Canadian Security Intelligence Service | Service canadien du renseignement de sécurité

FEBRUARY 2024
UNCLASSIFIED

AVOIDING COMPLICITY IN MISTREATMENT BY FOREIGN ENTITIES ACT

Annual Report to the Minister of Public Safety

A safe, secure and prosperous Canada through trusted intelligence, advice and action.
Des renseignements, des conseils et des interventions fiables pour un Canada sûr et prospère.

Canada

Table of Contents

Introduction

1. Exchanging information with foreign agencies is an integral part of the Service's mandate, and is a crucial component of Canada's ability to effectively investigate, assess, and counter threats to Canada and its interests. Many of the national security challenges facing Canada originate from or have a strong nexus to events, foreign governments, individuals and groups overseas. In order to fulfil its mission to protect Canada from threats to our national security in this context, CSIS relies on timely information sharing with foreign partners.

2. CSIS recognizes the need to share information in accordance with Canadian values, the rule of law, the Canadian Charter of Rights and Freedoms, and international legal obligations. These obligations are captured in the July 2019 Avoiding Complicity in Mistreatment by Foreign Entities (ACMFE) Act, which recognizes that foreign information sharing is "fundamental to the Government of Canada's national security requirements." The act requires that exchanges between Canadian federal government departments and agencies and our foreign counterparts do not result in a "substantial risk" of mistreatment against individuals.

3. The ACMFE Act requires the Governor-in-Council to issue directions to certain Deputy Heads of federal government departments and agencies that conduct information sharing activities with foreign entities. The related Order-in-Council (OiC) issued to the Director of CSIS in September 2019, outlines the Service's responsibilities when disclosing, requesting, or using information from foreign entities and is consistent with requirements outlined in the prior 2017 Ministerial Direction (MD) on ACMFE. The Act requires Deputy Heads to whom directions have been issued to submit to the appropriate Minister a report on the implementation of those directions during the previous calendar year. This report outlines the key components of the Service's implementation of the ACMFE Act and related OiC during the 2023 calendar year reporting period.

CSIS Foreign Information Sharing and Human Rights

4. CSIS has more than 300 foreign relationships in over 150 countries, each authorized by the Minister of Public Safety after consultation with the Minister of Foreign Affairs, in accordance with s.17(1)(b) of the *CSIS Act*. The process to establish new arrangements with foreign agencies is stringent and takes into consideration a wide range of issues, including Canadian security requirements, as well as the reliability of the foreign agency and its human rights track record. Prior to seeking the Minister's approval for new arrangements, CSIS proactively consults with Global Affairs Canada (GAC) on such initiatives in instances where there are specific human rights or foreign policy considerations.

5. As has been the case since its inception in 1984, CSIS regularly assesses all of its arrangements with foreign entities, including human rights considerations. As part of this, CSIS summarizes key human rights considerations based on a range of classified and open source material, including CSIS reporting, GAC country human rights profiles, and unclassified US State Department Country Reports. CSIS also reviews relevant and credible open-source reporting from established non-governmental entities such as Amnesty International and Human Rights Watch for all countries where the Service has implemented arrangements. This includes a review

of the human rights environment of each country's security community, and more specifically the human rights reputations of the foreign agencies with which the Service has established such arrangements.

6. CSIS implemented a revised human rights assessment methodology in 2023, which includes updated indicators with an associated numerical rating system and a more consistent and objective review process. CSIS continues to review the methodology to ensure rigour and quality.

7. Information sharing with foreign partners is carefully considered and documented by the Service on a case-by-case basis. All exchanges are assessed against the threshold of whether there is a substantial risk of mistreatment to an individual if CSIS information is shared with a foreign partner, and whether that risk can be mitigated through a variety of potential measures (see below). As required in the *ACMFE Act* and related OiC, if a substantial risk of mistreatment cannot be mitigated, the information is not shared. In cases where CSIS engages in information exchanges with foreign agencies where human rights concerns exist, the Service takes an incremental approach, in order to gauge the reliability of the agency and the usefulness of such an arrangement. Such exchanges are also commensurate with the degree of trust established over a period of time and reflective of the human rights climate within the country in question.

CSIS Foreign Agency Restrictions Mechanism

8. Prior to the 2017 Ministerial Direction (MD), the Service on a case-by-case basis suspended its engagement with foreign entities where serious human rights issues arose. The 2017 MD on ACMFE required the Service to impose "restrictions" on information sharing if it was assessed that a foreign entity was engaging in, or contributing to, mistreatment. Restrictions are imposed on the foreign information sharing approval process due to serious human rights allegations levelled against the partner or the country's broader security community. This does not mean no sharing of any information; rather, a higher level of approval is required for information sharing to take place. In 2018, CSIS assessed all of the entities in countries rated as "High" on the Service's Human Rights Country Risk Ratings and then assigned appropriate levels of restriction to the bulk of the affected agencies. With the introduction of CSIS' new Foreign Information Sharing Framework in January 2021, the three levels of restriction were collapsed into one overarching set of foreign information procedures, resulting in two categories: "suspended" or "restricted." Currently, over 75 foreign entities are subject to restrictions.

