines the prerogative as the "powers and privileges accorded by the common law to the Crown." Peter W Hogg, *Constitutional Law of Canada* (Toronto: Thomson Reuters, 2016) volume 1, chapter 1 at 1-18. See also AV Dicey, *Introduction to the Study of the Law of the Constitution*, 10th edition (London: Macmillan, 1959) at 424.

[164] The other four key domains of the prerogative are: war and peace, treaty making, defence and the armed forces, and other acts of state in matters of foreign affairs. Additionally, other powers and privileges of the Crown include those respecting passports, power of mercy, diplomatic appointments, public inquiries, hiring and dismissal of public servants, administration and disposal of public lands, copyright, armorial bearings, and honours and titles. Department of National Defence, Office of the Judge Advocate General. The Crown Prerogative as Applied to Military Operations. June 2008.

[165] *The British Broadcasting Corporation (BBC) v FD Johns (HM Inspector of Taxes*, [1954] 1 All ER 923 in the decision of Lord Diplock. See also Paul Lordon, *Crown Law* (Toronto: Butterworths, 1991) at 64.

[166] [redacted] Factual Accuracy Comments, October 5, 2020. Emphasis by [redacted]

Notwithstanding any security markings appearing on this record, the information contained herein is declassified to UNCLASSIFIED

raises legal challenges that require further consideration. NSIRA notes two issues concerning the its practical invocation as a lawful authority: (1) requests invoking the prerogative were not sufficiently precise and did not point to discrete prerogative powers, and (2) putting this issue aside, the Crown prerogative serves as an unclear authority for the collection of CII.

Requests invoking prerogative not sufficiently precise

131. (TS) [redacted]

132. (U) Many requests invoke prerogative authority broadly, without reference to which discrete prerogative power is at issue. To identify a specific prerogative power, inquiries need to be made into both the historical prerogative (as it is from these archaic powers that the current powers are derived), and whether these historical powers have been limited or displaced by statute or otherwise over time.[168] NSIRA views the invocation of simply the "Crown Prerogative" to serve as the lawful authority for CII requests, alone and without further elaboration, akin to using the word "statute" alone and without further explanation. This is insufficient.

133. (TS) [redacted]

134. (TS) NSIRA [redacted] cautions that CSE should not be quick to accept its clients' general claims of Crown prerogative without more substantial consideration of its applicability. [redacted] NSIRA is not prepared to accept that [redacted] may justify <u>any</u> activity it undertakes under prerogative.

135. (TS) Of course, this is only one part of what is required for the disclosure of CII, and a robust operational justification would still be necessary. NSIRA has observed that of the requests that implicitly or explicitly invoked the Crown prerogative, the operational justification did not warrant the release of 70% of requested identifiers.[170]

---

167 [redacted]
168 [redacted]
169 [redacted]
170 E.g. Disclosures [redacted]

Notwithstanding any security markings appearing on this record, the information contained herein is declassified to UNCLASSIFIED

Crown prerogative as a lawful authority to collect CII

136. (U) Because the Crown prerogative is the only legal instrument invoked by CSE's clients that does not derive from legislation, NSIRA set out to understand how this mechanism may authorize the collection of personal information about Canadians. NSIRA notes two characteristics of the prerogative worthy of consideration when assessing whether it can serve as an authority to collect information about Canadians. First, a widely accepted feature of the prerogative limits its use in infringing on civil liberties of citizens. Second, the question of whether the prerogative can be used to create an "operating program or activity" to meet section 4 collection limitations of the *Privacy Act* has not been sufficiently considered as part of CSE's disclosure regime.

137. (U) A widely accepted limitation on the prerogative prevents its use to infringe on individual liberties, and there is strong support in Canadian case law for the connection between privacy and liberty interests.[171] In addition, the *Privacy Act* is expressly binding on the Crown,[172] and where an *Act* binds the Crown, the prerogative may not be used to circumvent its provisions.[173] Lastly, the prerogative cannot escape the limitations imposed by the *Charter*, and must be exercised with an eye to an individual's reasonable expectation of privacy.

