

TOP SECRET // SI // CEO



**National Security
and Intelligence
Review Agency**

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

Review of the Communications Security Establishment's Signals Intelligence Data Retention

NSIRA // Review 23-14

TOP SECRET // SI // CEO

Table of Contents

List of Abbreviations	ii
Glossary of Terms	iii
Executive Summary	iv
1. Introduction	1
Authority	1
Scope of the Review	1
Methodology	1
Review Statements	2
2. Background	2
Legal Framework for SIGINT Data Retention	3
Collection, Retention, and Disposition of SIGINT Data	3
3. Findings, Analysis, and Recommendations	5
Handling of Canadian Information.....	5
Information with No Foreign Intelligence Value.....	7
Issues in SIGINT Policy and Practice	12
4. Conclusion.....	18
Annex A. SIGINT Data Retention Schedule.....	20
Annex B. Technical Inspection Summaries	22
Annex C. Findings and Recommendations	25

List of Abbreviations

Chief Chief of CSE

[REDACTED]

CSE Communications Security Establishment

FI Foreign intelligence

FIA Foreign intelligence authorization

FVEY Five Eyes

GC Government of Canada

IC Intelligence Commissioner

IRTC Information relating to Canadians or persons in Canada

**MND or the
Minister** Minister of National Defence

MPS FI Mission Policy Suite Foreign Intelligence

NSIRA National Security and Intelligence Review Agency

SIGINT Signals intelligence

Glossary of Terms

Five Eyes	International intelligence-sharing partnership between Canada, Australia, New Zealand, the United Kingdom, and the United States.
Foreign intelligence	Information about the capabilities, intentions or activities of a foreign individual, state, organization, or terrorist group, as they relate to international affairs, defence, or security.

Incidental collection	Acquisition of information that was not itself deliberately sought as part of an information acquisition activity and that was not directed at a Canadian or person in Canada.
Mission Policy Suite Foreign Intelligence	The Mission Policy Suite Foreign Intelligence (MPS FI) is CSE's SIGINT operational policy. Throughout this report, references to the MPS FI refer to the version approved in August 2023.
Selectors	Unique identifiers associated with an entity, such as a phone number, email address, or social media account.
SIGINT data	For the purpose of this report, SIGINT data refers to all raw and processed communication "traffic" (see below), acquired under section 16 of the CSE Act, held in collection stores accessible to and under the control of CSE.
Target	Any entity (individual, corporation, organization, or foreign state) that is of foreign intelligence interest to CSE.
Targeting	Activities undertaken by CSE to gain access to information related to a target.
Traffic item	The fundamental unit of SIGINT content data within CSE systems. Individual communication, or signal transmitted over a communication channel, that has been collected for SIGINT purposes. Traffic items may also consist of content other than communications, such as files [REDACTED]

TOP SECRET // SI // CEO

Executive Summary

Within the Government of Canada, the Communications Security Establishment (CSE) is the national signals intelligence (SIGINT) agency for foreign intelligence. To collect foreign intelligence, CSE develops, operates, and maintains extensive capabilities to collect, process, and analyse electronic communications.

While CSE is empowered to take extraordinary measures in collecting this information, with oversight provided through authorizations issued by the Minister of National Defence and approved by the Intelligence Commissioner, it is subject to conditions when doing so.

A central constraint on CSE's collection concerns information related to a Canadian or a person in Canada (IRTC). The CSE Act prohibits CSE from directing its activities at Canadians, though it is permitted to incidentally acquire IRTC in the course of its activities. Where this information has foreign intelligence value, CSE can retain it, subject to certain safeguards; if it is not of value, CSE must delete it.

More generally, CSE is subject to the condition that any information acquired under an authorization must be retained for no longer than is reasonably necessary. Setting and adhering to a retention schedule is key for CSE's compliance with this condition.

In this review, the National Security and Intelligence Review Agency (NSIRA) examined the technical ecosystem that enables CSE to retain SIGINT data. NSIRA sought to determine if and how CSE met its legal obligations related to SIGINT data retention. NSIRA also assessed whether CSE holds onto SIGINT data for no longer than its retention schedule, and whether the schedule adequately reflects all types of data CSE collects.

Many of CSE's SIGINT systems have automated policy enforcement mechanisms, including measures to protect IRTC. These enable CSE to delete IRTC with no foreign intelligence value, or other information it collected in a non-compliant manner.

Nonetheless, NSIRA identified an area of primary concern in CSE's treatment of information with no foreign intelligence value. While this primarily concerns non-Canadian information, it nonetheless creates potential for over-retention of information:

- CSE's foreign intelligence retention schedule does not differentiate between non-Canadian information with potential or identified foreign intelligence value and non-Canadian information determined to have no foreign intelligence value. This is indicative of a gap between how CSE's collection and retention authorities are presented to the Minister and how they are reflected in CSE's operational policies and practices.

TOP SECRET // SI // CEO

- In at least two instances (of four inspections conducted), CSE planned to retain collected non-Canadian information despite having determined that it had no foreign intelligence value. This may not be in compliance with the terms and conditions of the *Foreign Intelligence Authorization for Network Operations*, issued under section 26 of the CSE Act.
- More generally, CSE lacks mechanisms to delete certain non-Canadian information determined to have no foreign intelligence value prior to the end of its retention period. This may cause CSE to retain such information for longer than reasonably necessary.

In addition to this area of concern, NSIRA found inadequacies and limitations in the following areas of CSE's SIGINT-related policy and practice:

- ensuring analysts de-target selectors [REDACTED] that are no longer of foreign intelligence interest;
- requesting authority from the Minister to retain [REDACTED] information [REDACTED] despite a lack of readiness to do so in practice, and no policy requirement to periodically assess the information for foreign intelligence value;
- handling SIGINT data stored outside of CSE's main, managed systems for SIGINT data; and
- ensuring data retention requirements are respected when sharing with other agencies, such as its Five Eyes partners.

15(1)(d)
15(1)(f)

Given the varied operational needs of SIGINT collection—which can be difficult to predict in advance, and change over time—CSE requires data to carry out its mission, while being subject to important constraints on its retention of collected data. CSE's commitment to respecting data retention requirements was evident in this review, especially in its handling and protection of IRTC. Nevertheless, given the issues noted above, including instances of potential non-compliance with its *Foreign Intelligence Authorization for Network Operations*, CSE must continue to prioritize data retention and compliance.

TOP SECRET // SI // CEO

1. Introduction

Authority

1. This review was conducted under the authority of paragraph 8(1)(a) of the *National Security and Intelligence Review Agency Act* (NSIRA Act).