9. Notable changes during the period under review include the removal of restrictions from one foreign partner. The Service increased the human rights risk rating for one s.17 partner country from "Medium" to "High" because of a deterioration in the country's human rights environment due to armed conflict. The Service decreased the human rights risk rating for one s.17 partner country from "Medium" to "Low" and for another country from "High" to "Medium" due to an amelioration in their respective human rights environment over the past several years.

Mitigation Measures

10. When it is assessed that a proposed disclosure to a foreign partner would give rise to a substantial risk of mistreatment, CSIS can consider a range of measures to mitigate the risk of mistreatment below the “substantial” threshold. Mitigation efforts can include obtaining updated human rights assurances from a foreign agency, placing caveats on information shared with a foreign agency, and using a redacted version of the information (e.g. a Form of Words).

11. In 2023, the Service continued a process of seeking human rights assurances from foreign agencies regarding their use of CSIS information, a practice which began in 2009. Human rights assurances are sought to ensure that the foreign agency understands and abides by CSIS expectations (and those of the broader Government of Canada (GC)) regarding the use of information provided by CSIS vis-à-vis human rights, including the treatment of detainees. These assurances outline expectations to foreign agencies that individuals will not be mistreated in any way as a result of CSIS information exchanges with the foreign agency, and that individuals will be treated in a manner consistent with domestic and international law, including the *United Nations Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment.*

12. CSIS also applies appropriate human rights caveats on case-specific information shared with foreign partners. These caveats provide clear expectations with regard to human rights vis-à-vis the specific information being exchanged. In brief, the caveats state that the Service expects the recipient foreign agency will respect and adhere to human rights requirements and international law. Separate caveats on “3rd-Party Rule” expectations regarding dissemination of information are also included to ensure the recipient foreign agency is not disseminating CSIS information to 3rd parties without prior consent.

13. Caveats and assurances are among the key measures considered by CSIS to mitigate risks of mistreatment stemming from information sharing with foreign entities. CSIS tracks the receipt of assurances received for each individual foreign agency, as well as instances where CSIS may suspect that a foreign agency may not have adhered to such assurances or violated caveats. In instances where CSIS suspects non-compliance by a foreign agency to such caveats or assurances, CSIS raises the issue with the affected entity. While violations of CSIS caveats or assurances provided by a foreign entity are very difficult to confirm or corroborate, the Service does seek updated assurances from foreign entities in instances where uncorroborated reporting may indicate concerns with potential human rights issues, or potential complicity in such violations by the affected foreign agency.

14. For foreign entities that are restricted, CSIS approaches like-minded allies to compile their experience and feedback about the local practices when sharing information with the entities in question, including their human rights practices broadly and as it relates to information sharing. This feedback assists the Service in making its own assessment about the likelihood of mistreatment by a restricted partner.

Collaboration with Other Government Departments

15. CSIS continued to be involved in Information Sharing Coordination Group (ISCG) discussions and other interdepartmental initiatives to understand respective frameworks in the spirit of the recommendations from NSIRA's 2021 *Avoiding Complicity in Mistreatment by Foreign Entities Act (ACA)* review.

16. The ISCG, chaired by Public Safety Canada, is the primary interdepartmental forum for supporting interdepartmental collaboration and information-sharing between the departments and agencies that received, or were considered for receipt of, Governor-in-Council Directions. The ISCG was convened on multiple occasions in 2023, continuing discussions on the implementation of the Act, associated directions, reporting requirements, methodologies, and responses to external review body recommendations.

17. In late 2023, select members of the ISCG, including the Department of National Defence (DND), the Communications Security Establishment (CSE), and CSIS once again participated in a human rights summit. This was the second year the summit ran. CSIS presented its human rights methodology, risk ratings, and human rights assessments. Through these discussions, CSIS was able to identify and understand the differences between the organisations' methodologies and ratings, as well as identify similarities and differences between the needs of other organisations and CSIS concerning human rights assessments. This also informed CSIS of future areas for consideration as the Service continuously evaluates the implementation of its human rights methodology. Summit participants requested that the Summit occur on an annual basis and be broadened to include all ISCG members.

18. CSIS also continued to share its human rights assessments, upon request, with other Canadian government departments that are subject to the *ACMFE Act*, in order to support greater coordination of shared assessments. CSIS also advises those departments and agencies when the Service imposes restrictions on specific foreign arrangements.