138. (U) In its review, NSIRA considered the question whether the prerogative may serve as a collection authority arising from section 4 of the *Privacy Act,* where an institution can show that collection relates directly to one of its operating programs or activities. To determine whether the prerogative may serve as the authority for creating an "operating program or activity" as understood in this section, we turn to the TBS Policy of Privacy Protection, which operationalizes the *Act* pursuant to section 71(1)(d)[174] and defines the term as:

> For the purposes of the appropriate collection, use, or disclosure of personal information by government institutions subject to this policy, a program or activity [is] authorized or approved by Parliament. Parliamentary authority is usually contained in an Act of Parliament or subsequent regulations. Parliamentary authority can also be in the form of approval of expenditures proposed in the Estimates and as authorized by an appropriation Act. Also included in this definition are any activities conducted as part of the administration of the program.[175]

139. (U) In the above definition, it is clear that TBS provides institutions with latitude in the derivation of their collection authorities – but the overarching requirement is that it must derive from some form of Parliamentary authorization. NSIRA notes that the Crown prerogative is by its nature not grounded in Parliamentary authority, and Parliament rarely approves its use. Therefore, if it is to be consistent with this interpretation of section 4, an institution's authority to collect personal information must derive from one of the forms of Parliamentary authority described above, such as an *Appropriation Act* approving an entity's expenditures.[176]

140. (U) [redacted]

---

[171] Hogg (above), chapter 1 at 1-20. See also Patrick J Monahan, Byron Shaw, and Padriac Ryan, *Constitutional Law,* 5th edition (Toronto: Irwin Law, 2017) at 57-58. Government of Canada, Office of the Judge Advocate General, *Crown Prerogative: The Crown Prerogative as applied to Military Operations*, Strategic Legal Paper Series Issue 2 (Ottawa: National Defence, 4 June 2018) at para. 2. *Entick v Carrington,* [1765] EWHC KB J98, 95 ER 807. *R v Mills,* [1999] 3 SCR 668 at para. 79

[172] Para. 76 of the *Privacy Act*

[173] Hogg (above), chapter 1 at 1-20, and chapter 10 at 10-15.

[174] Para. 71(1)(d) of the *Privacy Act* states: "The designated Minister shall cause to be prepared and distributed to government institutions directives and guidelines concerning the operation of this Act and the regulations."

[175] TBS Policy on Privacy Protection, Definitions.

[176] A notable exception to this is where statute expressly preserves prerogative, as in section 749 of the Criminal Code.

Notwithstanding any security markings appearing on this record, the information contained herein is declassified to UNCLASSIFIED

[redacted]

141. (U) Overall, the Crown prerogative is one of the most complex legal concepts in Canada's system of governance, with which Canadians are not generally familiar. NSIRA is concerned about its broad invocation to collect personal information about Canadians without clients specifying the discrete prerogative powers, demonstrating how this instrument meets the requirements of the *Privacy Act*, nor articulating a strong justification that warrants its invocation in every instance of collection.

142. (U) NSIRA remains unconvinced that federal institutions have adequately addressed the prerogative's applicability as an authority to disclose and collect information for national security purposes, and none of the consulted agencies have demonstrated an assessment of the prerogative in view of its widely accepted limitations against infringing on civil liberties of citizens.

177 [redacted]

Notwithstanding any security markings appearing on this record, the information contained herein is declassified to UNCLASSIFIED

ANNEX B: Disclosure of CII in relation to the *Investment Canada Act*

What is the *Investment Canada Act*?

143. (U) Throughout NSIRA's review, the *Investment Canada Act* (ICA) emerged as one of the primary legal instruments invoked by CSE's clients in requests for CII. The ICA enables the Minister of ISED to conduct national security reviews of proposed foreign investments into the Canadian economy to determine if they would be injurious to national security. Such investments can take the form of a non-Canadian acquiring control of all or part of a Canadian business. Regulations made under the *Act* designate federal departments and agencies as investigative bodies that may participate in such reviews.[178]

144. (S) Departments listed as investigative bodies review foreign investments by participating in interdepartmental committees at various levels of representation – ranging from the analyst to the Deputy Minister levels. Investigative bodies provide expertise in subject areas in line with their departmental mandates. [redacted].[179]

145. (TS//SI) While clients invoked the ICA in relation to relevant intelligence reporting,[180] some also invoked it the ICA in relation to reports in entirely different subject areas [redacted] Clients invoked the ICA both in relation to [redacted] and to [redacted]

146. (U) ICA-related disclosures contained [redacted] identities of corporations or other entities, but [redacted] of the [redacted] identifiers released for this purpose also contained personal information.[184] Given CSE's commitment to protect both types of information equally, NSIRA assessed disclosures of Canadian entities with the same lens as those that contained personal information.

147. (U) Upon noting irregularities in disclosures related to the ICA, NSIRA expanded the sample for these types of disclosures to encompass the period of July 1, 2015 to July 31, 2019 to better contextualize its findings.[185]

---

[178] *National Security Review of Investments Regulations.*

[179] CSE Response, "RE: PARTIAL RESPONSES TO Q 2, 2a, 11, 11a, 12b, 12c, 12d, 14 of RFI-14 - NSIRA Disclosures Review – ICA," February 6, 2020. CSE further explains, [redacted]

[180] E.g. Report serial [redacted] These are examples of reports detailing [redacted]

[181] E.g. Report serial [redacted] This is a report

[182] E.g. Report serial [redacted]

[183] E.g. [redacted]

[184] NSIRA's "Review Tracking Document."