Scope of the Review

2. NSIRA examined the technical ecosystem that enables CSE to retain SIGINT data (information acquired under section 16 of the CSE Act). NSIRA sought to determine if and how CSE met its legal obligations related to SIGINT data retention. NSIRA focused on CSE's retention of data in operational systems, including those used for collection, processing, and analysis.
3. CSE's retention of SIGINT data is guided by a retention schedule (see Annex A). NSIRA assessed whether CSE retained SIGINT data for no longer than this schedule, and whether the schedule adequately reflects all types of data CSE collects.
4. CSE's technical ecosystem for SIGINT data retention is complex, including numerous systems and capabilities. After reviewing these systems at a high level, NSIRA focused on a subset of the systems used to collect, process, visualize, and retain SIGINT data.
5. The period under review was October 2020 to April 2024.

Methodology

6. NSIRA received briefings and attended onsite technical demonstrations delivered by CSE subject matter experts. NSIRA also requested written documentation from CSE, including written responses to specific questions.
7. NSIRA conducted four technical inspections as part of its verification of CSE's SIGINT data retention policies, practices, and technical measures. These enabled NSIRA to assess statements made by CSE about its practices by inspecting actual collected data within CSE's SIGINT systems. For each, NSIRA met with CSE staff responsible for targeting, acquiring, and assessing a specific stream of SIGINT data. NSIRA describes these in detail in Annex B.

TOP SECRET // SI // CEO

Review Statements

8. The NSIRA Act grants NSIRA rights of timely access to any information in the possession or under the control of a department (except for Cabinet confidences) and to receive from the department any documents and explanations NSIRA deems necessary. NSIRA monitors cooperation with access requests, including the completeness and accuracy of disclosures, which inform its overall assessment of a department's responsiveness in each review.¹
9. CSE partially met NSIRA's expectations for responsiveness during this review. CSE officials ensured NSIRA received documents requested in a timely way and proactively provided information during meetings and briefings. However, CSE did not provide NSIRA with direct access to the collaborative tools it operates. Instead, it provided NSIRA with copies of the information in a format that was difficult to review. In addition, NSIRA was unable to review CSE's use of Five Eyes collaborative tools, because CSE did not provide access to this information. Despite CSE only partially meeting NSIRA's expectations for responsiveness, NSIRA remains confident in the findings and recommendations contained in this report.

2. Background

10. As the Government of Canada's (GC) SIGINT agency, CSE acquires information about the activities of foreign entities that are of interest to the GC, as expressed in its intelligence priorities. CSE uses advanced capabilities to collect, understand, and interpret any kind of electronic communication—including telephone calls, text messages, computer and internet communications, and satellite signals.
11. This collection is vast. Electronic communication occurs in differing formats, at significant speeds and volumes, according to frequently changing or evolving protocols, and is subject to the increasing adoption of strong encryption practices. In response, SIGINT agencies collect data both passively, by copying communications traffic, and [REDACTED] To enable this, CSE has developed a range of capabilities and sources to identify, retrieve, and securely store information for its foreign intelligence (FI) mandate. This information is then processed, analysed, and disseminated to GC clients.
12. As a federal agency, CSE is subject to the law and GC policies in regard to the handling and disposition of information in its holdings. This extends to the

¹ NSIRA's "Expectations for Responsiveness in Reviews" are online at <https://nsira-ossnr.gc.ca>.

TOP SECRET // SI // CEO

information CSE collects for intelligence purposes. Accordingly, retention is a core concern of CSE's policy compliance for its FI activities.

Legal Framework for SIGINT Data Retention

13. CSE's legal authorities for SIGINT data retention begin with its authority to collect SIGINT data. Section 16 of the CSE Act sets out the FI aspect of CSE's mandate which is to acquire SIGINT information and use the information acquired to provide FI in accordance with the government's intelligence priorities.
14. Practically, CSE exercises this aspect of its mandate through the authorities set out in foreign intelligence authorizations (FIAs). These FIAs, issued by the Minister and approved by the Intelligence Commissioner (IC), set out the means and methods for CSE to carry out this aspect of its mandate. Particularly relevant to the activities described in this report is the *Foreign Intelligence Authorization for Network Operations*, a version of which was issued each year of the period under review.
15. The approved FIAs do not exist in isolation. The Minister issues an FIA based on the written application of the Chief of CSE, and the same information is subsequently provided to the IC. The contents of the application package necessarily inform the decisions made by the Minister and the IC, and the application must set out the facts that would allow the Minister to conclude that the authorization is necessary and that the conditions for issuing it are met.
16. The Mission Policy Suite Foreign Intelligence (MPS FI), CSE's main policy for the conduct of its FI activities, is appended to the application itself. The MPS FI includes a retention schedule based on the type of information, how it was acquired, and whether it has a recognized Canadian privacy interest (see Annex A). Prior to issuing an FIA, the CSE Act requires the Minister to conclude that there are reasonable grounds to believe that any information acquired will be retained for no longer than is reasonably necessary (paragraph 34(2)(a)). The retention schedule represents CSE's policy interpretation of what is "reasonably necessary".

Collection, Retention, and Disposition of SIGINT Data

17. What data to retain, and for how long to retain it, is a core concern for CSE. First, CSE is subject to significant constraints for SIGINT data related to Canadians and persons in Canada. If such data is collected and is found to not be essential to CSE's mission, CSE must be able to remove it from its systems—to shorten its retention, in other words. Second, CSE cannot practically collect and retain all data that *might* be of interest. Storing data is expensive, as is the technical expertise to develop and maintain CSE's systems to collect, retain, and query SIGINT data.

15(1)(f)

TOP SECRET // SI // CEO

While CSE may have the authority to retain data for a certain period of time, [REDACTED]
[REDACTED]

18. SIGINT data has a lifecycle. Data goes through a series of systems designed to collect, enrich, process, store, and ultimately make it available to CSE's intelligence analysts. Typically, SIGINT data is processed by multiple systems before an intelligence analyst can query and analyze it. When an analyst finds useful information, they can reference it in an intelligence report or use it to develop future collection.
19. All collected SIGINT data is assigned a series of identifiers attached to the data which allows CSE's systems to process it according to its characteristics, including the authority under which it was collected and its scheduled deletion date. Notably, this enables CSE's systems to automatically identify and delete data as required.
20. Data is subject to different retention periods, depending on its characteristics. These retention periods are established in CSE's retention schedule (see Annex A). For example, if data is recognized as having a Canadian privacy interest, it generally has a much lower retention period—or cannot be retained at all. For other types of data, retention periods range from [REDACTED] for certain unselected information, to [REDACTED] for most of the communications CSE collects. [REDACTED]
[REDACTED]
21. During the period under review, CSE sought policy exemptions to extend the retention for specific data beyond its standard retention period, for operational reasons.
22. When analysts assess data, CSE can take one of three actions to affect its retention period.
 - First, data can be "reported". This is used when analysts include or refer to collected data in an intelligence product. The data's retention period is then extended to [REDACTED]
 - Second, data can be "annotated". This is used to indicate a recognized Canadian privacy interest. If the data does not meet the standards for continued retention, it is then scheduled for deletion within [REDACTED]
 - Third, data can be "purged". This is used when data has been collected in a non-compliant manner. The data is then prioritized for deletion across all CSE systems (and Five Eyes systems, if the data was shared) within [REDACTED]

Only certain analysts, tasked with providing data assurance, can initiate purge requests; this usually occurs in response to a compliance incident. Purges have higher reporting requirements than conventional deletions: system owners must

TOP SECRET // SI // CEO

confirm the data was deleted; the number of affected traffic items is tracked through a compliance report.

