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

TECHNICAL ASSURANCE REVIEW
FORM E – ASSESSMENT OUTCOME

Review of CSE's Deletion of Data from Select [redacted] Partners

Department	Communications Security Establishment (CSE)
File Number	25-11
Notification Date	September 4, 2025
Assessment Date	November 6, 2025
Report Date	December 10, 2025
Assurance Rating	Medium

In this review, the National Security and Intelligence Review Agency (NSIRA) examined elements of the Communications Security Establishment's (CSE) process for deleting signals intelligence (SIGINT) data pursuant to a deletion request. This review considered a sample of data received [partners] [redacted] and confirmed that the data was deleted. However, while conducting the assessment, CSE proactively informed NSIRA that data subject to one deletion request remained on the system. NSIRA assigned a medium assurance rating to the effectiveness of the deletion process.

Authority

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

Background

In March 2025, NSIRA was notified by CSE of a SIGINT compliance incident where datasets were shared with [redacted] intelligence partners. Consequently, CSE submitted a request to each partner to purge the information in each dataset. NSIRA sought to understand how CSE handles these types of deletion requests when requested by its intelligence partners.

The information collected by CSE or shared with CSE is handled, processed and stored in systems which are subject to data governance requirements. One such requirement is the ability for any system that stores SIGINT data for more than [redacted] to process deletion requests. CSE and its [redacted] intelligence partners may exchange data or enable the collection of information for each other.

When exchanging data, if one agency has shared data that it later determines should be deleted, pursuant to its own requirements, it is standard practice for this agency to send a deletion request to any partner with whom it shared the data. That partner is then expected to delete the data and confirm its deletion.

When one agency collects data on behalf of another, it is standard practice for the requesting agency to respect the partner's policies. In these cases, the requesting agency will delete the affected data and confirm its deletion with the partner.

Objective and Scope

The objective of this review was to assess instances of CSE's deletion of SIGINT information received from an international partner.

The original scope was to assess select [redacted] intelligence partners' deletion requests from January 1, 2023 to August 31, 2025. However, CSE informed NSIRA that no such requests existed in their holdings during this timeframe. Accordingly, NSIRA decided to assess deletion requests from [redacted] partners instead.

This review did not examine any downstream processing, transformation, or use of the [redacted] partner information. Further, this review was not a comprehensive assessment of the entire deletion process and did not seek to assess the deletion process for all requests or systems. NSIRA assessed the deletion process in two of CSE's most widely used SIGINT systems by randomly selecting one traffic item per request to confirm its deletion. A traffic item is a fundamental unit of SIGINT content data within CSE systems. It is an 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] Traffic items have unique CSE assigned identification numbers associated to them.

Methodology

NSIRA requested that CSE provide a list of all deletion requests related to data received or collected from a [redacted] partner between July 1st and August 31st, 2025. Out of the list [#] deletion requests received, NSIRA selected three for review:

[redacted]

NSIRA requested all the information associated with these deletion requests, including information on their associated traffic items, communications with [redacted] partner, system logs and artifacts generated by the deletion process. All three of the deletion requests related to a period of time when a [redacted] CSE's technical process for data deletion is the same irrespective of if the data originates from the partner directly (through exchange) or collected by a partner on their behalf. These were not deletion requests that were received by [redacted] partner, rather, they were initiated by CSE to comply with partner [redacted] NSIRA selected two of CSE's main SIGINT systems [redacted] to verify deletion.

CSE found no traffic items in its systems when the [partner] request was processed, and, as such, there was no data to delete. Accordingly, NSIRA only reviewed the documentation related to this request. NSIRA randomly selected one traffic item associated with each of the remaining deletion requests to review its deletion in the selected systems.

NSIRA convened an assessment session with CSE personnel who held the necessary system accesses to verify the deletion of the traffic items in the identified systems. Before the session, NSIRA provided CSE the identification numbers of the randomly selected traffic items.

During the assessment, for each system observed, CSE staff opened the selected system and confirmed it was functioning correctly. CSE staff then queried each of the NSIRA-provided traffic items to confirm their deletion from the systems.

Finally, CSE queried its deletion system [redacted] database for each of the deletion requests and exported the resulting logs. The logs confirm that data associated with these deletion requests was tasked to be deleted.

Findings

Finding 1. NSIRA found that CSE had deleted the data from the selected deletion requests by the time of NSIRA's assessment.

During the assessment, NSIRA observed that both of CSE's systems [redacted] were functioning as expected. Further, for each deletion request, NSIRA observed that the selected traffic items were no longer present in the systems.

Finding 2. NSIRA found that, despite Finding 1, one system did not respond to either automatic deletion request; CSE manually deleted the data in that system.

After independently reviewing the logs retrieved from CSE's deletion system [redacted] NSIRA can confirm that the [redacted] deleted traffic items at the time the request was initiated in [redacted]. [redacted], however, according to [redacted] had not responded to the request in either case. CSE analysts indicated that they manually deleted traffic from [redacted] – several weeks after the requests had been initiated.

The timelines for deleting the respective data with the two requests can be summarized as follows:

SIGINT Compliance Notified	[redacted]
Deletion Request Initiated	
Automatic Deletion Process	
Deletion of [redacted] Data	
Partner Notified of Deletion	
NSIRA Verification Date	

Finding 3. NSIRA was notified by CSE that one traffic item that should have been deleted had erroneously not been deleted.

Prior to the assessment, CSE proactively disclosed to NSIRA that it had discovered a remaining traffic item and subsequently deleted it. NSIRA did not examine this issue further as it was not one of its selected samples. NSIRA notes that this topic may be the subject of future review as the observed instances of manual deletion raise concerns with the process of traffic item deletion.

Overall Assurance Rating

Undetermined	Low Assurance	Medium Assurance	High Assurance	Very High Assurance
		^		

NSIRA is assigning a **Medium Assurance** rating for this assessment, based on the following factors:

Factor 1. Access Limitations

For CSE to achieve a very high assurance rating, NSIRA would need direct access to CSE's systems and data.

Factor 2. Incomplete Deletion of Data Following the Automatic Process

As detailed in Findings 2 and 3, traffic items that were expected to be deleted were not deleted following the automatic deletion process. CSE had not deleted these traffic items until four days after NSIRA requested the list of deletion requests, despite these requests having been outstanding for several weeks. While there is no timeline in policy for deleting [redacted] partner traffic items, this incomplete deletion raises concerns about the reliability and timeliness of the deletion process.

Factor 3. Level of Detail in Deletion Logs

The logs from CSE's deletion system [redacted] describe which traffic items were queued for deletion and how many items each system deleted. There are no logs available, through [redacted] or otherwise, to confirm when a specific traffic item was deleted. This limits NSIRA's ability to confirm that the traffic items in question were deleted at the time the tickets were processed – NSIRA can only confirm that the traffic items no longer existed by the time of the assessment session.

Conclusion

While the traffic items selected for verification had been deleted, the incomplete initial deletion following an automatic process indicates that CSE can improve its deletion process. More broadly, NSIRA notes that the reliability of the deletion process is particularly crucial as the same process is used to delete data that could relate to Canadians. While CSE noted that it assigns a higher priority to Canadian data, this was not examined in this review. In the future, NSIRA may use the established process of this review to conduct assessments on data that relates to Canadians or other international partners.