[185] NSIRA recognizes that due to the expansion of the review period, some of the disclosures it reviewed may have been previously reviewed by OCSEC.

Notwithstanding any security markings appearing on this record, the information contained herein is declassified to UNCLASSIFIED

CSE's assessment of mandates and operational rationales

148. (U) NSIRA has observed that requests for CII in relation to the ICA have many of the same systemic issues as the disclosure program writ large. Entities request and receive CII based on reporting that does not relate to their mandates,[186] and cite the ICA in relation to reporting that bears no tangible relation to the Act[187] or in relation to economic activity over which it would not have jurisdiction.[188] Clients often invoke tenuous rationales for requesting CII,[189] which CSE accepts. Finally, the supervisor approval required to release CII for ICA purposes does not document why requests were approved.[190]

ICA as a lawful authority

149. (S) The ICA is one of the many legal instruments CSE has preapproved for citation by clients within the previously referenced operational procedures.[191] In majority of disclosure requests, clients invoked the ICA itself and/or their status as an investigative body under the Act as lawful authority.[192] In responses to NSIRA, CSE has stated that it disclosed CII using the authorities of the ICA, and based on requesters' designation as an investigative body under the Act,[193] demonstrating its acceptance of the ICA as lawful authority. When asked whether citing the ICA is sufficient to demonstrate clients' lawful authority, CSE responded that [redacted]

150. (S) Throughout the review, NSIRA was only presented with a legal opinion that stated that [redacted]

---

[186] E.g. Disclosures [redacted]

[187] E.g. Disclosures [redacted] These requests were largely made [redacted] NSIRA considers this connection [redacted] tenuous. [redacted] could more defensibly investigate this type of activity as part of its [redacted] mandate, and not for ICA purposes.

[188] E.g. Disclosures [redacted] These requests were largely based on reports that detailed [redacted] This type of CII cannot be requested in relation to an ICA matter, [redacted] as the ICA does not have jurisdiction over [redacted] as told to NSIRA [redacted] to their potential contravention, but not the ICA.

[189] Disclosure [redacted]

[190] E.g. Approvals for disclosures [redacted]

[191] [redacted] SOP: Releasing Suppressed Information.

[192] E.g. [redacted] and [redacted] In both cases the requester clearly states that their perceived lawful authority for collecting the CII is the *Investment Canada Act*. Other examples: [redacted]

[193] CSE Response, "PARTIAL RESPONSE Q1: NSIRA Disclosures Review - RFI-04," 7 October 2019. Also, in disclosure [redacted] analyst prompts the requester to potentially invoke the ICA for the request.

[194] CSE Response, "FINAL ANSWERS – RFI-4 – CII Review 2018-19," October 15, 2019, Q7a. Emphasis by NSIRA.

[195] CSE DLS Legal Opinion, March 10, 2017.

Notwithstanding any security markings appearing on this record, the information contained herein is declassified to UNCLASSIFIED

[redacted][196] When asked how CSE assessed whether the ICA serves as a collection authority, CSE stated that it has not sought a legal opinion on the subject.[197]

151. (U) The statements made by CSE above, its approval of the associated disclosures, and inclusion of the ICA in its procedures demonstrate CSE's certainty that the ICA is sufficient lawful authority for clients' collection of CII.

152. (S) As the review progressed, NSIRA made further inquiries in relation to the ICA, and received additional answers and a briefing from a key CSE group [redacted] In these later responses and in the briefing provided to NSIRA, CSE provided the following assessment of the ICA's authorities, which is also described similarly within the [redacted]

> [The investigative body] designation does not provide CSE with any new authorities outside of its regular mandate, except to receive, use, and disclose ICA privileged information in the execution of our native mandate. During the period under review…CSE's authority to conduct activities…under the ICA was derived from CSE's three-part mandate as described in subsection 273.64(1) of the National Defence Act (NDA).[198]

153. (U) It stands to reason that if its designation as an investigative body does not grant CSE with any new authorities outside of its regular mandate, neither does it grant any other investigative body such an authority. Further, if CSE conducted its activities in support of ICA reviews – including obtaining CII – under the authority of its core mandate, so too must the other investigative bodies requesting these identities rely on their core mandates. NSIRA agrees with this interpretation of the provisions of the ICA, but notes that it is incompatible with CSE's previously provided responses on the subject, with CSE's preclearance of the ICA in its operational procedures, and with its approvals of ICA-related disclosures that NSIRA has observed in practice.

