UNCLASSIFIED

Avoiding Complicity in Mistreatment by Foreign Entities Act

Annual Report to the Minister of Public Safety

February 2022

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.

Canadian Security Intelligence Service
Service canadien du renseignement de sécurité

Canada

Table of Contents

Introduction

1. The security environment remains complex and dynamic, transcending national boundaries. The global pandemic only reinforced the increasingly blurry distinction between domestic and foreign threats. Over the past two years, CSIS noted an increase in both the scope and scale of hostile threat actors' activities targeting innovative sectors of the Canadian economy, as well as increased levels of foreign interference in Canada. As such, domestic national security threats are more often influenced by and connected to events or trends outside Canada.

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,*" while requiring 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* required 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 2021 calendar year reporting period**. During this period and as previewed in last year's report, CSIS implemented a robust new approach further to a periodic review of our foreign information sharing regime.

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

[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.*"

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. 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 *ACFME 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 also continues 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.

CSIS Foreign Agency 'Restrictions' Mechanism

8. The 2017 Ministerial Direction (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. While it is often difficult to corroborate allegations that a foreign agency engages in or contributes 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. Currently, over 80 foreign entities are subject to such restrictions.

9. The restrictions mechanism that existed prior to the January 2021 introduction of the new Foreign Information Sharing Framework had three categories of partners, of which one involved a complete suspension of classified exchanges and another required foreign information sharing instances to be automatically referred to the Information Sharing Evaluation Committee (ISEC).

10. During the period under review, the Director did not carry out any change to the 'Restricted' list. The Service did increase the human rights risk rating of a country where we have a s.17 partner from 'Low' to 'Medium' due to a deterioration in the country's human rights environment over the past several years.

Mitigation Measures

11. 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).

12. 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*.

13. 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.

14. 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. In this reporting period, CSIS began implementing a new Human Rights Assurances procedure, which requires seeking updated assurances every two years from 'Restricted' partners.

Information Sharing Evaluation Committee (ISEC)

15. 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 senior managers from CSIS. Representatives from the Department of Justice and GAC also attend as observers to provide valuable 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, are there mitigation measures in place which 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.

16. 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

17. As previewed in last year's 2020 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 during this 2021 reporting period**. The key changes are to:

- integrate the previous Deputy Director Operations' Directive on ACMFE and related 'Restrictions' mechanism into one overarching set of foreign information procedures on disclosures/requests and on use of information, incorporating the status of the arrangement and the assessment criteria into the evaluation and then requiring approval levels commensurate with risk;
- provide updated tools to employees and managers to ensure a common understanding of the policies and procedures;
- collapse multiple levels of 'Restrictions' into two categories ('Suspended' or 'Restricted'), allowing for a more clear and consistent approval processes 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.

18. Taken together, the intent of these changes is to facilitate better informed, more nimble information sharing with foreign partners, while ensuring compliance with our legal obligations under the *ACMFE Act* and related OiC. The changes should achieve those results by creating one overarching approach which aims to: offer greater precision on levels of approval commensurate with the risk involved; simplify foreign agency 'Restriction' levels; empower senior officials to make decisions on the 'substantial risk' of mistreatment and their mitigation measures while retaining a role for ISEC; and institute a more robust and consistent approach to seeking human rights assurances.

19. Under the new Framework, CSIS officers must evaluate all proposed exchanges with a foreign entity against specific criteria:

a) Based on the available information about the foreign entity, if the information is disclosed or requested, is it more likely than not that the foreign entity will engage in torture or other forms of cruel, inhuman or degrading treatment or punishment against an individual;
b) If the information is disclosed or requested, is it more likely than not that the foreign entity will disseminate the information in an unauthorized manner to a 3rd party, which may result in torture or other forms of cruel, inhuman or degrading treatment or punishment against an individual by that 3rd party;
c) If the information is disclosed or requested, is it more likely than not that it may result in the extraordinary rendition of an individual by the foreign entity which would lead to the individual being tortured or subject to other forms of cruel, inhuman or degrading treatment or punishment;

d) If the information is disclosed or requested, is the possibility of an extra-judicial killing of an individual by the foreign entity or other security entities within the country more likely than not.

Additionally, proposed exchanges with agencies on the 'Restricted' list require review / approvals at more senior levels within the Service.

20. 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 are accompanied by reference tools, training, and enhanced measures to assess human rights risks. The reaction to the new framework has generally been positive as operational sections have benefited from the increased policy and procedural guidance and the lowered approval levels for some lower risk situations. Specifically, some teams have highlighted that the new framework increased the volume and timeliness of exchanges, and that it has thus improved CSIS's relationships with foreign partners.

21. In keeping with the ever-changing nature of our legal, policy and geopolitical landscapes, we intend to manage foreign information sharing dynamically and in a spirit of continuous improvement. Over the coming year, we intend to carry out a review of the new procedures, develop and implement an internal online training course and strive for enhanced interdepartmental coordination, particularly when assessing and mitigating the risk of mistreatment in countries where there are serious human rights concerns.

Integrated Terrorism Assessment Centre (ITAC)

22. Canada's Integrated Terrorism Assessment Centre (ITAC) has a mandate to produce accurate, relevant and timely threat assessments on terrorism for the Government of Canada. ITAC is housed within CSIS National Headquarters and its governing body is the Deputy Ministers' Committee on National Security. ITAC is not mentioned in the *ACMFE Act* nor has it been issued an OiC. However, the *CSIS Act* as and related CSIS internal corporate and operational policies apply to ITAC, as per the 2005 Treasury Board decision that created it. ITAC mirrors Ministerial guidance issued to CSIS and has adapted the Service's foreign information sharing policies and procedures for its own use. ITAC operates under CSIS' broader authorities and policies, including those associated with the *ACMFE Act*.

Information obtained from a detainee, regardless of whether mistreatment is suspected, is only used if it is critical in supporting ITAC's assessment and only if is corroborated by other sources. In cases where this information is required to support the assessment of an ITAC product, only the ITAC Executive Director is authorized to review the request and, if applicable, approve its use. ITAC makes use of CSIS risk assessments characterizing source agencies in determining whether mistreatment was likely in acquiring information, as it does not possess resources to do so independently.