Canadian Security Intelligence Service | Service canadien du renseignement de sécurité

Avoiding Complicity in Mistreatment by Foreign Entities Act

Annual Report to the Minister of Public Safety

February 2023

A SAFE, SECURE AND PROSPEROUS CANADA THROUGH TRUSTED INTELLIGENCE AND ADVICE.
DES RENSEIGNEMENTS ET DES CONSEILS FIABLES POUR UN CANADA SÛR ET PROSPÈRE.

Canada

Table of Contents

Introduction

1. Many of the national security challenges facing Canada originate from or have a strong nexus to events, foreign governments, individuals and groups overseas. Thus, 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.

2. 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. CSIS recognizes the need to do this 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'[1] 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 2022 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 assesses all of its arrangements with foreign entities, including human rights considerations**. 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

[1] While not defined in the *ACMFE Act* or related September 4, 2019 OiC, CSIS continues to apply the definition of '*Substantial Risk*' as outlined in the prior September 2017 Ministerial Direction on ACMFE, as follows: "*A personal, present and foreseeable risk of mistreatment. In order to be 'substantial', the risk must be real and must be based on something more than mere theory or speculation. In most cases, the test of a substantial risk of mistreatment will be satisfied when it is more likely than not that there will be mistreatment; however, in some cases, particularly where the risk is of severe harm, the 'substantial risk' standard may be satisfied at a lower level of probability*."

has implemented arrangements. As part of this process, CSIS reviews 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. Information sharing with our 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.

7. CSIS continued the process of reviewing its current human rights risk rating methodology, and identified some areas in which it could be made more rigorous and objective. The revised methodology will include updated indicators with an associated numerical rating system, as well as a more consistent review process. CSIS is in the process of finalizing this updated methodology, and implementing it in the coming year.

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. 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 various levels of 'Restrictions' to the bulk of the affected agencies. With the introduction of the new Foreign Information Sharing Framework in January 2021, the three levels of restrictions were collapsed into one overarching set of foreign information procedures, resulting in two categories – suspended or restricted. Currently, over 80 foreign entities are subject to restrictions.

9. Notable changes during the period under review include the removal of restrictions from four foreign partners. The Service increased the human rights risk rating for two countries where we have s.17 partners from 'Low' to 'Medium' due to a deterioration in the countries' human rights environment over the past several years. The Service decreased the human rights risk rating for one country where we have s.17 partners from 'Medium' to 'Low' and from another country from 'High' to 'Medium', due to an amelioration in the country's 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 2009, the Service implemented a process of seeking **human rights assurances** from foreign agencies regarding their use of CSIS information, a practice which continues to be applied. Human rights assurances are sought to ensure the foreign agency understands and abides by CSIS expectations (and those of the broader Government of Canada) 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. Specifically, caveats on information shared with foreign agencies outline the requirement to ensure that no individual will be mistreated as a result of the shared information, and 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 under the restricted status, CSIS approaches like-minded allies in applicable regions 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.

15. In 2021, CSIS implemented a new Human Rights Assurances procedure, which required seeking updated assurances every two years from 'Restricted' partners. While CSIS has received updated assurances from some of these partners, CSIS is in the process of reviewing and requesting updated assurances from outstanding partners in the coming year as required.

Collaboration with Other Government Departments

16. CSIS continued to be involved in the Information Sharing Coordination Group (ISCG) discussions and 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.

17. The ISCG, chaired by Public Safety Canada, is the primary interdepartmental forum for

supporting interdepartmental collaboration and information-sharing between the departments and agencies, who received, or were considered for receipt of Governor-in-Council Directions. The ISCG was convened on multiple occasions in 2022, continuing discussions on the implementation of the Act, associated directions, reporting requirements, methodologies, and responses to external review body recommendations.

18. In late 2022, select members of the ISCG, including the Department of National Defence (DND), the Communications Security Establishment (CSE), GAC, and CSIS participated in a human rights summit. 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' methodology and ratings. Additionally, through this exercise, CSIS was able to update its profiles to include information shared during the summit, and also provide information to the other participants, assisting them in updating their respective assessments, further aligning the departments with one another. This also informed CSIS of potential considerations as the Service updates its human rights methodology. ISCG members have requested that the Summit occur on an annual basis and be broadened to include all ISCG members.

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

20. 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 GoC.

Information Sharing Evaluation Committee (ISEC)

21. 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 to ensure the use of such information will not lead to mistreatment of individuals.

22. 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

23. As noted in last year's 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 key changes were to: integrate the previous Deputy Director Operations' Directive on ACMFE and related 'Restrictions' mechanisms into one overarching set of foreign information procedures; collapse multiple levels of 'Restrictions' into two categories ('Suspended' or 'Restricted'), allowing for a more clear and consistent approval process on foreign information sharing requests; focus decision making at the 'substantial risk' threshold as defined in the prior 2017 MD on ACMFE, which the Service continues to apply under the 2019 *ACMFE Act* and OiC; and require updated assurances every two years from foreign agencies on the 'Restricted' list.

24. The official launch of this new framework occurred in late January 2021, preceded by outreach to all affected employees, including a series of information sessions. The updated procedures were accompanied by reference tools, training, and enhanced measures to assess human rights risks. Reactions to the new framework generally continue to be positive with operational sections benefitting from the increased policy and procedural guidance and the lowered approval levels for some lower risk situations.

Training Initiatives

25. 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, and would ensure CSIS employees in these program 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 pulling together the content for the course, and is currently building a prototype with CSIS' internal developers. The training course is expected to roll out in the coming year.

26. CSIS continued to provide in-person information sessions to program areas, and foreign officer classes, to strengthen and reinforce key elements of the *ACMFE Act* and related OiC, as well as CSIS' Foreign Information Sharing Framework, and associated policies and procedures.

27. 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)

28. Canada's Integrated Terrorism Assessment Centre (ITAC) has a mandate to produce relevant and timely threat assessments on terrorism for the Government of Canada. ITAC relies on intelligence collected by partners and openly available information to report on terrorism threats, trends, and events; recommend the National Terrorism Threat Level for Canada; and set threat levels for Canadian interests world-wide. ITAC is housed within CSIS National Headquarters and 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*.

29. ITAC hosts analysts from across the Government of Canada with varying degrees of 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. Assessments are approved at a senior level and products are disseminated to international partners who are entitled to the information, in particular, because they fall within CSIS ACMFE governance.

Conclusion

30. 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.

31. Over the coming year, CSIS also intends to implement its internal online training course, update its human rights methodology, and continue to contribute to interdepartmental coordination to support and promote the protection of human rights in information sharing with foreign entities.