23. Once data reaches its retention period, it must be disposed of, unless it has archival value (i.e., it supports an intelligence report). The Librarian and Archivist of Canada permits CSE to dispose of 'all raw and processed communication "traffic" held in collection stores accessible and under the control of CSE'—what is referred to in this report as SIGINT data—when CSE determines it has "no remaining operational or legal requirements" to retain it.

3. Findings, Analysis, and Recommendations

Handling of Canadian Information

Finding 1. NSIRA found that CSE implemented safeguards to protect the privacy of Canadians and persons in Canada within SIGINT data retention systems, tools, and capabilities.

24. CSE acquires, processes, and retains SIGINT data using a complex and ever-changing ecosystem of databases, applications and services. The nature of SIGINT data requires CSE to regularly develop and modify its collection and processing systems. Periodically, CSE also retires systems, migrating their functionality into existing systems or developing new ones.
25. In addition to its own systems, CSE relies [REDACTED] services and tools—developed and maintained [REDACTED] and Five Eyes (FVEY) partners alike—which contribute additional complexity to CSE's ecosystem. These tools often require CSE to adapt to data and technologies it cannot control. The retention implications of this reliance are discussed under Finding 10.
26. CSE manages its complex technical ecosystem in a "distributed" manner, meaning ownership of the components are not centralized. [REDACTED] engineers and computer scientists develop and maintain the repositories, applications, and services within CSE's ecosystem.
27. The MPS FI requires a consistent approach to the development and maintenance of systems. This includes ensuring that systems receive and retain compliant data, that appropriate access controls are in place, and that systems are documented. NSIRA observed various practices within CSE to ensure that policy and the systems implementing that policy are mutually informed. For example, staff from a major collection program described their annual input to the ministerial

15(1)(d)

15(1)(f)

TOP SECRET // SI // CEO

authorization process, ensuring the technical details of their collection are accurately reflected, while also confirming their understanding of the compliance requirements deriving from the authorization. Similarly, staff responsible for a core analytical system described how CSE's policy teams engage proactively when new policy requirements emerge.

28. The CSE Act prohibits CSE from directing its activities at Canadians or persons in Canada. CSE has implemented many controls and mechanisms to limit the likelihood of acquiring or retaining information relating to a Canadian or person in Canada (IRTC). For example, one set of tools uses [REDACTED] to filter traffic before it enters CSE's data retention platforms. CSE analysts are also required to conduct foreignness assessments throughout the SIGINT lifecycle, to limit the likelihood that CSE directs its activities at Canadians or persons in Canada.
29. Despite these controls, CSE may still inadvertently collect IRTC. For these cases, CSE has implemented processes to handle IRTC that is collected and recognized as such. Once recognized, there are two ways that an analyst can handle IRTC:
 - If the analyst deems the data essential to international affairs, defence, or security (per 34(2)(c) of the CSE Act), they must annotate it as essential IRTC, and it remains retained. Its retention period, however, is shortened to [REDACTED]; to retain the data past these [REDACTED], the analyst must re-assess whether the data remains essential, restarting the [REDACTED] window each time.
 - If the analyst does not deem the data essential, they must annotate it as non-essential IRTC, which triggers a deletion process in CSE's systems. Systems must delete the data within [REDACTED] of the annotation.
30. When data is collected in a non-compliant manner (e.g., data collected from a target while they were in Canada), CSE uses a purge mechanism to prioritize its deletion from their systems.
31. One of the four inspections conducted included data that had been subject to a purge request. NSIRA reviewed correspondence tracking the purge request, and confirmed that the affected traffic items had been purged.
32. Given the nature and volume of modern communications, and the scope of its FI mandate, it is inevitable that CSE will encounter IRTC in carrying out its FI collection. While CSE may not seek such information—and CSE has implemented safeguards to prevent directing its activities at Canadians or persons in Canada—it will encounter it, and therefore should have robust processes for handling it once identified. The systems that enable SIGINT provide analysts tools for this task, balancing the inevitability of encountering IRTC with mechanisms to delete or purge it.

TOP SECRET // SI // CEO

Information with No Foreign Intelligence Value

Finding 2. NSIRA found that CSE's foreign intelligence retention schedule does not account for non-Canadian information with no foreign intelligence value.

Finding 3. NSIRA found that CSE lacks institutional mechanisms to delete certain non-Canadian information with no foreign intelligence value, posing a risk that CSE retains such information for longer than reasonably necessary.

Finding 4. NSIRA found that CSE retained collected non-Canadian information despite having determined that the information had no foreign intelligence value. This may not be in compliance with the terms and conditions of the *Foreign Intelligence Authorization for Network Operations* issued under section 26 of the CSE Act.

33. Determining FI "value" is not straightforward. It is a subjective determination, based on knowledge and expertise by individuals working on ever-evolving sets of targets. If the vast information CSE collects is a haystack, the information with FI value therein is the needle—but, crucially, what may appear to be a needle to one analyst, may seem mere hay to another, depending on what is of value to their respective areas. Similarly, what may appear not to be a needle today could be one tomorrow, as the FI landscape shifts. As a result, CSE errs on the side of caution in its handling of collected information, preferring to retain as much as possible within the bounds of its retention schedule—what is deleted often cannot be collected again.
34. Despite this, there are situations where intelligence analysts determine collected information to have no FI value. This section addresses such situations. Of note, NSIRA did not independently assess the FI value of collected information—the observations below are based on the assessment of CSE analysts.
35. The FIA application and subsequent approval process involves multiple steps and review by the Chief, the Minister, and the Intelligence Commissioner. Paragraph 35(d) of CSE Act requires the FIAs to specify "any terms, conditions or restrictions that the Minister considers advisable....to ensure the reasonableness and proportionality of any [authorized activity]." The Minister included a condition in the *Foreign Intelligence Authorization for Network Operations* related to the acquisition and retention of information:

[I]nformation is acquired based on CSE foreign intelligence requirements. This serves to limit the amount of information that is retained to information that is believed to contain foreign intelligence or support CSE's foreign intelligence mandate.