19. Through this and the Summit, CSIS was able to continue to build key working relationships and partnerships, supporting the sharing of profiles between departments and agencies, which in turn supported key decision-making and implementation activities across the GC.

Information Sharing Evaluation Committee (ISEC)

20. CSIS' Information Sharing Evaluation Committee (ISEC) was created in 2011 to ensure senior-level review, when applicable, of specific CSIS information sharing cases that may pose a higher risk of mistreatment. The ISEC is composed of Director General-level employees from CSIS. Representatives from the Department of Justice and GAC also attend as observers to provide input on legal, foreign policy and human rights considerations. ISEC is responsible for assessing and deciding on potentially high-risk information sharing requests by determining whether requests meet the "substantial risk" threshold and if so, what mitigation measures may

reduce the risk below that threshold. When applicable, ISEC may also be convened to assess and make determinations on "use" of information obtained from foreign agencies. This is to ensure both that the information received was not the result of mistreatment and that the use of such information will not lead to mistreatment of individuals.

21. If ISEC determines there is no "substantial risk," or that such a risk can be mitigated, the request to share is approved. If ISEC determines there is a "substantial risk" which cannot be mitigated, the request is not approved. If a "substantial risk" is identified but ISEC cannot determine whether the risk can be mitigated, the matter is referred to the CSIS Director for decision. If, based on all information available, the Director assesses that the risk can be mitigated, the request for the exchange is approved or conversely, not approved if the Director assesses the "substantial risk" cannot be mitigated.

Changes to CSIS' Foreign Information Sharing Framework

22. As noted in the 2021 report on the Service's implementation of the *ACMFE Act* and OiC requirements, CSIS implemented changes to its procedures and processes related to its foreign information sharing framework. The updated procedures were accompanied by reference tools and training. In the spirit of continuous improvement, CSIS made further modifications in 2023. This was the creation of an additional category of restriction ("paused"), allowing CSIS a means of agile response within foreign arrangements when events such as a coup d'état or other political instability unfold in partner nations. Reactions to the new framework have been positive, with operational sections benefitting from the increased policy and procedural guidance.

Training Initiatives

23. As noted in last year's report, CSIS has been working to develop and implement an internal online training course. The training would be required for all employees in affected program areas, ensuring CSIS employees in these areas fully understand how to practically apply the assessment and decision-making policies and procedures associated with foreign information sharing, while ensuring full compliance with the *ACMFE Act* and related OiC. CSIS has completed the process of developing content, and is currently building a prototype with CSIS' internal developers. The training course is expected to roll out in 2024.

24. CSIS continued to provide numerous in-person information sessions to program areas, all new intelligence officers, and foreign officer classes (to ensure robust familiarity before deployment oversees). This strengthened and reinforced employee knowledge of key elements of the *ACMFE Act* and related OiC, as well as CSIS' Foreign Information Sharing Framework, and associated policies and procedures.

25. CSIS will continue to ensure that resources and learning material are available to employees in those program areas who regularly need to apply the associated policies and procedures in the course of their duties and functions when considering dissemination of information to, or requests for information from, foreign agencies as well on the use of information obtained from foreign entities.

Integrated Terrorism Assessment Centre (ITAC)

26. Canada's Integrated Terrorism Assessment Centre (ITAC) has a mandate to produce relevant and timely threat assessments for the GC. ITAC relies on intelligence collected by partners and openly available information to report on threats, trends, and events; recommend the National Terrorism Threat Level for Canada; and set threat levels for Canadian interests worldwide. ITAC is housed within CSIS National Headquarters. It operates under the authority of the Director of CSIS in consultation with the National Security and Intelligence Advisor, who provides strategic guidance on policy and operations. It is subject to the CSIS Act, Ministerial Direction, and related internal CSIS corporate and operational policies; this includes the Service's foreign information sharing policies and procedures, including those associated with the ACMFE Act.

27. ITAC hosts analysts from across the GC with diverse experience handling sensitive information with potential implications for ACMFE. For this reason, ITAC has developed internal direction and processes to identify risk and support compliance. ITAC is an assessment body, not an intelligence collection agency.

Conclusion

28. In keeping with the ever-changing nature of our legal, policy and geopolitical landscapes, CSIS intends to continue to manage foreign information sharing dynamically and in a spirit of continuous improvement. CSIS will continue to implement the updated policy framework, develop tools to enhance objectivity in decision making, and increase awareness of responsibilities under the *Act*. CSIS' information sharing policies are also scheduled for review, which will be done in the coming year and applicable policies will be refreshed and updated where needed.

29. CSIS intends to continue implementing its internal training, to ensure its human rights methodology remains appropriate and robust, and continue to contribute to interdepartmental coordination to support and promote the protection of human rights in information sharing with foreign entities.