154. (U) NSIRA engaged with some of CSE's clients that invoked the authority of the ICA in their requests, observing a haphazard interpretation of the Act's authorities within the community of CII requesters. When asked about their interpretation of the ICA, some stated that they believed the ICA and their status as an investigative body granted them the authority to request and collect CII from CSE, and some appeared to equate CII with 'privileged information' collected under the *Act*.[199]

155. (S) In a written response following a meeting with NSIRA, Transport Canada elaborated the following interpretation of the ICA's authorities, with which NSIRA agrees:

> The *Investment Canada Act* (ICA) does not provide TC, as an investigative body under the ICA, with any authority to collect and/or use CII. Under the ICA, investigative bodies are intended to rely upon their own statutory authorities to collect and obtain information, including CII. The ICA only authorizes the Minister of Industry, as the responsible Minister under the ICA, to disclose privileged information (obtained by that Minister under the ICA) to TC as an investigative body. The ICA then permits TC, as

---

[196] NSIRA's Review Tracking Document. CSE released [redacted] Canadian identifiers on the authority of the ICA during the expanded review period.

[197] CSE Response, "PARTIAL RESPONSE: Q1a. RFI-14 – NSIRA Disclosures Review – ICA," March 2, 2020, Q1. NSIRA posed the question: "Why or why not? If yes, please provide the legal opinion. If no, how has CSE assessed the applicability of the ICA as legal authority to receive and disclose CII?"

[198] CSE Response, "PARTIAL RESPONSES TO Q 2, 2a, 11, 11a, 12b,c,d, 14 of RFI-14 – NSIRA Disclosures Review – ICA," Q2a. Emphasis by NSIRA. This was further reiterated in a briefing to NSIRA on January 28, 2020. See also [redacted] Emphasis by NSIRA.

[199] Meetings with GC entities.

Notwithstanding any security markings appearing on this record, the information contained herein is declassified to UNCLASSIFIED

an investigative body, to further disclose the privileged information for the purposes of TC's investigations under the ICA. The privileged information received by TC from the Minister of Industry would not contain CII.[200]

156. (S) NSIRA notes that the inconsistent understanding of the roles and responsibilities of investigative bodies in relation to collection of CII may derive in part from a misinterpretation of the term 'privileged information.' For example, a CSE CRO wrote on behalf of ISED in one instance that "the regulations [made under the ICA] also provide a list of investigative bodies with which classified information can be shared and which may be used for the purpose of their own investigation."[201] Additionally, CSE's [redacted] related to the ICA also appears to classify CII as privileged information.[202]

157. (U) The only activity explicitly conferred on investigative bodies under the *Act* is the receipt, communication, or disclosure of privileged (not classified) information, for the purposes of administering or enforcing the *Act* and for conducting its own lawful investigations.[203] Further, the regulations referred to in the above request do not state anything beyond which entities are considered investigative bodies under the *Act*.[204] ISED confirmed to NSIRA that the term 'privileged information' pursuant to section 36 of the ICA includes proprietary information belonging to private entities submitted to and/or collected by the Minister of Industry as part of reviewing a foreign investment and would not refer to CII necessarily or explicitly.[205]

158. (U) The inconsistency in the interpretation of the various provisions of the ICA by CSE and requesting departments alike, both within disclosure requests and in responses to NSIRA on the subject, demonstrates a systemic misunderstanding within the community of the lawful authority underpinning one of the most prevalent types of CII disclosures.

'Double-blind' nature of requests

159. (S) Another characteristic of ICA-related disclosures is that they can most closely be described as 'double-blind.' On the one hand, clients often justify their requests by stating that the CII will support a specific investment review, at times providing [redacted] unit do not generally have knowledge of [redacted][207] and thus cannot confirm if the requested CII is actually connected. On the other hand, the clients themselves are also 'blind' as to the actual CII they are requesting because it is suppressed in the report. As a result, neither party can ascertain whether the requested CII is related to the ICA review until the client receives the CII.

---

[200] GC entity response, Annex B – TC Response to NSIRA RFI – March 2020. Emphasis by NSIRA.
[201] Disclosure [redacted]
[202] [redacted] April 2018, section 4.3: [redacted]
[203] *Investment Canada Act*, section 36(1)(3.1).
[204] *National Security Review of Investments Regulations*, para. 7.
[205] Briefing with ISED, February 3, 2020.
[206] For example, refer to disclosure request [redacted] Requesters elaborate a similar argument in [redacted] among other requests.
[207] [redacted] CSE Response, "FINAL ANSWERS – RFI-4 – CII Review 2018-19," October 15, 2019, Q7b.