15(1)(d)
15(1)(f)

TOP SECRET // SI // CEO

This condition applies to all activities conducted under the FIA, and offers a standard for FI value: whether information is believed to contain FI or support CSE's FI mandate. To the extent that data is determined not to meet this condition, then its continued retention may not be authorized under the FIA issued pursuant to section 26 of the CSE Act.

36. The FIA application packages throughout the period under review explain adherence to this condition by stating that "CSE only retains information that will further the foreign intelligence aspect of CSE's mandate per [MPS FI]." Given this statement, it is reasonable to expect that CSE distinguishes between information of realized or potential value (information that will further its FI mandate aspect) and information without such value (information that will *not* further its FI mandate aspect). However, the MPS retention schedule makes no such distinction, except for IRTC. The MPS does not reflect the statement made to the Minister—there is no requirement that would see CSE "only retain" such information, nor support to remove data with no FI value prior to the end of its retention period.
37. In the course of this review, NSIRA conducted four inspections of data CSE had collected [REDACTED] (see Annex B). In one of these inspections (inspection 3), the data collected enabled further FI activities. In the other three inspections, CSE analysts had found that the information collected from [REDACTED] had no FI value:
 - In inspection 1, CSE had a particular target in mind, and believed that [REDACTED] was used by that target. The collected information revealed [REDACTED] did not belong to the intended target, but rather to an unrelated individual who was not of FI interest.
 - In inspections 2 and 4, CSE did not have a named or known target in mind; rather, it [REDACTED] based on [REDACTED]. The collected information revealed that the owners of [REDACTED] did not fit that profile, and [REDACTED] were not of FI interest.
38. In inspection 2, the analyst identified a weak indication of a potential connection to Canada and deleted the data. This occurred through CSE's purge process, and included adding [REDACTED] to the protected entity list to prevent future targeting. This inspection confirmed CSE's processes for deleting information with a Canadian privacy interest working as they should.
39. In inspections 1 and 4, the analysts marked the collected data to indicate it had no FI value, expecting this action to also prevent future targeting of [REDACTED]. This did not work as the analysts had intended, an issue discussed under Finding 6.

15(1)(d)
15(1)(f)

TOP SECRET // SI // CEO

Nevertheless, it was a clear assessment, by experts on these targets, that the collected information had no FI value.

40. Despite the determination that the data had no FI value, there was neither an expectation for analysts to delete it from CSE systems, nor a known mechanism for them to do so. Later in the review, when pressed on this point, CSE noted that "a manual, ad-hoc deletion process can be initiated by submitting a request to our system administrators through our ticketing system". However, CSE did not demonstrate to NSIRA that it had communicated this process to analysts. By contrast, if there had been an indication of a connection to Canada, as with inspection 2, the analyst could have initiated CSE's purge process.
41. CSE relied on the FI retention schedule set out in the MPS to retain the data from ██████ reviewed in inspections 1 and 4. However, there appears to be a gap between the CSE Act, the FIAs, and the MPS with regard to the retention of data with no FI value. As described above, while the MPS does not distinguish between information with and without FI value, the FIA and its supporting application both establish a standard for retaining information tied to its value. CSE determined this information had no FI value. Continuing to retain this information may not meet the condition for retention set out in the FIA.
42. CSE's information acquisition and retention authority is not indiscriminate. While the CSE Act and FIAs authorize the initial acquisition of information that responds to the GC's intelligence priorities, subsequent assessment of that information may reveal that it does not, in fact, respond to those intelligence priorities. Absent a policy that differentiates between data with and without FI value, CSE risks continuing to retain information contrary to the FIA condition noted above.
43. The value of collected data may not be immediately clear, or data may be without value to one team but potentially of value to another. A decision to retain this data, in some cases, may not run counter to the condition. Policy can address such reasonable nuances. However it is not reasonably necessary to retain data for ██████ when that data has been assessed to have no FI value. This is especially clear in data reviewed during the inspections: in one, the data did not correspond to the known, intended target; in two others, the data revealed that the individuals targeted did not fit the expected ██████ and were not of FI interest.

Recommendation 1. NSIRA recommends that CSE immediately delete the data determined to have no foreign intelligence value identified in inspections 1 and 4, as retaining this data is not reasonably necessary.

15(1)(d)

15(1)(f)

TOP SECRET // SI // CEO

Recommendation 2. NSIRA recommends that CSE amend the Mission Policy Suite to create a category for non-Canadian information determined to have no foreign intelligence value, and set a timeline for its deletion that ensures it is retained for no longer than reasonably necessary.

Finding 5. NSIRA found that CSE's chosen approach to processing some types of SIGINT data into "traffic items", by which multiple individual communications are sometimes grouped into a single item, may lead to retention of information with no foreign intelligence value.

44. When CSE collects SIGINT data, it processes it to produce and retain discrete "traffic items", the fundamental unit on which CSE's retention mechanisms operate. What constitutes a traffic item will vary by the method of collection and how CSE has chosen to process it.
45. CSE's [REDACTED] program allows CSE to access [REDACTED] contained within them. Acquiring information directly [REDACTED] is one method CSE uses [REDACTED] communications transiting information networks.
46. [REDACTED] traffic items are not necessarily equivalent to individual communications. When, for example, CSE collects [REDACTED] it chooses to do so through a single traffic item: [REDACTED] and, once processed, stored as a single traffic item. In this case, a single traffic item includes multiple, [REDACTED] of individual communications. In other cases, CSE's collection and processing could result in [REDACTED] traffic item that contains a single [REDACTED] found on [REDACTED]
47. Given the wide variety of communications technologies from which CSE conducts [REDACTED] collection, [REDACTED] traffic items can be complicated for analysts to review. To facilitate their work, CSE has built secondary processing systems that [REDACTED]
[REDACTED]
Continuing the [REDACTED] example, this would present each [REDACTED] as an [REDACTED] These secondary processing systems can improve over time, such as [REDACTED]
[REDACTED] necessitate a change to the secondary processing. When this occurs, CSE [REDACTED]
[REDACTED]
[REDACTED] This reduces the need for analysts to [REDACTED]

15(1)(d)
15(1)(f)

TOP SECRET // SI // CEO

████████████████████ enabling them to focus on their assessment and reporting of FI.

