



Canadian Security  
Intelligence Service

Service canadien du  
renseignement de sécurité



# *Avoiding Complicity in Mistreatment by Foreign Entities Act*

2025 Annual Report

Canada 

**Land acknowledgment**

The Canadian Security Intelligence Service acknowledges that this report was written and published on the traditional and unceded territory of the Algonquin Anishinaabeg People.

Cat. No.: PS71-5E-PDF

ISSN: 2819-1080

[www.canada.ca/CSIS](http://www.canada.ca/CSIS)

Photography: © CSIS Photography

© His Majesty the King in Right of Canada, as represented by the Minister of Public Safety, 2026.

Published in April 2026.

Aussi disponible en français sous le titre : *Loi visant à éviter la complicité dans les cas de mauvais traitements infligés par des entités étrangères.*

# Table of contents

Introduction	4
CSIS foreign information sharing and human rights	4
CSIS foreign agency restrictions mechanism	5
Mitigation measures	5
Collaboration with other government departments	5
Information Sharing Evaluation Committee	6
Changes to CSIS' Foreign Information Sharing Framework	6
Training initiatives	6
Integrated Threat Assessment Centre	7
Conclusion	7

## Introduction

Canada exists in a complex global environment, and our national security frequently has links to events, people, and entities outside of our borders. As a result, the Canadian Security Intelligence Service (CSIS) engages in international information exchanges as a critical component of its mandate to protect Canada's national security interests. CSIS is committed to adhering to Canadian laws, values, and international obligations, including the principles outlined in the *Canadian Charter of Rights and Freedoms*. The *Avoiding Complicity in Mistreatment by Foreign Entities Act* (ACMFE Act) requires CSIS to conduct information sharing with foreign partners in a manner that does not result in a "substantial risk" of contributing to the mistreatment of any individual. This ensures that national security objectives are achieved, while still upholding Canada's commitment to human rights and the rule of law.

The ACMFE Act requires the Governor-in-Council to issue directions to deputy heads of federal government departments and agencies that conduct information sharing activities with foreign entities. The September 2019 Order-in-Council (OiC) to the Director of CSIS outlines CSIS' responsibilities when disclosing, requesting, or using information from foreign entities. The ACMFE Act requires deputy heads, to whom directions have been issued, to submit a report to the appropriate minister on the implementation of those directions during the previous calendar year. This report outlines the key components of CSIS' implementation of the ACMFE Act, and the related OiC, during the 2025 calendar year.

## CSIS foreign information sharing and human rights

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, the reliability of the foreign agency, and the human rights track record of the country. CSIS conducts regular reviews of these arrangements, a process which includes a comprehensive search of classified and open-source information from reputable sources to evaluate the human rights situation.

In 2025, CSIS continued to implement its revised human rights assessment methodology, a process which began in 2023. When conducting the research for these assessments, CSIS consults its classified holdings, trusted partners, and reputable open-source resources. This approach, in addition to updated indicators and a weighted numerical rating system, allows for a more consistent and objective review process.

CSIS carefully documents the information it shares with foreign partners. 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 if so, whether that risk can be mitigated (see section on mitigation measures).

As required in the ACMFE Act and the related OiC, if a substantial risk of mistreatment cannot be mitigated, the information is not shared.

## **CSIS foreign agency restrictions mechanism**

CSIS introduced its Foreign Information Sharing Framework in 2021. This framework included the creation of two categories of arrangement, “restricted” and “suspended,” for use with foreign entities who do not share Canada’s respect for human rights. Restrictions do not mean information cannot be shared; rather, a higher level of review and approval is required to ensure robust compliance with the ACMFE Act before information sharing takes place. Currently, over 70 foreign entities are subject to restrictions.

## **Mitigation measures**

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 below the “substantial” threshold. Mitigation efforts can include obtaining updated human rights assurances from a foreign agency, placing caveats on information shared, and using a redacted version of the information (e.g. a form of words).

As part of its risk management strategy, CSIS seeks human rights assurances from its foreign partners. These assurances outline that CSIS’ information is not to be used in any way that would result in the mistreatment of any individual, and that adherence to international law, including the

*United Nations Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment*, is maintained. In addition to seeking assurances, CSIS applies human rights caveats to case-specific information shared with foreign partners. These caveats provide clear expectations regarding the handling of sensitive information and the protection of human rights, and include provisions related to the dissemination of information to third parties. CSIS also leverages its relationships with like-minded allies to gather information about their experiences and feedback regarding the human rights practices of these entities.