Notwithstanding any security markings appearing on this record, the information contained herein is declassified to UNCLASSIFIED

160. (U) As a result, NSIRA could not confirm the proportion of released identifiers that were connected with the cited investment reviews. However, a case study of several disclosures where the requested CII was explicitly stated shows the release of identifiers that clients did not request.

161. (TS//SI) [redacted][208][redacted][209]

162. (TS//SI) [redacted][210]

Investigating economic activity outside ICA reviews

163. (TS) In some cases, clients cited the ICA as a lawful authority to obtain CII that appear to have pertained directly to ICA reviews [redacted].[211] NSIRA notes that the scope of the ICA covers only reviews of foreign investments into the Canadian economy, and NSIRA does not believe it authorizes investigative bodies' general investigations into any activities with a nexus to the Canadian economy.

164. (TS) Clients also often invoke the ICA to collect CII for the purposes of [redacted] outside the purview of a specific foreign investment review.[212] CSE describes this practice as [redacted] for which CII is considered an important component.[213] In practice, NSIRA has observed disclosures made for this purpose when intelligence reporting [redacted][214] In NSIRA's view, obtaining CII for this purpose constitutes [redacted] and not for a review conducted under the ICA.

---

[208] The clients reading the report would not know whether [redacted]

[209] [redacted]

[210] [redacted]

[211] E.g. CII released in relation to reports [redacted]

[212] E.g. Disclosures [redacted] In the first request, CSE states that it is being made [redacted]

[213] CSE Response, "PARTIAL RESPONSE: Q9,10, 13f,g,h RFI-14 - NSIRA Disclosures Review – ICA," March 3, 2020.

[214] E.g. Disclosures [redacted]

Notwithstanding any security markings appearing on this record, the information contained herein is declassified to UNCLASSIFIED

165. (TS) During NSIRA's engagement with ISED, NSIRA learned that there exist [redacted] distinct types [redacted]

166. (U) NSIRA does not dispute that these types of activities warrant comprehensive investigation by the federal government, but note that these transactions are by their nature outside the authority of the ICA itself. The most defensible manner of investigating these activities would be on an investigative body's own, independent authorities to conduct such investigations, and if they yield fruits over which the ICA would have jurisdiction, such as reviewable transactions that have not been brought to the Minister's attention, the Minister could then appropriately take jurisdiction. Until the jurisdiction of the ICA has been ascertained in respect of a transaction, CII collected in support of such investigations would be most appropriately collected on an investigative body's independent legal authorities, with a potential link to the ICA as the operational justification.

167. (TS) In its response to NSIRA on the subject, CSE stated that when the contents of an intelligence report are not clearly connected to a review, [redacted][216] As with regular CII disclosures, CSE assumes the existence of collateral information available to analysts as justification to approve requests that are not clearly connected to the ICA.

168. (TS) In summary, NSIRA believes the most defensible approach would be for clients to collect CII related to economic activity is under their own statutory authorities, if the reporting and type of CII aligns with the client's subject area of responsibility. If the requester believes the identity may be relevant to an ICA matter, it should be noted in the operational justification for the request, but the overall operational rationale should detail how the information will relate to the entity's own investigations related to economic security and the applicable authorities.[217]

169. (TS) This would not be a novel approach for CSE or the client community.[218] In nearly all requests for CII in this subject area, [redacted] cited its own collection authority, and noted ICA matters or economic security investigations as the operational justification.[219] As well, several requests made by [redacted] under the authorities of the ICA could be defensible if they were instead made under the [redacted] core collection authority.[220] If formalized as part of comprehensive information sharing agreements, NSIRA would consider this approach better aligned with the community's responsibilities

---

[215] Meeting with ISED, February 3, 2020; and CSE Factual Accuracy Comments, October 5, 2020.
[216] CSE Response, "FINAL RESPONSE - RFI-14, Q 7, 8," March 4, 2020, Q8.
[217] [redacted]
[218] CSE Response, FINAL RESPONSE – RFI-14, Q 7, 8." Q8. CSE itself explains here that the ICA serves as an operational justification under which the mandates of investigative bodies intersect, but that ultimately, each body is conducting an investigation under its own mandates and for their own operational purposes.
[219] E.g. Disclosures [redacted]
[220] E.g. Disclosure [redacted] which is based on reporting that directly relates to [redacted]

Notwithstanding any security markings appearing on this record, the information contained herein is declassified to UNCLASSIFIED

to protect both Canada's economic security and the privacy of Canadians.