48. Within CSE's SIGINT systems as currently architected, the original █████ traffic items are the foundation for its reporting and retention processes. When reporting, for example, on █████ CSE would adjust the retention period of the original traffic item containing the entire database of █████ from █████ Because the retention period adjustment occurs at the traffic item level, █████ in the database would be retained for the extended period, not just █████ used for the reporting.
49. This constrains the options available to analysts when faced with IRTC, or information collected in a non-compliant manner. For example, if a foreign target had a █████ exchange with a Canadian, that Canadian's █████ would have a Canadian privacy interest, but the communications with non-Canadians would not. In this case, CSE would only be able to delete █████ with the Canadian privacy interest by deleting the entire database of █████ collected from the target's phone.
50. This poses a clear dilemma for CSE when a █████ might have some █████ of FI value, alongside other █████ with a Canadian privacy interest but no FI value. With CSE's current implementation, an analyst could only retain those messages of FI value by also retaining the █████ with a Canadian privacy interest that had no FI value.
51. This dilemma is not merely a hypothetical possibility. In 2023, an intelligence team within CSE shared details of a potential incident with CSE's internal compliance team responsible for ensuring compliance with the MPS. At issue were certain █████ collected from █████ collection, which appeared to be IRTC. While CSE ultimately deemed the collection to be compliant, the intelligence team noted this very problem when discussing potential remedies: when advised by the compliance team that the IRTC █████ in question must be annotated for deletion, the intelligence team responded that the only way to do so was to delete the entire database of collected █████ However, doing so would delete other █████ that had clear FI value and would not have required annotation had they been collected separately.
52. CSE raised technical limitations when asked if they had considered solutions to address this issue. The ever-shifting nature of █████ for example, can pose issues with reliably deconstructing a database of collected █████ into its constituent parts; CSE's current implementation retains the entire database of this type of collection as the raw traffic item on which it bases all subsequent processing and analysis. But CSE's choice to do so is not without consequence.

15(1)(d)
15(1)(f)

TOP SECRET // SI // CEO

Notably, CSE has responsibilities related to retention, especially when compliance concerns (like Canadian privacy interests) arise. As a result of this approach, CSE may retain information of no FI value, including, potentially, such information with Canadian privacy interests.

53. While this issue was immediately apparent in CSE's [REDACTED] program, it could apply to its other collection programs. For example, CSE's [REDACTED] program enables CSE to collect transmissions transiting over infrastructure [REDACTED]. These transmissions, in many cases, correspond directly to communications, such as [REDACTED]. When processed as traffic items, CSE can then apply its retention and deletion methods more surgically; when a single [REDACTED] is a single traffic item, the dilemma noted above is less likely to arise. But CSE's [REDACTED] program is not infallible in this regard: it could collect [REDACTED]. This would present the same compliance concerns.
54. Processing information in this way is not CSE's only option. CSE could, for example, maintain its current approach to processing collected data into traffic items as the default, but incorporate an exceptional process that converts that derivative information into traffic items when some contents are of value but others raise compliance concerns. These derivative items could replace the original traffic item, allowing retention or deletion decisions to occur at a more granular level.

Recommendation 3. NSIRA recommends that CSE establish a process for the handling of traffic items that contain both information with foreign intelligence value and information that must be deleted.

Issues in SIGINT Policy and Practice

Intelligence Analysts and Targeting Decisions

Finding 6. NSIRA found that CSE intelligence analysts do not consistently stop targeting [REDACTED] that are no longer of foreign intelligence interest.

55. Intelligence analysts play a fundamental role in SIGINT data retention: they identify selectors for collection, assess the collected data, and make decisions affecting its retention. Intelligence analysts, for example, are responsible for applying annotations and reporting compliance incidents relating to IRTC, with impacts on retention. The business needs of intelligence analysts also influence CSE's policy

15(1)(d)
15(1)(f)

TOP SECRET // SI // CEO

decisions related to retention, as well as the priorities for technical teams designing tools used for retention.

56. Intelligence analysts use multiple tools and interact with several SIGINT systems within CSE's ecosystem, which are updated on an ongoing basis. In addition, the functionality of these tools is not always fully documented, and training can be at times more informal than formal.
57. In two inspections, two different intelligence analysts assumed that marking [REDACTED] as being of no FI interest in one system would automatically prevent any future collection [REDACTED] in all systems. However, this was not the case and [REDACTED] remained actively targeted in CSE's targeting tool. Both incidents occurred within the span of a year and a half. While this violated CSE's targeting policies, technical and procedural safeguards prevented CSE from collecting further content from [REDACTED]. None of these selectors appeared to be related to Canadians or persons in Canada.
58. When asked if CSE had made any adjustments to its training program for analysts, CSE stated that they could not speak to the practices in each team. They did, however, modify communications to staff to remind analysts that, after using the feature to mark [REDACTED] as being of no FI interest, they must also separately update the targeting tool to stop targeting [REDACTED].

Recommendation 4. NSIRA recommends that CSE develop mechanisms and staff training to ensure that it stops targeting [REDACTED] when intelligence analysts determine that [REDACTED] is no longer of foreign intelligence interest.

[REDACTED] Retention of [REDACTED] Information

Finding 7. NSIRA found that CSE sought and received authorization from the Minister to retain [REDACTED] information [REDACTED] despite not having plans to implement [REDACTED] retention capability for that information.

Finding 8. NSIRA found that CSE's policy for [REDACTED] retention of [REDACTED] information did not include a requirement to periodically assess the information for foreign intelligence value.

59. [REDACTED] information encompass a wide range of identifying information that may be associated with a CSE target. Examples include [REDACTED]
[REDACTED]
[REDACTED] In CSE's view, this information can reveal insights into a legitimate target that may be crucial to its mandate.

15(1)(d)

15(1)(f)

TOP SECRET // SI // CEO

60. In 2020, CSE first included [REDACTED] information as separate information types in its retention schedule. [REDACTED] information were initially assessed as requiring a retention period of [REDACTED]
61. The following year, CSE increased the retention period for [REDACTED] [REDACTED] information to be [REDACTED]
62. This change was authorized based on language that was introduced in CSE's applications for FIA in 2021, which makes the case that [REDACTED] information are uniquely valuable to CSE over time. Specifically, the application sought to obtain the Minister's "approval to extend the retention period of this information from [REDACTED] as long as the information is assessed to have foreign intelligence value". The latter sentence was repeated in subsequent applications in the following form: "For these reasons, CSE may retain this information [REDACTED] as long as it is assessed to have foreign intelligence value." This language is repeated in the Minister's authorizations. The use of "as long as the information is assessed..." implies a requirement to periodically reassess the information for its FI value.
63. However, in response to NSIRA requests for information, CSE described the [REDACTED] retention of this information as having "no requirement to review [...] whether or not the data is still useful". This means that if [REDACTED] information was assessed as having FI value at one point in time, it could be retained [REDACTED] Other than the retention schedule itself, no information was included in the FIA application that would indicate that the Minister was apprised of CSE's interpretation that no review was required. The omission of this requirement in the retention schedule is inconsistent with the "as long as the information is assessed..." language included in the FIA.
64. While this [REDACTED] retention has been authorized since 2021, CSE stated to NSIRA that it was not using this retention authority. When asked how it has put into practice the [REDACTED] retention of [REDACTED] information, CSE stated that it "does not employ automated means to identify this type of information" and that "intelligence analysts may identify this type of information manually". However, CSE also stated that it does not currently have a policy or technical means to enable analysts to recognize information as [REDACTED] [REDACTED] information and change its retention period. Any efforts to implement such technical means remained in very early stages as of late 2024, years since this authority was first requested.
65. This calls into question the necessity of including it in the FIA. FIA applications are a key conduit for CSE to inform the Minister of its activities. They are the record the

15(1)(f)

TOP SECRET // SI // CEO

Minister uses to determine whether to issue an FIA, including any conditions they see fit. Without precision in its FIA applications, it is unclear whether what the Minister authorizes will actually be put into effect. CSE could improve its accountability to the Minister by ensuring its application for this authority reflects the reality of its practices. CSE risks diminishing this accountability if it repeatedly requests authorization to conduct activities it does not intend to carry out.