CSIS tracks the receipt of assurances from foreign agencies, and investigates instances where there may be concerns about non-compliance. When concerns exist, CSIS may limit or further restrict the information to be shared. CSIS also regularly seeks updated assurances from foreign entities to ensure that their information-sharing activities are aligned with Canada’s human rights obligations.

## **Collaboration with other government organizations**

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 National Security and Intelligence Review Agency’s 2021 ACMFE Act review.

The ISCG, chaired by Public Safety Canada, is an interdepartmental forum to support collaboration and information-sharing

between departments and agencies that received, or were considered for receipt of, Governor-in-Council directions. In 2025, the ISCG was convened on multiple occasions to continue discussions on the implementation of the Act, associated directions, reporting requirements, methodologies, and responses to external review body recommendations.

CSIS also continued to share its human rights assessments, upon request, with other Canadian government organizations that are subject to the ACMFE Act, to support greater coordination of shared assessments.

## **Information Sharing Evaluation Committee**

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. ISEC is composed of director general-level employees from CSIS. Representatives from the Department of Justice and Global Affairs Canada also attend as observers to provide input on legal, foreign policy, and human rights considerations. ISEC assesses potentially high-risk information sharing requests by determining whether requests meet the "substantial risk" threshold, and if so, decides 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 that CSIS' use of such information will not lead to mistreatment of individuals.

If ISEC determines there is no "substantial

risk," or that such a risk can be mitigated, the request to share, or use, the information 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 Director of CSIS for decision. If, based on all information available, the Director assesses that the risk can be mitigated, the request for the exchange or use is approved, or conversely, not approved if the Director assesses the "substantial risk" cannot be mitigated.

## **Changes to CSIS' Foreign Information Sharing Framework**

In 2021, 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.

## **Training Initiatives**

Throughout 2025, CSIS continued to provide numerous in-person information sessions to program areas, including new intelligence officers and foreign officer classes (to ensure robust familiarity before deployment overseas). This strengthened and reinforced employee knowledge of key elements of the ACMFE Act and the related OiC, CSIS' Foreign Information Sharing Framework, and the associated policies and procedures. CSIS has continued to work on developing and implementing further training initiatives to augment the regular in-person sessions.

CSIS will continue to ensure that resources and learning materials are available to employees that 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 Threat Assessment Centre**

The Integrated Threat Assessment Centre (ITAC) is a specialized organization in the Canadian intelligence community responsible for providing timely, relevant, and objective assessments based on all-source information. Those assessments enable decision makers and security partners to safeguard Canadians and advance Canadian interests, both at home and abroad. ITAC actively monitors both intelligence collected by partners, and a variety of open sources of information, to make recommendations to the Director of CSIS on the National Terrorism Threat Level (NTTL), and to produce reports containing data, trend analysis and strategic assessments.

ITAC operates within the CSIS national headquarters and is accountable to the Director. ITAC is subject to ministerial direction, and related internal CSIS corporate and operational policies. This includes its foreign information sharing policies and procedures, such as those associated with the ACMFE Act.


Where required, the Executive Director of ITAC has the authority to develop policies and practices specific to ITAC's circumstances. Because of the regular

rotation of seconded personnel, and due to its specific mandate, ITAC has unique training and practices in place to ensure compliance.

Finally, ITAC does not directly disseminate its intelligence products outside of the Five Eyes. The sharing of ITAC assessments to foreign entities beyond the Five Eyes is governed by CSIS operational policies and procedures to ensure compliance with information-sharing requirements.

## **Conclusion**

In keeping with the ever-evolving nature of our legal, policy, and geopolitical landscapes, CSIS will continue to manage foreign information sharing dynamically and in a spirit of continuous improvement. CSIS will also continue to implement the updated policy framework, develop new and better tools to enhance objectivity in decision making, and increase awareness of responsibilities under the ACMFE Act.



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.

**For more information, contact us at:**

**Canadian Security Intelligence Service  
PO Box 9732 STN T  
Ottawa ON K1G 4G4  
Canada**

**Telephone: 613-993-9620  
TTY and or TDD: 613-991-9228**

[www.canada.ca/CSIS](http://www.canada.ca/CSIS)