The way forward

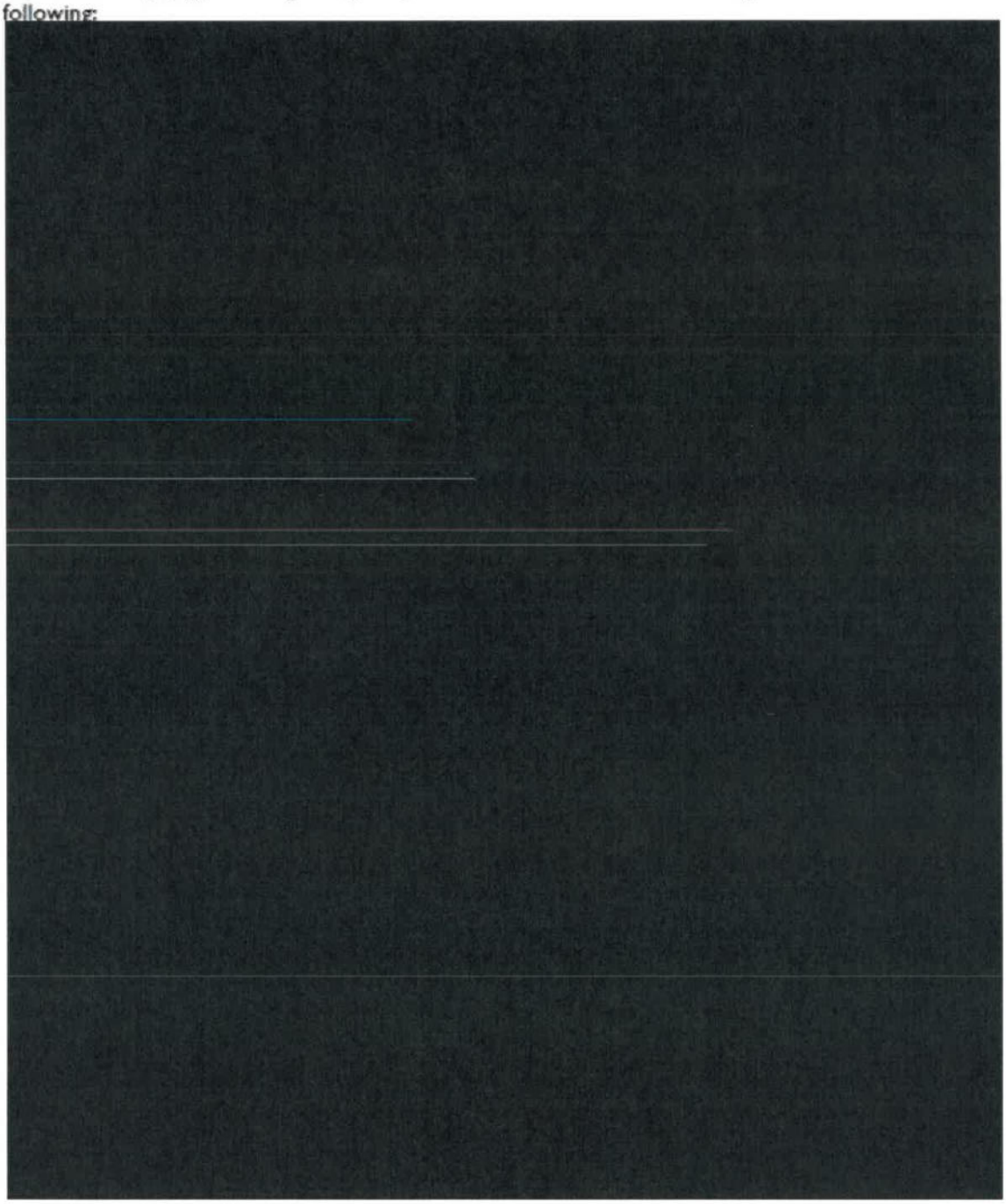
170. (U) Economic security is one of the most important pillars of Canada's national security. Investigating threats to Canada's economic security and [redacted] is essential to achieving that goal. NSIRA believes that this can be accomplished with a consistent, well-understood, and lawfully sound disclosure framework that is formalized in information sharing agreements with all GC clients that regularly request CII. At present, both CSE and its community of GC clients have systemically misinterpreted the provisions and authorities conferred on them by the *Investment Canada Act*, leading to its erroneous invocation and acceptance as a general lawful authority to collect CII.

Notwithstanding any security markings appearing on this record, the information contained herein is declassified to UNCLASSIFIED

ANNEX C: CSE's summary of client authorities

171. The following is the summary of client lawful authorities that CSE provides to its analysts who assess requests for CII.