66. One of the conditions for authorizations under section 34 of the CSE Act is that the Minister have reasonable grounds to believe that the information acquired under the authorization will be retained for no longer than is reasonably necessary. NSIRA considers that, to meet that condition, CSE must have some means to ensure, on an ongoing basis, the necessity of continuing to retain specific [REDACTED] information.

Recommendation 5. NSIRA recommends that CSE ensure the information concerning retention of [REDACTED] information in its applications for foreign intelligence authorizations reflects its actual retention practices. If CSE chooses to retain such information [REDACTED] it must establish a mechanism to ensure it is retained for no longer than reasonably necessary.

SIGINT Data Stored in Peripheral Systems

Finding 9. NSIRA found that CSE stores SIGINT data in systems and tools not subject to CSE's automated deletion processes. This requires the manual deletion of data, which introduces compliance risks.

67. The MPS FI requires SIGINT systems to follow data stewardship principles. These are meant to ensure that the same governance requirements follow data when it is transferred between systems and individual analysts.
68. Most of CSE's main SIGINT systems employ automated means to ensure that data is handled according to these principles. While CSE demonstrated strong practices for deletion within its core collection, processing, and analytical systems, it acknowledged the risk that data that analysts remove from these systems is not subject to automatic oversight.
69. For example, analysts can download queried SIGINT data to their workstation to conduct further analysis. This contributes, with some regularity, to compliance incidents where analysts or teams discover local copies of data that are past their retention limits. While deleted from the core, automated systems, there is no mechanism to automatically delete these local copies of data once past the retention limit; their identification and deletion relies on manual intervention.

TOP SECRET // SI // CEO

70. More generally, SIGINT data is at times handled or stored in systems which are not built to adhere to CSE's data governance framework. These peripheral systems include tools that CSE uses to manage projects and process workflows, communicate internally and with partner agencies, and collaborate on or share knowledge about projects, operations, tools, and processes.
71. This is understandable, to a point: it is natural for analysts to, in the course of their work, require local copies of data to develop and apply novel analytical tools or practices; indeed, doing so contributes to the innovation that makes SIGINT possible. Nonetheless, CSE and individual analysts are responsible for the data they handle, to ensure it is managed according to CSE's data stewardship principles.
72. Given this, CSE has implemented certain practices to mitigate the risk that data is stored outside systems subject to automated deletion ("managed systems"):
 - CSE continues to develop a more expansive analytical toolkit within managed systems, enabling analysts to do more of their work without making local copies of data.
 - When analysts do attempt to download data from managed systems, certain systems warn analysts of their responsibility for the proper handling and timely deletion of their local copies.
73. However, CSE's MPS FI says very little on any specific requirement or data handling practices that analysts must follow when handling data outside of managed systems. It states that "retention schedules must be applied to all SIGINT data regardless of media or location". This requirement, however, is discussed in a section on "SIGINT systems", creating ambiguity as to which requirements to follow if analysts are working outside SIGINT systems.
74. Throughout this review, NSIRA has sought to understand what CSE staff consider to be SIGINT data and whether principles are shared and understood across the different teams involved in the production of SIGINT.
75. NSIRA has observed selectors and identifiers being shared over email with CSE's counterparts, and the use of SIGINT data in CSE's project management platform. In all cases, there were legitimate reasons for data to be manipulated in these peripheral systems. However, these did not follow CSE's data governance framework, they did not employ automated means of processing data, and CSE staff, due to the ambiguities noted above, may not always have been aware of the requirement to ensure that data stored in these systems was deleted according to its retention allowance.

TOP SECRET // SI // CEO

76. This practice may extend to CSE's use of FVEY collaborative tools. CSE itself appears to have little insight into the full extent of its staff's use of such tools. When asked about CSE's auditing practices in place for those tools, CSE stated that it "cannot audit them", but believed them to be audited by the FVEY partner, and expected to collaborate with their FVEY partner to audit any incidents if necessary.
77. These peripheral systems serve an important function: given the speed at which technology and SIGINT practices evolve, CSE staff must remain agile in their use of collected data and in their internal and external collaboration. However, the retention of data in peripheral systems can and does introduce compliance risks. CSE should ensure that its policies account for the handling and retention of SIGINT data in all environments.

Recommendation 6. NSIRA recommends that CSE update the Mission Policy Suite to eliminate ambiguity about SIGINT data stored in peripheral systems, and provide direction on how to ensure compliance with retention requirements.

Sharing SIGINT Tools and Data with Five Eyes Partners

Finding 10. NSIRA found that CSE's sharing of SIGINT data with other agencies, such as Five Eyes partners, limits its ability to directly ensure data is retained according to CSE policies.

78. The Five Eyes (FVEY) partnership has enabled significant advances in the development of technologies that are crucial for the production of SIGINT. As noted, CSE's systems are complex and distributed among different teams responsible for the production of SIGINT. Some of the systems CSE uses, from the collection of data to its retention, originate from its FVEY partners or from a collaboration between them.
79. The strong integration among FVEY members has enabled CSE to use tools that would otherwise be difficult, if not impossible, to create independently, and CSE benefits from being able to access FVEY technical expertise and software development professionals. However, this integration also has a direct effect on CSE's ability to meet its policy requirements when it comes to the retention of SIGINT data. CSE noted it must separately develop and maintain certain features [REDACTED] developed primarily by a FVEY partner, to ensure compliance with Canadian retention requirements.
- 15(1)(d)
15(1)(f) 80. The partnership also has strong information sharing and operational integration components. CSE may [REDACTED] directly from FVEY partner agencies, which are subject to the same criteria as those imposed on

15(1)(d)
15(1)(f)

TOP SECRET // SI // CEO

CSE's intelligence analysts. Some [REDACTED] SIGINT data may also be shared [REDACTED] with CSE's FVEY partners upon its collection. This review did not assess these [REDACTED] sharing practices in-depth. It did, however, examine some of the retention implications of sharing SIGINT data.

