



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 and Emergency Preparedness Canada

February 2021

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.....	p.3
Foreign Information Sharing & Human Rights	p.3
Foreign Agency ‘Restrictions’ Mechanism	p.4
Mitigation Measures	p.5
Information Sharing Evaluation Committee (ISEC).....	p.6
Changes to the Foreign Information Sharing Framework....	p.6
Canada’s Integrated Terrorism Assessment Centre (ITAC)	p.7

Introduction

1. The ability to share information in a timely manner with our foreign partners is critical to CSIS' ability to identify and manage threats to Canada's national security and the safety of Canadians. 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.
2. 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 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 *ACMFE 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 2020 calendar year reporting period.** During this period, CSIS continued to apply its existing foreign information sharing framework, while developing and implementing a robust new approach further to a periodic review of our current posture.
3. The security environment is dynamic, complex, and transcends national boundaries, including in a borderless online space. Canada must rely on timely and efficient information sharing with foreign agencies to address security threats to Canada and Canadian interests, at home and abroad. Moreover, just as we would expect foreign partners to advise us of any information they may acquire regarding threats to Canada, we have an obligation to do the same should we obtain information on potential security threats to our foreign partner nations. This is especially true on the counter terrorism front.

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 and Emergency Preparedness and supported by the Minister of Foreign Affairs, in accordance with s.17(1)(b) of the *CSIS Act*. The process to establish CSIS arrangements with foreign agencies is stringent and takes into consideration a wide range of issues, including Canadian security requirements, respect for human rights and the reliability of the foreign agency. Prior to seeking the Minister's approval for new arrangements, CSIS also proactively consults with Global Affairs Canada (GAC) on such initiatives in instances where there are human rights or foreign policy considerations.

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."

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 and risks of mistreatment.** CSIS also reviews various yearly government human rights reports (e.g. GAC human rights reporting; US State Department Country Reports) and open-source reporting from non-governmental entities (e.g. Amnesty International; Human Rights Watch; reporting from established media outlets etc.) for all countries where the Service has implemented Ministerially-approved 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. 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 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 prior 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, CSIS assessed all of the entities with which we have established arrangements in countries rated as 'High' on the Service's 'Human Rights Country Risk' ratings. CSIS then assigned various levels of 'Restrictions' to the bulk of the affected agencies. Currently, over 80 foreign entities are subject to such restrictions. The restrictions mechanism used during this review period was in effect since March 2018.

9. When a foreign agency is defined as 'Restricted' from a human rights perspective, CSIS must evaluate all proposed exchanges with the agency against specific criteria:

- a) Based on the available information about the foreign entity, if the information is disclosed or requested, is there a probability 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 there a probability 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 there a possibility 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 there a possibility of an extra-judicial killing of an individual by the foreign entity or other security entities within the country.

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

10. During the period under review, the Director approved the removal of one foreign agency from the 'Restricted' list and lowered the country's 'Human Rights Risk Rating' from 'High' to 'Medium' due to a lack of specific allegations of mistreatment against the agency for the past several years, and an overall improvement of the human rights environment within the country's broader security sector. Furthermore, one agency was added to the 'Restricted' category due to allegations of mistreatment noted in open-source human rights reporting, while the 'Country Risk Rating' for two other countries was raised from 'Medium' to 'High' due to increased reporting noting allegations of mistreatment within the broader security community.

Mitigation Measures – Assurances and Caveats

12. CSIS must assess and attempt to mitigate substantial risks of mistreatment when considering sharing certain types of information with foreign entities. Mitigation efforts include – but are not limited to – obtaining updated human rights assurances from a foreign agency and placing caveats on information shared with a foreign agency.

13. 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 apply. 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*.

14. 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.

15. 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.

Information Sharing Evaluation Committee (ISEC)

16. 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 as well as representatives from the Department of Justice and GAC. 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.

17. 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

18. As reported in last year's 2019 report on the Service's implementation of the *ACMFE Act* and OiC requirements, **CSIS continued to undertake an extensive internal process to review and update its procedures and processes related to its foreign information sharing framework during this 2020 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; 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.

19. Taken together, these changes are intended 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.

20. The official launch of this new framework was initially targeted for mid-2020 following a planned series of information sessions to key stakeholders. However, initial delays were incurred in the finalization of this entire process at the onset of the COVID-19 pandemic. Briefings to internal stakeholders were subsequently delivered from July to November 2020, outlining the key components of the *ACMFE Act* and the OiC, as well as planned changes to the procedures. These updated procedures and associated tools and guides were being finalized at the end of this reporting period, and officially launched in late January 2021. The updated procedures are accompanied by reference tools, training, and enhanced measures to assess human rights risks. Results of this initiative will be reported to the Minister in the next *ACMFE Act* annual report covering the 2021 calendar year period.

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. For example, we will strive for enhanced interdepartmental coordination with other Government of Canada departments and agencies which are also subject to the *ACMFE Act*, 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* 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 it 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.