In identifying the lawful authority (i.e. mandate) under which the information is being requested, the requester will have to identify an Act, an Order-in-Council, ministerial direction or other lawful authority (e.g., crown prerogative) to receive the information. Examples include the following:



Notwithstanding any security markings appearing on this record, the information contained herein is declassified to UNCLASSIFIED

ANNEX D: CSIS and CSE: Differences in treatment of CII

[redacted]

[redacted]

Notwithstanding any security markings appearing on this record, the information contained herein is declassified to UNCLASSIFIED

[redacted]

[redacted]

Notwithstanding any security markings appearing on this record, the information contained herein is declassified to UNCLASSIFIED

ANNEX E: Objectives, scope, and methodology

172. (U) This review examined a selected sample of disclosures for the period of July 1, 2018 to July 31, 2019. The review period was chosen as the juncture at which the CSE-related provisions of the *National Defence Act* were repealed, and the *Communications Security Establishment (CSE) Act* came into force.

173. (U) The review period for disclosures made under the ICA and in relation to section 16 of the *CSIS Act* were expanded as the review progressed, resulting in the analysis of further disclosures. NSIRA researchers examined CSE's electronic records, files, correspondence, and other documentation such as policies, procedures, and legal opinions of relevance to the disclosure of CII.

174. (U) NSIRA researchers submitted over 30 requests for information to CSE, CSIS, PCO, GAC, CRA, and TC from August 2019 to July 2020, and in totality received dozens of documents and responses to over a hundred questions.

175. (U) CSE organized eight briefings and information sessions for NSIRA in relation to this review, in addition to several other foundational briefings to provide NSIRA with broader knowledge of CSE's activities and operations. Informal meetings also regularly took place between NSIRA researchers and their CSE liaison counterparts to discuss the status of the review and to clarify information and document requests. As the review progressed, NSIRA requested briefings from six other GC entities in relation to their requests for CII, which were held at NSIRA and stakeholders' premises from November 26th to February 10th, 2020.

Notwithstanding any security markings appearing on this record, the information contained herein is declassified to UNCLASSIFIED

ANNEX F: Entities requesting CII

Client	Total identifiers processed by CSE, 1-Jul-18 to 31-Jul-19	% of all identifiers	Identifiers in NSIRA's Sample, 1-Jul-15 to 31-Jul-19[231]
Canadian Security Intelligence Service (CSIS)	[redacted]	[redacted]	[redacted]
Royal Canadian Mounted Police (RCMP)	[redacted]	[redacted]	[redacted]
Canada Border Services Agency (CBSA)	[redacted]	[redacted]	[redacted]
Communications Security Establishment (CSE)	[redacted]	[redacted]	[redacted]
Canadian Centre for Cyber Security (CCCS)	[redacted]	[redacted]	[redacted]
Privy Council Office (PCO)	[redacted]	[redacted]	[redacted]
Global Affairs Canada (GAC)	[redacted]	[redacted]	[redacted]
Public Safety and Emergency Preparedness Canada (PC)	[redacted]	[redacted]	[redacted]
Department of National Defence (DND)	[redacted]	[redacted]	[redacted]
Innovation, Science, and Economic Development Canada (ISED)	[redacted]	[redacted]	[redacted]
Canada Revenue Agency (CRA)	[redacted]	[redacted]	[redacted]
Financial Transactions and Reports Analysis Centre (FINTRAC)	[redacted]	[redacted]	[redacted]
Public Services and Procurement Canada (PSPC)	[redacted]	[redacted]	[redacted]
Integrated Terrorism Assessment Centre (ITAC)	[redacted]	[redacted]	[redacted]
Transport Canada (TC)	[redacted]	[redacted]	[redacted]
TOTAL	[redacted]	**100%**	[redacted]

[231] NSIRA's sample includes disclosures that extended beyond the initial review period, and as a result the number of identifiers for some departments exceeds the total amount of disclosures in the first column. Additionally, the number of identifiers in the first column may be understated because CSE employs a different methodology whereby multiple identifiers may be counted in one suppression.

Notwithstanding any security markings appearing on this record, the information contained herein is declassified to UNCLASSIFIED

ANNEX G: Meetings and briefings

- August 12, 2019: Briefing from CSE
- September 10, 2019: Briefing from CSE
- September 13, 2019: Briefing from CSE
- September 26, 2019: Briefing from CSE
- October 15, 2019: Briefing from CSE
- October 16, 2019: Briefing from CSE
- October 23, 2019: Briefing from CSE
- November 26, 2019: Meeting with Public Safety Canada
- December 2, 2019: Meeting with CSIS
- January 23, 2020: Meeting with CRA
- January 28, 2020: Briefing from CSE
- February 3, 2020: Meeting with ISED
- February 4, 2020: Meeting with PCO
- February 5, 2020: Meeting with GAC
- February 10, 2020: Meeting with RCMP
- March 6, 2020: Meeting with TC