81. When shared through automated means, CSE stated that CSE-collected SIGINT data is accompanied by its CSE-created identifiers, which follow a common format within the FVEY partners and include scheduled deletion dates. Furthermore, it stated its understanding that when partners receive CSE data, the shorter of either CSE's or the partner's retention period is applied to the data in the partner's systems. While these identifiers do enable partners to delete shared data according to CSE's retention schedule, creating multiple copies of data outside of CSE's own systems inherently diminishes CSE's control over that data's retention.
82. This automatic sharing complicates the purging of non-compliant traffic items, such as data acquired from the inadvertent targeting of a Canadian, as CSE must request that their counterpart who received the information also initiate a purge of the information in their systems. While CSE may receive a confirmation from the partner that the purge was conducted – and NSIRA did see evidence of this in the course of its review – CSE cannot be certain of the complete destruction of the information, as it does not have visibility into their partners' systems.
83. More recently, CSE has introduced a new mechanism for sharing some of its collected data ("query-in-place"). The mechanism allows FVEY analysts to retrieve data from CSE's holdings, with a justification. It enables CSE to track and monitor who accesses and retrieves data to ensure that their access to information was compliant with CSE's policies. This does not entirely eliminate the issues noted above: if CSE later deemed certain data had to be purged, it would still have to request the partner agency purge the data itself. Compared to automatic sharing, which CSE continues to do for some data, it does reduce the volume of data being shared, thus potentially reducing the likelihood of issues arising.

4. Conclusion

84. Given the varied operational needs of SIGINT collection—which can be difficult to predict in advance, and change over time—CSE requires data to carry out its mission, while being subject to important constraints on its retention of collected data. CSE's commitment to respecting data retention requirements was evident in this review, especially in its handling and protection of IRTC.

TOP SECRET // SI // CEO

85. While this commitment is real and notable, CSE had certain shortcomings related to its retention of SIGINT data, as detailed in this report. Most significantly, CSE lacks mechanisms to delete certain non-Canadian information without FI value. Through its inspections, NSIRA found that CSE retained collected non-Canadian information that it had determined to not be of FI value. Doing so may not be in compliance with the terms and conditions of its *Foreign Intelligence Authorization for Network Operations*. More generally, the lack of such mechanisms may cause CSE to retain such information for longer than reasonably necessary.
86. CSE must continue to prioritize data retention in the design and implementation of its policies, processes, systems, and staff training. The CSE Act requires that SIGINT data be retained for no longer than reasonably necessary. This must be reflected throughout CSE's operations, in both principle and practice.

15(1)(d)
15(1)(f)

TOP SECRET // SI // CEO

Annex A. SIGINT Data Retention Schedule

The MPS FI includes the following data retention schedule.

Type	Retention	Comments
If the content of selected information has a recognized Canadian privacy interest, and is assessed as essential to international affairs, defence, security, including cybersecurity, then:		
[REDACTED] [REDACTED] [REDACTED] [REDACTED]	[REDACTED] [REDACTED] [REDACTED]	Upon recognition, analysts must apply privacy annotations, as required, and retain any material that has been used in end products in secure containers. Retention of solicitor-client communications requires Ministerial approval.
If the content of selected information has a recognized Canadian privacy interest, and is assessed as non-essential to international affairs, defence, security, including cybersecurity, then:		
[REDACTED] [REDACTED]	[REDACTED] [REDACTED]	Upon recognition in content databases, analysts must apply privacy annotations, as required, for deletion of the material; content will automatically be deleted from the content databases after [REDACTED]
If the content of the selected information is recognized as a [REDACTED] Canadian, then:		
[REDACTED] [REDACTED]	No retention permitted	Upon recognition, analysts must mark these communications for deletion, and the Data Assurance team must be notified so they can review the relevant selectors and purge data.
For all other data, and communications with no Canadian privacy interest:		
[REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]	[REDACTED]	N/A
[REDACTED] [REDACTED] [REDACTED] [REDACTED]	[REDACTED]	N/A
[REDACTED] [REDACTED]	[REDACTED] [REDACTED]	N/A

[REDACTED] [REDACTED]		
[REDACTED] [REDACTED] [REDACTED] [REDACTED]	[REDACTED]	
Cipher Decrypt	[REDACTED]	Once the information is accessible, standard retention schedules apply.
[REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]	[REDACTED]	Information can be retained [REDACTED] for [REDACTED]. The owner of the information should conduct periodic revalidation of the need for retention. If the information is deciphered and assessed after the initial [REDACTED] retention limit, the following applies: - Assessed as FI based on current priorities and marked for use and retention - Assessed as no FI value and marked for deletion unless otherwise authorized.
[REDACTED] [REDACTED]	[REDACTED]	[REDACTED] information, such as [REDACTED] can be retained [REDACTED]
[REDACTED] [REDACTED]	[REDACTED]	[REDACTED] data such as [REDACTED] can be retained [REDACTED]. This includes [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]
[REDACTED] [REDACTED]	[REDACTED] [REDACTED]	Information will be retained for a period of no more than [REDACTED] from the date on which the information was first acquired. Following that [REDACTED] period, the information will be automatically deleted unless [REDACTED] is deemed to be of foreign intelligence interest.
[REDACTED] [REDACTED]	[REDACTED] [REDACTED]	This consists of unselected information acquired for the purpose of creating and [REDACTED]. Information will be retained for a period of no more than [REDACTED] from the date on which the information was first acquired. Ministerial approval is required to retain this information for longer than [REDACTED].

15(1)(d)
15(1)(f)

TOP SECRET // SI // CEO

Annex B. Technical Inspection Summaries

NSIRA identified the 4 datasets for its technical inspections by:

- Requesting a list of [REDACTED] datasets collected via [REDACTED] enabled by a particular [REDACTED] capability.
- Receiving a list of 321 datasets. The list included details about each dataset's [REDACTED]
[REDACTED]
[REDACTED]
- Filtering the list of datasets based on a number of criteria, such as the likelihood of IRTC and the novelty of the data. To verify CSE's description of the purge process, NSIRA included a purged dataset in this filtered list.

