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

May 31, 2021

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

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

Importance of independent external review

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

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

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

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

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

Canadian Identifying Information and CSE's Commitment to Privacy

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

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

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

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

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

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

Review Recommendations

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

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

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

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

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

Review Findings

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

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

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

Referral to Attorney General of Canada

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

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

Additional Information

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

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