Notwithstanding any security markings appearing on this record, the information contained herein is declassified to UNCLASSIFIED

ANNEX H: Findings and Recommendations

Findings

(U) Finding no. 1: NSIRA finds that CSE has developed policies and procedures designed as an internal oversight mechanisms for the disclosure of CII. However, NSIRA finds that CSE's implementation of these mechanisms was inadequate. The practices that NSIRA singles out for particular concern include:

a. CSE has accepted requests that do not state a lawful authority, even after the implementation of a new system meant to address this issue.

b. The analysts responsible for CII disclosures did not receive written guidance related to assessing the substance and validity of disclosure requests, as the guidance and training materials currently in place focus only on logistical procedures for releasing CII to domestic clients.

c. The analysts responsible for CII disclosures are not required to document their rationales and assessment of domestic requests, which could provide insight into how analysts have validated specific disclosures. As such, NSIRA was not able to assess if any further validation occurred for those disclosures where the clients did not state legal authorities or offered weak operational rationales.

d. CSE's current procedures do not provide Client Relations Officers sufficient guidelines in relation to advance releases of CII.

e. The CSE supervisor responsible for approving requests and conducting compliance checks did not document their rationale for request approvals, and did not identify any concerns regarding disclosures as part of their monthly compliance checks.

(U) Finding no. 2: NSIRA finds that CSE has not sufficiently assessed the legal instruments its clients invoke to collect CII. CSE has preapproved within its Standard Operating Procedures a number of legal instruments that clients can invoke to request CII, without conducting an underlying assessment. As a result, CSE has accepted clients' invocation of the Crown prerogative and the *Investment Canada Act,* that NSIRA believes may not grant departments powers to collect personal information about Canadians in the broad manner in which they have been applied.

(U) Finding no. 3: NSIRA finds that CSE's most frequent requesters of CII (CSIS, RCMP, and CBSA) articulated strong operational rationales that showed a direct relationship between the requested CII and their mandated activities, generally translating to their justified collection of CII from CSE.

(U) Finding no. 4: NSIRA finds that CSE's implementation of its disclosure regime may not have complied with its obligations under the *Privacy Act*. CSE has released CII to clients other than CSIS, RCMP, and CBSA that did not articulate a lawful authority and did not demonstrate a direct and immediate relationship between the CII and their mandated activities. Clients also at times received more information than they requested. CSE has not demonstrated that it has conducted a sufficient case-by-case evaluation of the justification invoked by the requesting clients prior to disclosing personal information.

(U) Finding no. 5: NSIRA found that the management of CSE's CII disclosure regime did not provide its community of clients a sufficient understanding of the structures and responsibilities underlying the

Notwithstanding any security markings appearing on this record, the information contained herein is declassified to UNCLASSIFIED

sharing of Canadians' personal information. This regime does not foster an arrangement in which clients and CSE can take equal responsibility for the disclosure and collection of Canadians' personal information.

(U) Finding no. 6: NSIRA finds that the Federal Court has not been fully informed about CSE's disclosure of personal information about Canadians, particularly relating to Canadian officials and other sensitive groups, derived from the warrants the Federal Court issued to CSIS in relation to s.16 of the *CSIS Act*. CSE has disclosed information collected pursuant to the Court's warrants in a manner that contradicts key principles previously outlined to the Court by CSIS.

Notwithstanding any security markings appearing on this record, the information contained herein is declassified to UNCLASSIFIED

Recommendations

(U) Recommendation no. 1: CSE should enhance the rigour of its internal practices related to CII. Firstly, CSE should update its policies to require that supervisors and analysts document their assessments and rationales for approving or denying disclosure requests.

(U) Recommendation no. 2: 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.

(U) Recommendation no. 3: CSE should ensure that the role of its Client Relations Officers is limited to facilitating the release of CII only when clients explicitly request it.

(U) Recommendation no. 4: 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.

(U) Recommendation no. 5: 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.

(U) Recommendation no. 6: CSE should revise its Standard Operating Procedures to reflect the legal advice it receives in response to Recommendation 5.

(U) Recommendation no. 7: NSIRA recommends that CSE cease disclosing CII to clients other than CSIS, RCMP, and CBSA until it implements the recommendations contained throughout this report.

(U) Recommendation no. 8: 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.

(U) Recommendation no. 9: NSIRA recommends that a Privacy Impact Assessment be undertaken in relation to CSE's CII disclosure regime.

(U) Recommendation no. 10: 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, particularly when it pertains to Canadian officials and other sensitive groups described in this report.

(U) Recommendation no. 11: NSIRA recommends that CSE cease disclosing CII collected pursuant to s.16 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.