Each of the four inspections enabled NSIRA to observe unique dimensions of the SIGINT collection and retention chain:

1. Inspection 1 reviewed [REDACTED] dataset that a [REDACTED] analyst targeted and assessed [REDACTED] The target was found through [REDACTED] using CSE and FVEY partner tools. They assessed the collected SIGINT data and determined that the [REDACTED] did not belong to the intended target. The information thus had no foreign intelligence (FI) value, so they marked [REDACTED] as being not of FI interest in CSE's [REDACTED] tool to prevent other analysts from targeting it. The data, collected in [REDACTED] remained in CSE's holdings as of the September 2024 inspection, and is not scheduled for deletion until its [REDACTED] age-off date.
2. Inspection 2 reviewed [REDACTED] dataset that a CSE [REDACTED] analyst targeted and assessed [REDACTED] The analyst identified the target based on [REDACTED] They assessed the collected SIGINT data and noted that [REDACTED] They did not find any other indicators of Canadian ties. While seeking these indicators, they also assessed that the information had no FI value. Since there was no FI value in the information, the analyst, upon consultation with CSE's compliance team, labelled the [REDACTED] as having a Canadian privacy interest "out of an abundance of caution". This initiated a purge process. The data, collected in February 2024, was purged from the system a few days later in [REDACTED] which NSIRA confirmed in the September 2024 inspection.
3. Inspection 3 reviewed [REDACTED] dataset that a CSE [REDACTED] analyst targeted and assessed [REDACTED] The analyst identified

15(1)(d)
15(1)(f)

TOP SECRET // SI // CEO

the target based on [REDACTED]. They assessed the collected SIGINT data and confirmed they were in the desired target set; the information had FI value. They retargeted [REDACTED] several times to collect additional information of FI value. The data, collected between [REDACTED] [REDACTED] remained in CSE's holdings as of the October 2024 inspection, and is not scheduled for deletion until its [REDACTED] age-off dates. [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

4. Inspection 4 reviewed [REDACTED] dataset that the same CSE [REDACTED] analyst from inspection 2 had targeted and assessed [REDACTED]. They identified the target using the same criteria as they did the target for inspection 2. They assessed the collected SIGINT data and determined that [REDACTED] did not belong to the intended target. The information thus had no FI value, just as with inspection 2. Unlike inspection 2, however, there were no indicators of Canadian ties, so the analyst could not delete or purge the data; they instead marked [REDACTED] as being not of FI interest in CSE's [REDACTED] tool to prevent future targeting, as with inspection 1. The data, collected in [REDACTED] remained in CSE's holdings as of the October 2024 inspection, and is not scheduled for deletion until its [REDACTED] age-off date.

While preparing for the first two inspections, CSE identified a compliance incident for each:

1. In inspection 1, the intelligence analyst assumed that marking [REDACTED] as being not of FI interest in one system would automatically de-target it in all systems. However, this was not the case and [REDACTED] remained marked as targeted in CSE's targeting tool. While this violated CSE's targeting policies, several technical and procedural safeguards prevented CSE from collecting further content [REDACTED]—as with [REDACTED] that is marked in this way. To remedy the issue, CSE detargeted [REDACTED] from all systems.
2. In inspection 2, a small number of empty transmissions were received from [REDACTED] after the purge request was initiated. These transmissions originated from CSE's [REDACTED]—they did not have any information in them, so they did not contain data from [REDACTED]. Due to a procedural oversight, CSE data assurance analysts only purged data received up to the last known collection date. These transmissions were received after that date, so they were not purged. This data remained in the system until CSE prepared for the inspection, at which point CSE initiated an incident and purged the data in September 2024.

TOP SECRET // SI // CEO

During the inspections, CSE shared incident details, including how they addressed the issues and steps they had taken or were considering taking to prevent similar incidents in the future.

TOP SECRET // SI // CEO

Annex C. Findings and Recommendations

NSIRA made the following findings and recommendations in this review:

Handling of Canadian Information

Finding 1. NSIRA found that CSE implemented safeguards to protect the privacy of Canadians and persons in Canada within SIGINT data retention systems, tools, and capabilities.

Information with No Foreign Intelligence Value

Finding 2. NSIRA found that CSE's foreign intelligence retention schedule does not account for non-Canadian information with no foreign intelligence value.

Finding 3. NSIRA found that CSE lacks institutional mechanisms to delete certain non-Canadian information with no foreign intelligence value, posing a risk that CSE retains such information for longer than reasonably necessary.

Finding 4. NSIRA found that CSE retained collected non-Canadian information despite having determined that the information had no foreign intelligence value. This may not be in compliance with the terms and conditions of the *Foreign Intelligence Authorization for Network Operations* issued under section 26 of the CSE Act.

Recommendation 1. NSIRA recommends that CSE immediately delete the data determined to have no foreign intelligence value identified in inspections 1 and 4, as retaining this data is not reasonably necessary.

Recommendation 2. NSIRA recommends that CSE amend the Mission Policy Suite to create a category for non-Canadian information determined to have no foreign intelligence value, and set a timeline for its deletion that ensures it is retained for no longer than reasonably necessary.

Finding 5. NSIRA found that CSE's chosen approach to processing SIGINT data into "traffic items", by which multiple individual communications are sometimes grouped into a single item, may lead to retention of information with no foreign intelligence value.

Recommendation 3. NSIRA recommends that CSE establish a process for the handling of traffic items that contain both information with foreign intelligence value and information that must be deleted.

15(1)(d)
15(1)(f)

TOP SECRET // SI // CEO

Issues in SIGINT Policy and Practice

Intelligence Analysts and Targeting Decisions

Finding 6. NSIRA found that CSE intelligence analysts do not consistently stop targeting [REDACTED] that are no longer of foreign intelligence interest.

Recommendation 4. NSIRA recommends that CSE develop mechanisms and staff training to ensure that it stops targeting [REDACTED] when intelligence analysts determine that [REDACTED] is no longer of foreign intelligence interest.

[REDACTED] Retention of [REDACTED] Information

Finding 7. NSIRA found that CSE sought and received authorization from the Minister to retain [REDACTED] information [REDACTED], despite not having plans to implement an [REDACTED] retention capability for that information.

Finding 8. NSIRA found that CSE's policy for [REDACTED] retention of [REDACTED] [REDACTED] information did not include a requirement to periodically assess the information for foreign intelligence value.

Recommendation 5. NSIRA recommends that CSE ensure the information concerning retention of [REDACTED] information in its applications for foreign intelligence authorizations reflects its actual retention practices. If CSE chooses to retain such information [REDACTED] it must establish a mechanism to ensure it is retained for no longer than reasonably necessary.

SIGINT Data Stored in Peripheral Systems

Finding 9. NSIRA found that CSE stores SIGINT data in systems and tools not subject to CSE's automated deletion processes. This requires the manual deletion of data, which introduces compliance risks.

Recommendation 6. NSIRA recommends that CSE update the Mission Policy Suite to eliminate ambiguity about SIGINT data stored in peripheral systems, and provide direction on how to ensure compliance with retention requirements.

Sharing SIGINT Tools and Data with Five Eyes Partners

Finding 10. NSIRA found that CSE's sharing of SIGINT data with other agencies, such as Five Eyes partners, limits its ability to directly ensure data is retained according to CSE policies.